Kementerian Pendidikan dan Kebudayaan
Republik Indonesia
2013

RANCANG BANGUN JARINGAN

UNTUK SMK / MAK KELAS XI

SEMESTER 2

PENULIS : **SONDY CK**

EDITOR :

EDITOR BAHASA :

ILUSTRASI SAMPUL :

DESAIN & ILUSTRASI BUKU :

Jl. Teluk Mandar, Arjosari Tromol Pos 5, Malang 65102, Telp. (0341) 491239, (0341) 495849, Fax. (0341) 491342, Surel: vedcmalang@vedcmalang.or.id, Laman: www.vedcmalang.com

KATA PENGANTAR

Puji syukur kami panjatkan kepada Tuhan Yang Maha Esa atas tersusunnya buku teks ini, dengan harapan dapat digunakan sebagai buku teks untuk siswa Sekolah Menengah Kejuruan (SMK) Program Keahlian Bidang Studi Teknik Komputer dan jaringan, Rancang Bangun Jaringan.

Penerapan kurikulum 2013 mengacu pada paradigma belajar kurikulum abad 21 menyebabkan terjadinya perubahan, yakni dari pengajaran (*teaching*) menjadi belajar (*learning*), dari pembelajaran yang berpusat kepada guru (*teachers-centered*) menjadi pembelajaran yang berpusat kepada peserta didik (*student-centered*), dari pembelajaran pasif (*pasive learning*) ke cara belajar peserta didik aktif (*active learning*) atau *Student Active Learning*.

Buku teks ″Rancang Bangun Jaringan″ ini disusun berdasarkan tuntutan paradigma pengajaran dan pembelajaran kurikulum 2013 diselaraskan berdasarkan pendekatan model pembelajaran yang sesuai dengan kebutuhan belajar kurikulum abad 21, yaitu pendekatan model pembelajaran berbasis peningkatan keterampilan proses sains.

Penyajian buku teks untuk Mata Pelajaran ″Rancang Bangun Jaringan″ ini disusun dengan tujuan agar supaya peserta didik dapat melakukan proses pencarian pengetahuan berkenaan dengan materi pelajaran melalui berbagai aktivitas proses sains sebagaimana dilakukan oleh para ilmuwan dalam melakukan eksperimen ilmiah (penerapan scientifik), dengan demikian peserta didik diarahkan untuk menemukan sendiri berbagai fakta, membangun konsep, dan nilai-nilai baru secara mandiri.

Kementerian Pendidikan dan Kebudayaan, Direktorat Pembinaan Sekolah Menengah Kejuruan, dan Direktorat Jenderal Peningkatan Mutu Pendidik dan Tenaga Kependidikan menyampaikan terima kasih, sekaligus saran kritik demi kesempurnaan buku teks ini dan penghargaan kepada semua pihak yang telah berperan serta dalam membantu terselesaikannya buku teks siswa untuk Mata Pelajaran Rancang Bangun Jaringan Kelas XI / Semester 2 Sekolah Menengah Kejuruan (SMK).

Jakarta, November 2013

Menteri Pendidikan dan Kebudayaan

DAFTAR ISI

DAFTAR GAMBAR

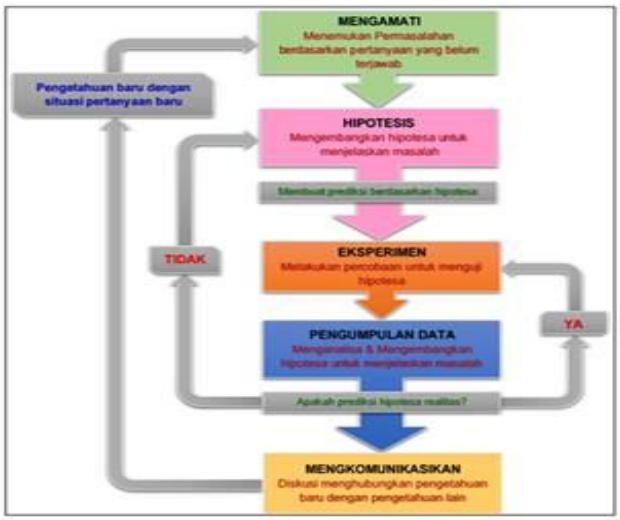
DAFTAR TABEL

BAGIAN 1 : PENDAHULUAN

1. Deskripsi

Rancang bangun jaringan adalah salah satu mata pelajaran wajib dasar program keahlian Teknik Komputer dan Informatika (TKI). Berdasarkan struktur kurikulum mata pelajaran perakitan komputer disampaikan di kelas X semester 1 dan semester 2 masing-masing 4 jam pelajaran. Untuk semester 1 topik materi pembelajaran menekankan pada memahami hubungan komputer ke jaringan, penyambungan internet melalui ISP, pengalamatan jaringan, layanan-layanan jaringan, internet dan pemanfaatannya, meja bantuan (help desk), perencanaan pemutakhiran jaringan dan perencanaan struktur pengalamatan. Sedangkan untuk semester 2 topik materi pembelajaran menekankan pada memahami konfigurasi peralatan-peralatan jaringan, routing jaringan komputer, layanan-layanan ISP, tugas dan tanggung jawab ISP, jaringan di enterprise, eksplorasi infrastruktur jaringan perusahaan, switching pada jaringan perusahaan.

Pembelajaran rancang bangun jaringan ini menggunakan metode pendekatan scientifik. Dalam pendekatan ini praktikum atau eksperimen berbasis sains merupakan bidang pendekatan ilmiah dengan tujuan dan aturan khusus, dimana tujuan utamanya adalah untuk memberikan bekal ketrampilan yang kuat dengan disertai landasan teori yang realistis mengenai fenomena yang akan kita amati. Ketika suatu permasalahan yang hendak diamati memunculkan pertanyaan-pertanyaan yang tidak bisa terjawab, maka metode eksperimen ilmiah hendaknya dapat memberikan jawaban melalui proses yang logis. Proses-proses dalam pendekatan scientifik meliputi beberapa tahapan (gambar 1.1) yaitu: mengamati, hipotesis atau menanya, mengasosiasikan atau eksperimen, mengumpulkan atau analisa data dan mengkomunikasikan. Proses belajar pendekatan eksperimen pada hakekatnya merupakan proses berfikir ilmiah untuk membuktikan hipotesis dengan logika berfikir.



Gambar 1.0 Diagram Proses Metode Scientifik-Eksperimen Ilmiah

2. Prasyarat

Berdasarkan peta kedudukan bahan ajar, mata pelajaran Rancang Bangun Jaringan ini berdiri sendiri dan bersama sama satu kelompok dengan mata pelajaran pemrograman web, system operasi, perakitan computer dan simulasi digital. Rancang Bangun Jaringan merupakan tahapan untuk memahami bagaimana suatu jaringan komputer dapat digunakan dan memberikan manfaat. Untuk memahami Rancang Bangun Jaringan, dibutuhkan pemahaman terhadap hubungan komputer dengan jaringan, peranan ISP dalam memberikan layanan-layanan internet, pengalamatan jaringan, fungsi dan tugas meja bantuan.

3. Petunjuk Penggunaan

Buku pedoman siswa ini disusun berdasarkan kurikulum 2013 yang mempunyai ciri khas penggunaan metode scientifik. Buku ini terdiri dari dua bab yaitu bab 1 pendahuluan dan bab 2 pembelajaran. Dalam bab pendahuluan beberapa yang harus dipelajari peserta didik adalah deskripsi mata pelajaran yang berisi informasi umum, rasionalisasi dan penggunaan metode scientifik. Selanjutnya pengetahuan tentang persyaratan, tujuan yang diharapkan, kompetensi inti dan dasar yang akan dicapai serta test kemampuan awal.

Bab 2 menuntun peserta didik untuk memahami deskripsi umum tentang topik yang akan dipelajari dan rincian kegiatan belajar sesuai dengan kompetensi dan tujuan yang akan dicapai. Setiap kegiatan belajar terdiri dari tujuan dan uraian materi topik pembelajaran, tugas serta test formatif. Uraian pembelajaran berisi tentang deskripsi pemahaman topik materi untuk memenuhi

kompetensi pengetahuan. Uraian pembelajaran juga menjelaskan deskripsi unjuk kerja atau langkah-langkah logis untuk memenuhi kompetensi skill.

Tugas yang harus dikerjakan oleh peserta didik dapat berupa tugas praktek, eksperimen atau pendalaman materi pembelajaran. Setiap tugas yang dilakukan melalui beberapa tahapan scientifik yaitu : 1) melakukan pengamatan setiap tahapan unjuk kerja 2) melakukan praktek sesuai dengan unjuk kerja 3) mengumpulkan data yang dihasilkan setiap tahapan 4) menganalisa hasil data menggunakan analisa diskriptif 5) mengasosiasikan beberapa pengetahuan dalam uraian materi pembelajaran untuk membentuk suatu kesimpulan 6) mengkomunikasikan hasil dengan membuat laporan portofolio. Laporan tersebut merupakan tagihan yang akan dijadikan sebagai salah satu referensi penilaaian.

4. Tujuan Akhir

Setelah mempelajari uraian materi dalam bab pembelajaran dan kegiatan belajar diharapkan peserta didik dapat memiliki kompetensi sikap, pengetahuan dan ketrampilan yang berkaitan dengan materi:

- Konfigurasi peralatan-peralatan jaringan
- Routing jaringan komputer
- Layanan-layanan ISP
- Tugas dan tanggung jawab ISP
- Jaringan di enterprise
- Eksplorasi infrastruktur jaringan perusahaan
- Switching pada jaringan perusahaan

5. Kompetensi Inti Dan Kompetensi Dasar

1. Kompetensi Inti 1 : Menghayati dan mengamalkan ajaran agama yang dianutnya.
   Kompetensi Dasar :

   1.1 Memahami nilai-nilai keimanan dengan menyadari hubungan keteraturan dan kompleksitas alam dan jagad raya terhadap kebesaran Tuhan yang menciptakannya
   1.2 Mendeskripsikan kebesaran Tuhan yang menciptakan berbagai sumber energi di alam
   1.3 Mengamalkan nilai-nilai keimanan sesuai dengan ajaran agama dalam kehidupan sehari-hari
2. Kompetensi Inti 2: Menghayati dan Mengamalkan perilaku jujur, disiplin, tanggung jawab, peduli (gotong royong, kerjasama, toleran, damai), santun, responsif dan proaktif dan menunjukan sikap sebagai bagian dari solusi atas berbagai permasalahan dalam berinteraksi secara efektif dengan lingkungan sosial dan alam serta dalam menempatkan diri sebagai cerminan bangsa dalam menempatkan diri sebagai cerminan bangsa dalam pergaulan dunia.
   Kompetensi Dasar:

   2.1 Menunjukkan perilaku ilmiah (memiliki rasa ingin tahu; objektif; jujur; teliti; cermat; tekun; hati-hati; bertanggung jawab; terbuka; kritis; kreatif; inovatif dan peduli lingkungan) dalam aktivitas sehari-hari sebagai wujud implementasi sikap dalam melakukan percobaan dan berdiskusi
   2.2 Menghargai kerja individu dan kelompok dalam aktivitas sehari-hari sebagai wujud implementasi melaksanakan percobaan dan melaporkan hasil percobaan
3. Kompetensi Inti 3: Memahami, menerapkan dan menganalisis pengetahuan faktual, konseptual, dan prosedural berdasarkan rasa ingin tahunya tentang ilmu pengetahuan, teknologi, seni, budaya, dan humaniora dalam wawasan kemanusiaan, kebangsaan ,

kenegaraan, dan peradaban terkait penyebab fenomena dan kejadian dalam bidang kerja yang spesifik untuk memecahkan masalah.

Kompetensi Dasar :

3.1 Memahami konfigurasi peralatan-peralatan jaringan
3.2 Memahami routing jaringan komputer
3.3 Memahami layanan-layanan ISP
3.4 Memahami tugas dan tanggung jawab ISP
3.5 Memahami jaringan di enterprise
3.6 Memahami eksplorasi infrastruktur jaringan perusahaan
3.7 Memahami switching pada jaringan perusahaan

4. Kompetensi Inti 4: Mengolah, menalar, dan menyaji dalam ranah konkret dan ranah abstrak terkait dengan pengembangan dari yang dipelajarinya di sekolah secara mandiri, dan mampu melaksanakan tugas spesifik dibawah pengawasan langsung.
   Kompetensi Dasar :

   4.1 Menyajikan hasil pengembangan jaringan sederhana
   4.2 Menganalisa routing jaringan komputer
   4.3 Menganalisa layanan-layanan ISP
   4.4 Menalar tugas dan tanggung jawab ISP
   4.5 Menalar jaringan di enterprise
   4.6 Menalar eksplorasi infrastruktur jaringan perusahaan
   4.7 Menalar switching pada jaringan perusahaan

6. Cek Kemampuan Awal

1. *Jelaskan konfigurasi peralatan-peralatan jaringan*
2. *Jelaskan routing jaringan komputer*
3. Jelaskan layanan-layanan ISP
4. Jelaskan tugas dan tanggung jawab ISP
5. Jelaskan jaringan di enterprise
6. Jelaskan eksplorasi infrastruktur jaringan perusahaan
7. Jelaskan switching pada jaringan perusahaan

BAGIAN 2 : PEMBELAJARAN

A. Deskripsi

Rancang bangun jaringan merupakan mata pelajaran yang membahas konfigurasi peralatan-peralatan jaringan, routing jaringan komputer, layanan-layanan ISP, tugas dan tanggung jawab ISP, jaringan di enterprise, eksplorasi infrastruktur jaringan perusahaan dan switching pada jaringan perusahaan.

B. Kegiatan Belajar

Kegiatan belajar menjelaskan tentang aktifitas pembelajaran yang dilakukan siswa, meliputi mempelajari uraian materi, mengerjakan test formatif dan tugas atau eksperimen dari proses mengamati sampai menyusun laporan

1. BAB I

1.1 Kegiatan Belajar 1 : Memahami Konfigurasi Peralatan-peralatan Jaringan

1.1.1 Tujuan Pembelajaran

Setelah mengikuti kegiatan belajar 1 ini siswa diharapkan dapat memahami konfigurasi peralatan-peralatan jaringan.

1.1.2 Aktifitas Belajar Siswa

1.1.2.1 Mengamati

Selama mengikuti kegiatan belajar 1 ini siswa diharapkan dapat mengamati :

- Inisiasi konfigurasi router ISR
- Setup fisik pada ISR
- Konfigurasi SDM Express
- Konfigurasi koneksi WAN menggunakan SDM Express
- Konfigurasi NAT menggunakan SDM
- Konfigurasi router menggunakan CLI IOS
- Konfigurasi default route
- Konfigurasi layanan DHCP
- Konfigurasi NAT dengan CLI
- Back-up konfigurasi router
- Hubungan CPE ke ISP
- Konfigurasi koneksi WAN

1.1.2.2 Menanya

Selama mengikuti kegiatan belajar 1 ini siswa diharapkan dapat :

- Mendiskusikan inisiasi konfigurasi router ISR
- Mendiskusikan setup fisik pada ISR
- Mendiskusikan konfigurasi SDM Express
- Mendiskusikan konfigurasi koneksi WAN menggunakan SDM Express
- Mendiskusikan konfigurasi NAT menggunakan SDM
- Mendiskusikan konfigurasi router menggunakan CLI IOS
- Mendiskusikan konfigurasi default route
- Mendiskusikan konfigurasi layanan DHCP
- Mendiskusikan konfigurasi NAT dengan CLI
- Mendiskusikan back-up konfigurasi router
- Mendiskusikan hubungan CPE ke ISP
- Mendiskusikan konfigurasi koneksi WAN

1.1.2.3 Mengumpulkan Informasi

Router ISR

ISR adalah singkatan dari Integrated

Services Router, dimana router ini menggabungkan beberapa layanan yang biasanya disediakan oleh peralatan-peralatan terpisah ke dalam satu router saja. Integrated Services Router yang sudah sampai pada versi 2 untuk saat ini (versi Cisco), dapat mengakomodasi kebutuhan antara kantor pusat dan kantor-kantor cabang akan video-conferencing dan layanan virtualisasi serta pertukaran data multimedia dalam jaringan WAN.

Dengan peningkatan jumlah kantor cabang atau perwakilan yang disertai dengan peningkatan jumlah karyawan, maka tim TI di suatu perusahaan menghadapi tantangan yang semakin besar. Tantangan tersebut adalah bagaimana menyediakan suatu layanan antara kantor-kantor cabang dan kantor pusat secara aman dan efisien dengan biaya yang murah. Dengan penggunaan Integrated Services Router maka kantor-kantor cabang dapat :

- Menyediakan layanan jaringan yang lebih maju dengan WAN yang ada
- Semakin produktif dengan menggunakan layanan berbasis kolaborasi video dan layanan multimedia lainnya
- Secara bertahap melakukan transisi yang aman dengan layanan-layanan cloud dan virtualisasi
- Memungkinkan penghematan biaya dengan penggunaan listrik yang kecil
- Menyediakan layanan yang handal dengan dukungan tim TI yang kecil

Gambar 1.1 Salah Satu Contoh ISR Cisco 819

Keunggulan ISR Dibandingkan dengan router-router

konvensional yang biasa digunakan, maka router dalam jajaran Integrated Services Router memiliki keunggulan-keunggulan sebagai berikut :

- Penggunaan layanan berbasi video yang unggul
- Dapat mendeteksi dan melakukan optimalisasi berbagai macam media dan aplikasi yang digunakan untuk memberikan pengalaman penggunaan yang lebih memuaskan
- Dapat mendeteksi perubahan jaringan dan perangkat serta layanan yang digunakan
- Memiliki media engine yang memungkinkan aplikasi berbasis video berkualitas tinggi digunakan dalam urusan bisnis
- Memberikan layanan video yang dapat disesuaikan dengan aplikasi yang digunakan (misalkan : telekonfrensi video, streaming video) dengan bandwidth yang sudah dioptimalkan
- Layanan virtualisasi yang memungkinkan inovasi bisnis yang efektif
- Memberikan layanan cloud dan virtualisasi untuk aplikasi critical ke kantor cabang
- Meluaskan cakupan layanan ke seluruh cabang, termasuk layanan keamanan, optimalisasi jaringan WAN, integrasi aplikasi dan penyatuan layanan komunikasi
- Memberikan harga kepemilikan (TCO) yang rendah

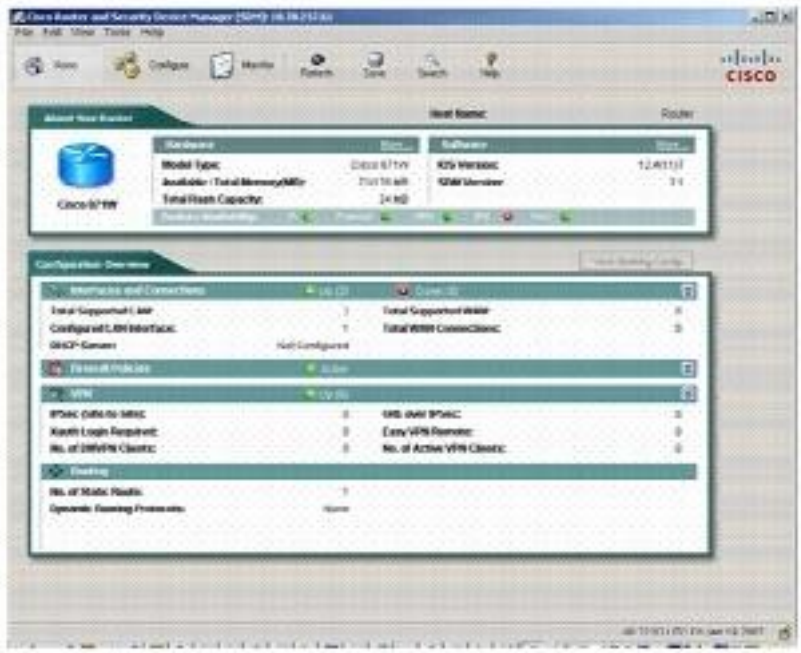
Gambar 1.2 ISR Cisco 819GW Dengan Kemampuan 3G Dan Wifi

SDM Express

SDM adalah singkatan dari Security Device Manager, yang dikeluarkan oleh Cisco sebagai manajemen perangkat berbasis web untuk menunjang penggunaan perangkat-perangkat routernya yang memiliki sistem operasi Cisco (Cisco IOS). Dengan SDM memudahkan pengguna untuk mengatur konfigurasi perangkat router dan keamanan dengan menggunakan smart-wizard yang menyediakan kemudahakan dalam membuat, menerapkan dan memantau perangkat router

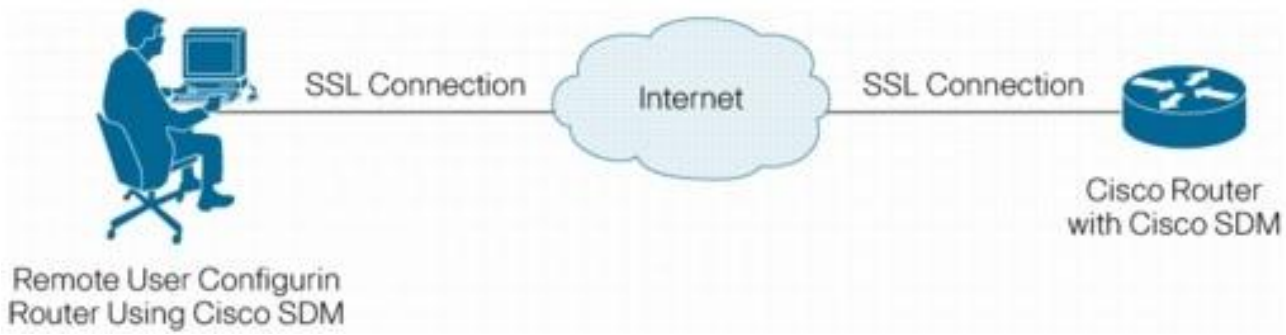
Cisco tanpa harus memiliki kemampuan untuk menggunakan perintah baris (Command Line Interface-CLI).

Dengan menggunakan SDM pengguna perangkat Cisco dapat dengan mudah mengkonfigurasi pengaturan routing, switching, keamanan, kualitas layanan (QoS), dan secara aktif dapat mengatur manajemen perangkat-perangkat melalui informasi monitoring yang tersedia. Pengguna SDM dapat mengatur perangkat router mereka dari jarak jauh tanpa harus menggunakan perangkat lunak perintah baris dari Cisco IOS. SDM juga dapat membantu para pengguna pemula dalam operasional harian, menyediakan smart-wizard yang mudah digunakan, pengaturan keamanan router secara otomatis dan membantu pengguna dengan berbagai bantuan online dan tutorial.



Gambar 1.3 Tampilan Awal Security Device Manager (SDM)

Panduan smart-wizard dari SDM akan membantu pengguna melalui serangkaian langkah-langkah alur kerja pengaturan router dan keamanan yang secara sistematis akan mengatur LAN, WLAN, dan WAN; firewall, sistem penangkal penyusupan (IPS) dan IP Security (IPSec) VPN. SDM ini juga secara otomatis dapat mendeteksi jika ada pengaturan yang tidak sesuai kemudian secara otomatis akan memperbaikinya agar supaya jaringan bisa berjalan dengan normal. Untuk pengguna yang sudah berpengalaman, maka SDM akan memungkinkan mereka untuk mengkonfigruasi pengaturan tingkat lanjut dan membolehkan mereka untuk mereview perintah-perintah yang dibuat oleh SDM sebelum diimplementasikan ke perangkat router. Selain itu SDM juga memungkinkan para administrator jaringan untuk mengkonfigurasi dan memonitor perangkat router di lokasi yang jauh melalui konekasi protokol SSL dan SSH. Teknologi ini memungkinkan koneksi yang aman melalui internet antara pengguna SDM dan perangkat routernya.



Gambar 1.4 Koneksi Aman Dengan Menggunakan SSL

Ketika melakukan instalasi perangkat router baru, pengguna dapat menggunakan SDM untuk mengkonfigurasi firewall secara cepat dan menerapkan rekomendasi terbaik berdasarkan International Computer Security Association (ICSA). Dengan menggunakan panduan yang ada pengguna dapat dengan mudah mengatur setelan firewall di bawah, menengah maupun tinggi. Pengguna SDM dapat pula mengatur setelan VPN yang aman dan secara otomatis melakukan audit keamanan.

Gambar 1.5 Audit Keamanan Dengan SDM

Konfigurasi Koneksi WAN Menggunakan SDM Express

Wide Area Network (WAN) adalah suatu jaringan yang digunakan untuk membuat interkoneksi antar jaringan komputer local yang secara fisik tidak berdekatan satu sama lain, yang secara fisik bisa dipisahkan dengan kota, propinsi, atau bahkan melintasi batas geography – lintas negara dan benua. Ada beberapa Teknologi Jaringan WAN saat ini yang bisa kita gunakan. Berbeda dengan jaringan LAN, ada perbedaan utama antara keduanya dimana terletak pada jarak yang memisahkan jaringan-2 yang terhubung tersebut. WAN menggunakan media transmisi yang berbeda, maupun hardware dan protocol yang berbeda pula dengan LAN. Data transfer rate dalam komunikasi WAN umumnya jauh lebih rendah dibanding LAN.

Fungsi Dan Tujuan Jaringan WAN

- Sharing resources

Kita dapat membagi sumber yang ada dalam arti dapat digunakan secara bersama-sama seperti program, peralatan, atau peripheral lainnya sehingga dapat dimanfaatkan setiap orang yang ada pada jaringan komputer tanpa harus terpengaruh oleh lokasi.

- Media komunikasi

Dapat memungkinkan terjadinya komunikasi antar pengguna jaringan, baik itu untuk teleconference, instant messaging, chatting, mengirim surat elektronik (e-mail) maupun mengirim informasi penting lainnya.

- Integrasi data

Dapat mencegah ketergantungan pada komputer pusat, setiap proses data tidak harus dilakukan pada satu komputer saja melainkan dapat didistribusikan ke tempat lainnya atau dengan kata lain dapat dikerjakan oleh komputer-komputer lain yang ada dalam jaringan.

- Keamanan data

Sistem jaringan komputer dapat memberikan perlindungan terhadap data melalui pengaturan hak akses pengguna dan password, serta teknik perlindungan yang lainnya.

- Web Browsing

Untuk mengakses informasi yang ada pada jaringan, contohnya web browsing. Hampir setiap orang yang membaca tulisan ini mungkin pernah menggunakan browser web (seperti Internet Explorer, Mozilla Firefox, Netscape, Opera dan yang lainnya). Browser web memungkinkan kita untuk melihat informasi yang ada di dalam sebuah web server di suatu tempat di dalam Internet.

- Mengkoneksikan device-device yang terpisahkan dalam area global,

- Menyajikan koneksifitas full-time/port-time,
- Beroperasi pada jangkauan geografis yang luas.

Kelebihan WAN :

- Bisa diakses dengan jangkauan area grografis yang luas sehingga berbisnis dengan jarak jauh dapat terhubung dengan jaringan ini
- Dapat berbagi (share) software dan resources dengan koneksi workstations.
- Pesan dapat dikirim dengan sangat cepat kepada orang lain pada jaringan ini (bisa berupa gambar, suara, atau data yang disertakan dengan suatu lampiran).
- Hal-hal yang mahal (seperti printer atau saluran telepon ke internet) dapat dibagi oleh semua komputer pada jaringan ini tanpa harus membeli perangkat yang berbeda untuk setiap komputernya.
- Semua orang yang ada di jaringan ini dapat menggunakan data yang sama. hal ini untuk menghindari masalah dimana beberapa pengguna mungkin memiliki informasi lebih tua daripada yang lain.
- Berbagi informasi/file (share) melalui area yang lebih besar
- Besar jaringan penutup.

Kekurangan WAN :

- Biaya operasional mahal dan umumnya lambat
- Memerlukan Firewall yang baik untuk membatasi pengguna luar yang masuk dan dapat mengganggu jaringan ini
- Menyiapkan jaringan bisa menjadi pengalaman yang sangat mahal dan rumit. Semakin besar jaringan semakin mahal harganya.
- Keamanan merupakan masalah yang paling nyata ketika orang yang berbeda memiliki kemampuan untuk menggunakan informasi dari komputer lain. Perlindungan terhadap hacker dan virus menambah kompleksitas lebih dan membutuhkan biaya.
- Setelah diatur, memelihara jaringan adalah pekerjaan penuh waktu (full time) yang membutuhkan jaringan pengawas dan teknisi untuk dipekerjakan.
- Informasi tidak dapat memenuhi kebutuhan lokal atau kepentingan.
- Rentan terhadap hacker atau ancaman dari luar lainnya.

Konfigurasi Layanan DHCP

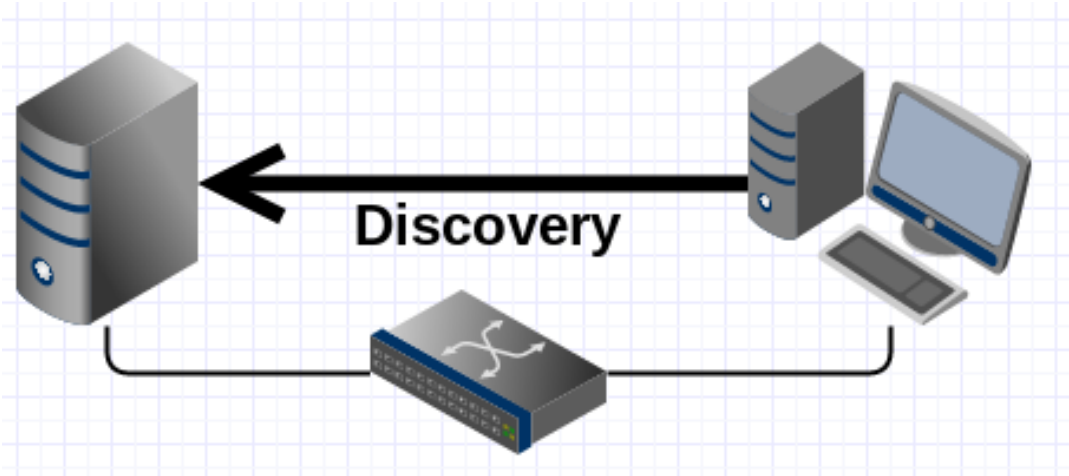
Dynamic Host Configuration Protocol atau sering disingkat dengan DHCP saja, adalah sebuah protokol yang melayani konfigurasi otomatis alamat IP, netmask, gateway, serta DNS. Proses koneksi ini terjalin dari 2 pihak yang terlibat serta bersifat connectionless. Sifat connectionless ini berarti saat akan menjalin koneksi tidak perlu ada konfirmasi terlebih dahulu (antara penerima dan pengirim paket) bahwa paket akan dikirim, atau paket telah diterima secara utuh. Karena komunikasi ini bersifat connectionless, maka protocol yang digunakan dalam layanan ini adalah protocol UDP (User Datagram Packet). Server akan membuka port 67 untuk menjalin komunikasi

dengan klien, sedangkan dari pihak klien akan membuka port 68 untuk berkomunikasi dengan server. Jika DHCP server dan klien berada pada subnet yang sama, maka koneksi terjalin menggunakan broadcast UDP, sedangkan apabila antara klien dan server DHCP berada pada subnet yang berbeda, maka layanan tersebut memerlukan DHCP relay agent untuk membangun koneksi.

Proses terjalinnya layanan DHCP ini terbagi menjadi 4 fase, yaitu:

- DHCP Discovery

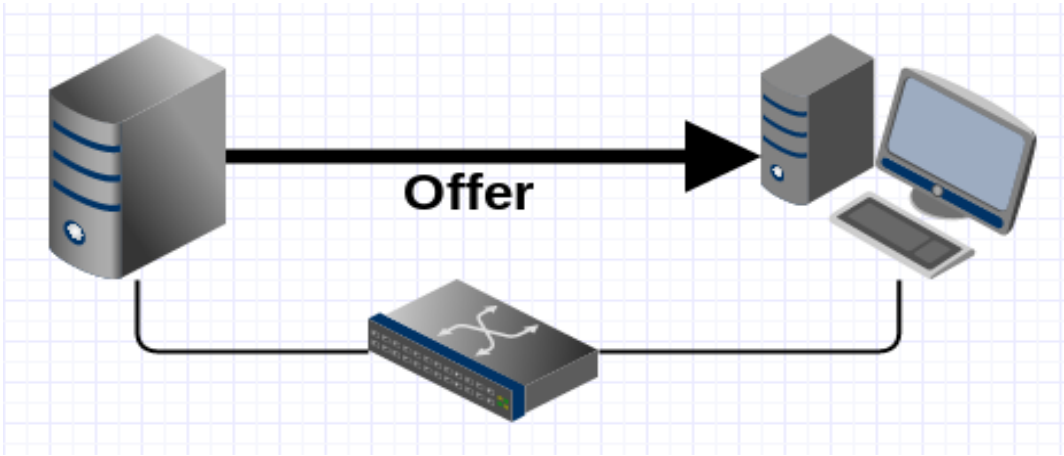
Adalah proses dimana komputer klien melakukan broadcast di sebuah network untuk mengetahui apakah terdapat layanan DHCP di dalam subnetnya. Komputer klien akan menyebarkan paket UDP dengan tujuan 255.255.255.255 atau ke alamat broadcast di dalam subnetnya. Komputer klien juga merequest IP yang sama (pernah dipakai), apabila sebelumnya pernah terlayani oleh server DHCP yang sama.



Gambar 1.6 Skema DHCP Recovery

- DHCP Lease Offer

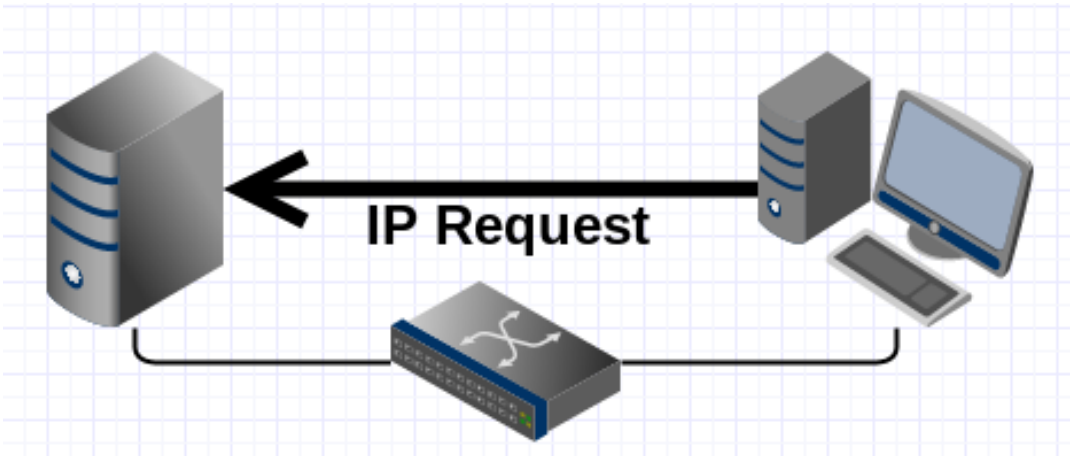
Adalah proses ketika DHCP server telah menerima request dari klien, membuat reservasi alamat IP kemudian menawarkan alamat yang telah dialokasikan kepada klien melalui paket DHCPOFFER melalui protocol UDP. Server DHCP menggunakan MAC Address dari kartu jaringan klien untuk membedakan request-request antar klien yang akan dilayaninya.



Gambar 1.7 Skema DHCP Offer

- DHCP Request

Adalah proses dimana klien telah menerima paket “tawaran” dari server DHCP dan meresponnya dengan melakukan requesting terhadap alamat IP yang telah di tawarkan oleh server DHCP dengan mengirimkan paket DHCPREQUEST kepada server. Klien dapat menerima beberapa tawaran sekaligus dari beberapa server DHCP, tetapi hanya tawaran yang berasal dari salah satu server yang akan diterima oleh klien. Melalui opsi identifikasi server, setiap server akan diberitahu oleh klien melalui paket ini (DHCPREQUEST) apabila ada klien yang telah memakai layanan DHCP, sehingga server DHCP yang menawarkan akan membatalkan tawaran mereka terhadap klien tersebut.

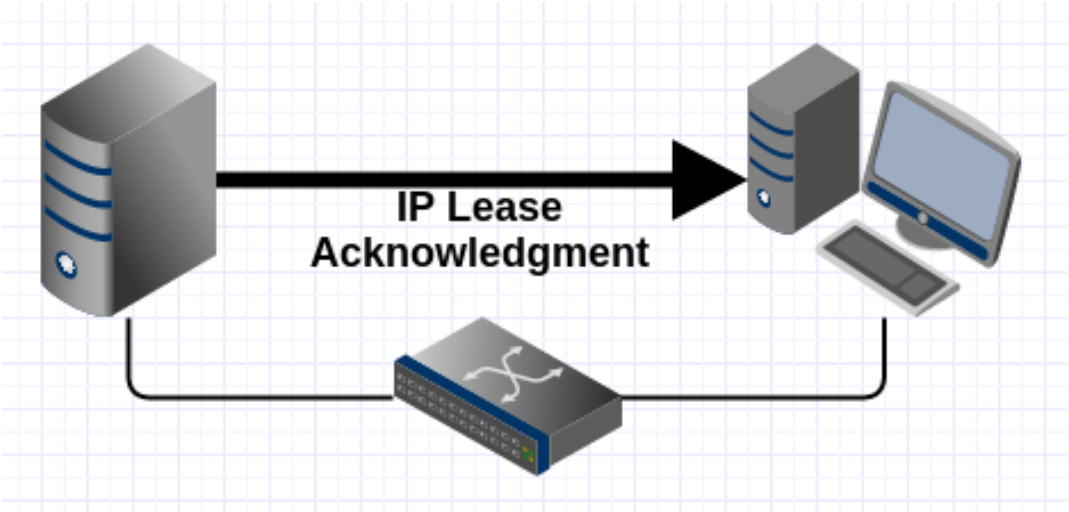


Gambar 1.8 Skema DHCP Request

- DHCP Lease Acknowledgement

Adalah proses final dari terjalinnya layanan DHCP ini, dimana server DHCP menerima paket DHCPREQUEST dari klien yang kemudian server DHCP akan mengirimkan paket DHCPACK kepada klien. Paket DHCPACK ini terdiri dari waktu atau durasi pelepasan IP yang dipakai, alamat IP

yang ditawarkan dan lain-lain. Pada poin ini, proses komunikasi antara klien dan server telah selesai dan klien akan melakukan konfigurasi secara otomatis dengan parameter-parameter (Alamat IP, Subnetmask, Alamat Gateway, Alamat DNS) yang telah di berikan oleh server DHCP.



Gambar 1.9 Skema DHCP Acknowledgment

Setelah konfigurasi selesai, maka klien menggunakan paket ARP untuk memberitahu server pemberi layanan, agar alamat IP yang telah digunakan tidak ditawarkan oleh klien lainnya. Ketika, waktu durasi pemakaian alamat IP yang diberikan oleh server DHCP habis, maka proses ini (4 fase) akan diulangi lagi oleh klien akan tetapi dengan merequest paket yang sama seperti yang telah di terima sebelumnya. Jika server DHCP adalah authoritative server, maka server DHCP akan menolak request tersebut dan menawarkan alamat IP yang baru terhadap klien. Klien akan mendapatkan alamat IP yang sama dengan sebelumnya ketika server DHCP adalah non authoritative server.

Back-up Konfigurasi Router

Membackup file konfigurasi ini sangat berguna selain untuk dokumentasi juga untuk backup kita saat melakukan konfigurasi ulang router kita jika kita kita ingin mencoba suatu konfigurasi yang baru, dan bila terjadi kegagalan dalam konfigurasi kita yang baru ini, kita dapat dengan cepat mengembalikannya ke konfigurasi semula dengan file backup konfigurasi kita tersebut.

Gambar 1.10 Skema Koneksi PC Backup Dengan Router Yang Akan Dibackup

a. Langkah-langkah melakukan backup file konfigurasi dari router ke PC adalah sebagai berikut ini :

- Masukkan perintah copy running-config tftp
- Masukkan IP address dari TFTP server
- Masukkan nama file konfigurasinya atau menerima nama defaultnya
- Tekan enter untuk konfirmasi dan menjalankan proses

Untuk lebih jelasnya konfigurasi pada terminal router sebagai berikut ini :

HDI>enable

HDI# HDI#copy running-config tftp

Address or name of remote host []? 172.18.18.254

Destination filename [HDI-confg]? HDI-Backup

!!

589 bytes copied in 10.7 secs

HDI#

b. Sedangkan untuk memanggil kembali file backup yang ada di PC TFTP Server untuk di kembalikan ke dalam router caranya adalah sebagai berikut ini :

- Masukkan perintah copy tftp running-config
- Pilih host atau network configuration file
- Masukkan IP address dari TFTP server
- Masukkan nama file konfigurasinya
- Tekan enter untuk konfirmasi dan menjalankan proses

Command Konfigurasi pada terminal router sebagai berikut ini :

HDI>enable

HDI# HDI#copy tftp running-config

Address or name of remote host []? 172.18.18.254

Source filename []? HDI-Backup

Destination filename [running-config]?

Accessing tftp://172.18.18.254/HDI-Backup

Loading HDI-Backup from 172.18.18.254

(via FastEthernet 0/1):

!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

(OK-589 bytes)

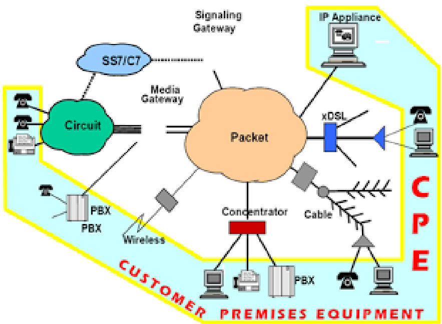
589 bytes copied in 10.2 secs

HDI#

Hubungan CPE Ke ISP

CPE (Customer Premises Equipment) adalah seluruh perangkat (terminal berikut infrastruktur jaringan pendukungnya) yang berada di tempat/lokasi pelanggan, yang digunakan dan dimiliki/dikuasai secara individu/privat serta menjadi tanggungjawab individu yang bersangkutan. Perkembangan perangkat CPE selain didrive oleh kebutuhan pasar juga sangat dipengaruhi perkembangan infrastruktur pendukungnya, yaitu teknologi jaringan transportasi (carrier grade) dan access network/gateway. Ketika ISDN belum dikenal, perangkat CPE hanya berupa pesawat telegrap (morse, telex, fax), setelah ISDN diimplementasikan, perangkat CPE dapat menggunakan PC, videophone, video conference, telemetri, dan lain-lain. Ketika teknologi gateway antara jaringan telekomunikasi dengan jaringan data dimungkinkan, muncul perangkat modem analog untuk akses internet dengan mode dial-up melalui Internet Service Provider (ISP). Ketika teknologi xDSL (khususnya ADSL) diimplementasikan muncul perangkat-perangkat CPE untuk akses internet non dialup.

Ketika teknologi memungkinkan informasi real time dapat dilewatkan jaringan paket dengan kualitas yang masih dalam batas-batas acceptable, muncul perangkat terminal H323. Ketika teknologi HFC diperkenalkan, muncul perangkat-perangkat CPE seperti Cable Modem, Set Top Box, perangkat Video on Demand (VoD) dan lain-lain. Demikian seterusnya dimana saat ini sedang berada pada masa transisi menuju NGN, bermunculan perangkat-perangkat CPE seperti IP Phone, terminal SIP, Soft Phone dan lain-lain.



Gambar 1.11 Perangkat CPE Dalam Suatu Jaringan

1.1.2.4 Mengasosiasi

Setelah mengikuti kegiatan belajar 1 ini siswa diharapkan dapat menyimpulkan pelbagai hasil percobaan dan pengamatan terkait dengan inisiasi konfigurasi router ISR, setup fisik pada ISR, konfigurasi SDM Express, konfigurasi koneksi WAN menggunakan SDM Express, konfigurasi NAT menggunakan SDM, konfigurasi router menggunakan CLI IOS, konfigurasi default route, konfigurasi layanan DHCP, konfigurasi NAT dengan CLI, back-up konfigurasi router, hubungan CPE ke ISP, dan konfigurasi koneksi WAN.

1.1.3 Rangkuman

Jaringan pada suatu perusahaan terdiri atas banyak perangkat keras maupun perangkat lunak. Tiap-tiap perangkat memiliki fungsi dan konfigurasi masing-masing untuk dapat digunakan dengan maksimal. Administrator jaringan harus memiliki pengetahuan dan pertimbahan yang baik dalam memilih perangkat yang sesuai dengan kebutuhan, serta pengetahuan yang memadai untuk dapat mengatur dan mengkonfigurasi perangkat-perangkat jaringan yang ada.

1.1.4 Tugas

Buatlah kelompok terdiri atas 2-3 orang. Masing-masing kelompok membuat ringkasan tentang konfigurasi peralatan-peralatan jaringan, kemudian secara bergantian masing-masing kelompok mempresentasikan hasilnya didepan kelas.

1. Bacalah uraian materi diatas dengan teliti dan cermat.
2. Buatlah ringkasan materi menggunakan aplikasi pengolah presentasi.
3. Presentasikan hasil ringkasan di depan kelas.

1.1.5 Penilaian Diri

Setelah mengikuti kegiatan belajar 1 ini diharapkan siswa memiliki wawasan pengetahuan dan dapat menjawab pelbagai hal terkait dengan inisiasi konfigurasi router ISR, setup fisik pada ISR, konfigurasi SDM Express, konfigurasi koneksi WAN menggunakan SDM Express, konfigurasi NAT menggunakan SDM, konfigurasi router menggunakan CLI IOS, konfigurasi default route, konfigurasi layanan DHCP, konfigurasi NAT dengan CLI, back-up konfigurasi router, hubungan CPE ke ISP, dan konfigurasi koneksi WAN.

BAB II

2.1 Kegiatan Belajar 2 : Routing Jaringan Komputer

2.1.1.Tujuan Pembelajaran

Setelah mengikuti kegiatan belajar 2 ini siswa diharapkan dapat memahami routing jaringan komputer.

2.1.2 Aktifitas Belajar Siswa

2.1.2.1 Mengamati

Selama mengikuti kegiatan belajar 2 ini siswa diharapkan dapat mengamati :

- Protocol routing interior umum
- Pengaturan routing dalam sebuah jaringan organisasi
- Konfigurasi dan verifikasi RIP
- Protocol routing eksterior
- Protocol routing eksterior yang ada pada ISP
- Konfigurasi dan verifikasi BGP

2.1.2.2 Menanya

Selama mengikuti kegiatan belajar 2 ini siswa diharapkan dapat :

- Mendiskusikan Protocol routing interior umum
- Mendiskusikan Pengaturan routing dalam sebuah jaringan organisasi
- Mendiskusikan Konfigurasi dan verifikasi RIP
- Mendiskusikan Protocol routing eksterior
- Mendiskusikan Protocol routing eksterior yang ada pada ISP
- Mendiskusikan Konfigurasi dan verifikasi BGP

2.1.2.3. Mengumpulkan Informasi

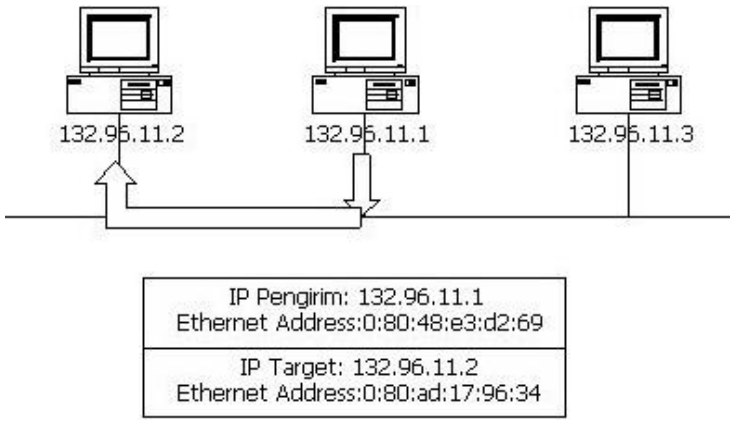
Protocol Routing Interior Umum

Routing adalah proses pengiriman data maupun informasi dengan meneruskan paket data yang dikirim dari jaringan satu ke jaringan lainnya. Interior Routing Protocol biasanya digunakan pada jaringan yang bernama Autonomous System, yaitu sebuah jaringan yang berada hanya dalam satu kendali teknik yang terdiri dari beberapa subnetwork dan gateway yang saling berhubungan satu sama lain.

Konsep Dasar Routing

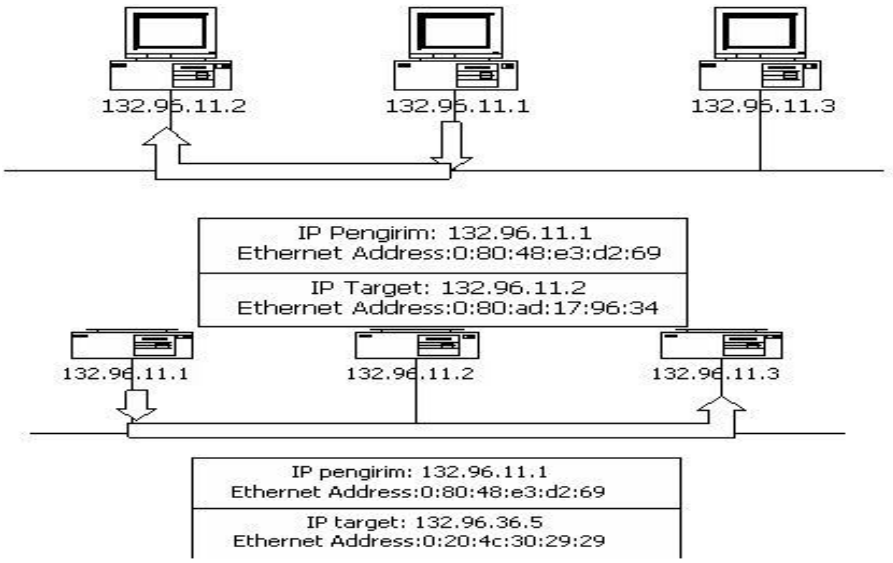
Bahwa dalam jaringan WAN kita sering mengenal yang namanya TCP/IP (Transmission Control Protocol/ Internet Protocol) sebagai alamat sehingga pengiriman paket data dapat sampai ke alamat yang dituju (host tujuan). TCP/IP membagi tugas masing-masingmulai dari penerimaan paket data sampai pengiriman paket data dalam sistem sehingga jika terjadi permasalahan dalam pengiriman paket data dapat dipecahkan dengan baik.

Berdasarkan pengiriman paket data routing dibedakan menjadi routing langsung dan routing tidak langsung. Routing langsung merupakan sebuah pengalamatan secara langsung menuju alamat tujuan tanpa melalui host lain. Contoh: sebuah komputer dengan alamat 192.168.1.2 mengirimkan data ke komputer dengan alamat 192.168.1.3



Gambar 2.1 Routing Langsung

Routing tidak langsung merupakan sebuah pengalamatan yang harus melalui alamat host lain sebelum menuju alamat hort tujuan. (contoh: komputer dengan alamat 192.168.1.2 mengirim data ke komputer dengan alamat 192.1681.3, akan tetapi sebelum menuju ke komputer dengan alamat 192.168.1.3, data dikirim terlebih dahulu melalui host dengan alamat 192.168.1.5 kemudian dilanjutkan ke alamat host tujuan.



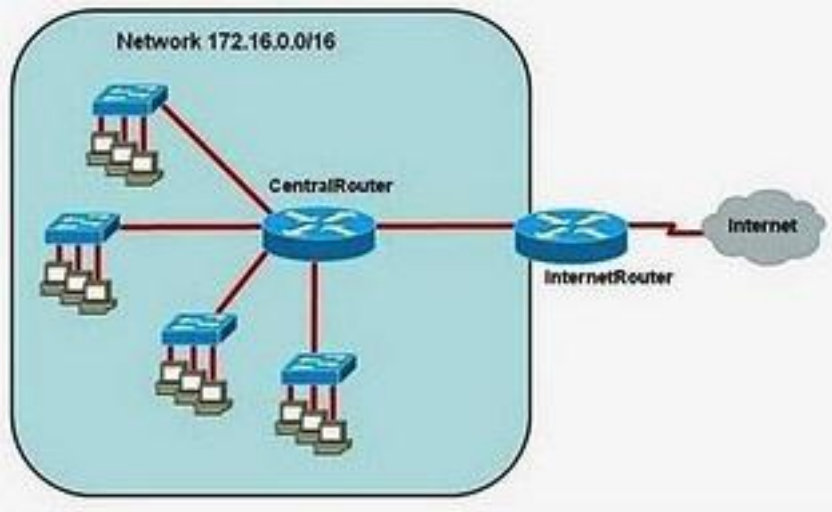
Gambar 2.2 Routing Tidak Langsung

Jenis Konfigurasi Routing

- Minimal Routing

  Dari namanya dapat diketahui bahwa ini adalah konfigurasi yang paling sederhana tapi mutlak diperlukan. Biasanya minimal routing dipasang pada network yang terisolasi

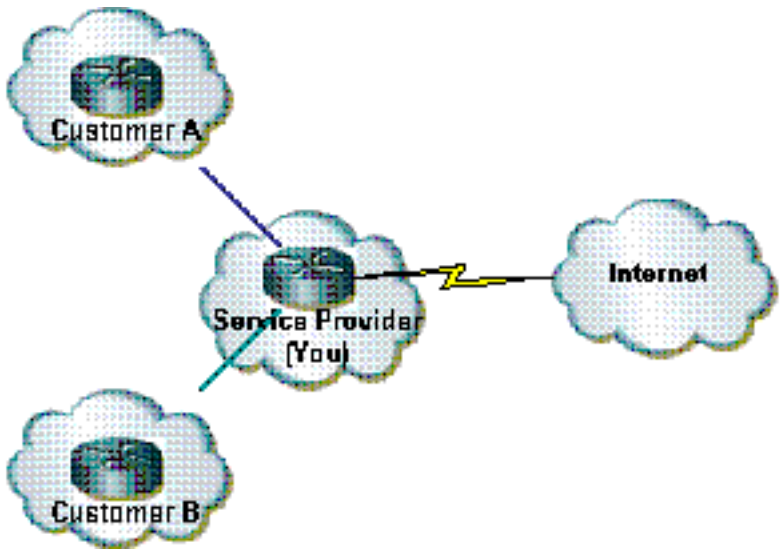
dari network lain atau dengan kata lain hanya pemakaian lokal saja.



Gambar 2.3 Minimal Routing

- Static Routing

  Dibangun pada jaringan yang memiliki banyak gateway. Jenis ini hanya memungkinkan untuk jaringan kecil dan stabil. Router meneruskan paket dari sebuah network ke network yang lainnya berdasarkan rute (catatan: seperti rute pada bis kota) yang ditentukan oleh administrator. Rute pada static routing tidak berubah, kecuali jika diubah secara manual oleh administrator.



Gambar 2.4 Static Routing

Kekurangan static routing adalah :

– Dengan menggunakan next hop, static routing yang menggunakan next hop akan mengalami multiple lookup atau lookup yg

berulang. lookup yg pertama yang akan dilakukan adalah mencari network tujuan, setelah itu akan kembali melakukan proses lookup untuk mencari interface mana yang digunakan untuk menjangkau next hopnya.

– Dengan menggunakan exit interface, kemungkinan akan terjadi eror ketika meneruskan paket. Jika link router terhubung dengan banyak router, maka router tidak bisa memutuskan router mana tujuanya karena tidak adanya next hop pada tabel routing, karena itulah, akan terjadi eror.

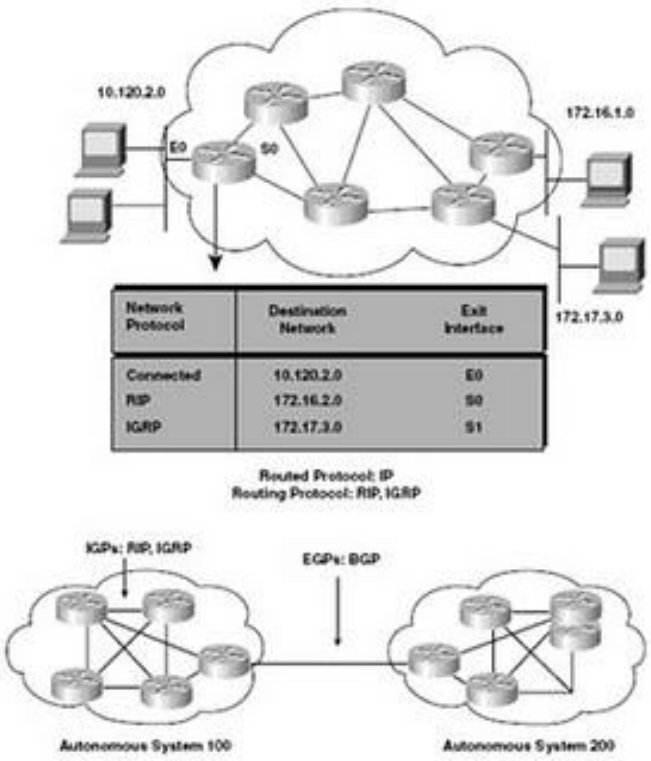
Kelebihan static routing adalah :

– Dapat mencegah trjadinya eror dalam meneruskan paket ke router tujuan apabila router yang akan meneruskan paket memiliki link yang terhubung dengan banyak router.itu disebabkan karena router telah mengetahui next hop, yaitu IP address router tujuan
– Proses lookup hanya akan terjadi satu kali saja (single lookup) karena router akan langsung meneruskan paket ke network tujuan melalui interface yang sesuai pada routing table
– Routing static dengan menggunakan next hop cocok digunakan untuk jaringan multi-access network atau point to multipoint sedangkan untuk jaringan point to point, cocok dengan menggunakan exit interface dalam mengkonfigurasi static route.

• Dynamic Routing

Biasanya digunakan pada jaringan yang memiliki lebih dari satu rute. Dinamic routing memerlukan routing protocol untuk membuat tabel routing yang dapat memakan resource komputer. Dynamic router mempelajari sendiri Rute yang terbaik yang akan ditempuhnya untuk meneruskan paket dari sebuah network ke network lainnya. Administrator tidak menentukan rute yang harus ditempuh oleh paket-paket tersebut. Administrator hanya menentukan bagaimana cara router mempelajari paket, dan kemudian router mempelajarinya sendiri. Rute pada dynamic routing berubah, sesuai dengan pelajaran yang didapatkan oleh router. Apabila jaringan memiliki lebih dari satu kemungkinan rute untuk tujuan yang sama maka perlu digunakan dynamic routing. Sebuah dynamic routing dibangun berdasarkan informasi yang dikumpulkan oleh protokol routing. Protokol ini didesain untuk mendistribusikan informasi yang secara dinamis mengikuti perubahan kondisi jaringan. Protokol routing mengatasi situasi routing yang kompleks secara cepat dan akurat. Protokol routng didesain tidak hanya untuk mengubah ke rute backup bila rute utama tidak berhasil, namun juga didesain untuk menentukan rute mana yang terbaik untuk mencapai tujuan tersebut.

Pengisian dan pemeliharaan tabel routing tidak dilakukan secara manual oleh admin. Router saling bertukar informasi routing agar dapat mengetahui alamat tujuan dan menerima tabel routing. Pemeliharaan jalur dilakukan berdasarkan pada jarak terpendek antara device pengirim dan device tujuan.

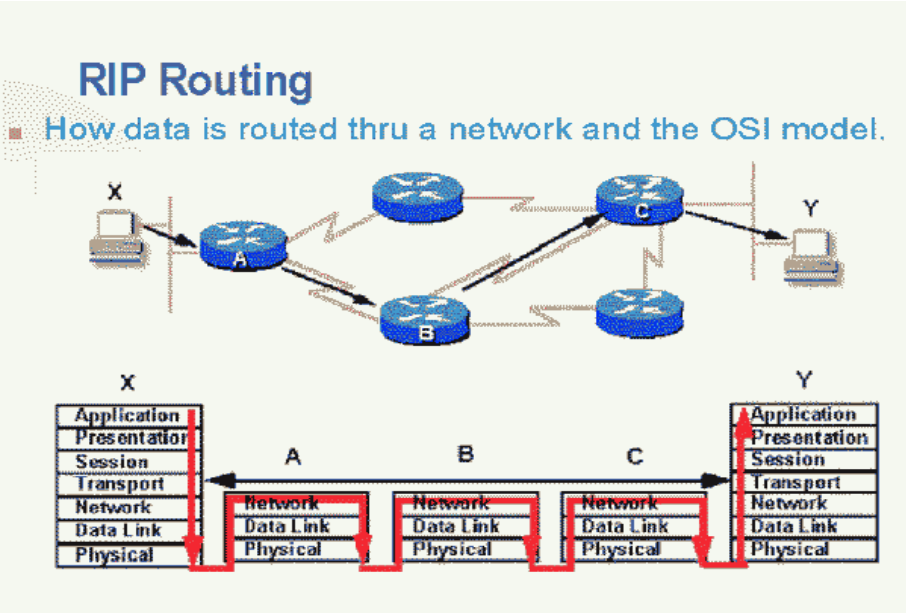


Gambar 2.5 Dynamic Routing

Macam-macam Routing Dynamic :

- RIP (Routing Information Protocol)

  Routing Information Protocol (RIP) adalah sebuah protokol routing dinamis yang digunakan dalam jaringan LAN (Local Area Network) dan WAN (Wide Area Network). Oleh karena itu protokol ini diklasifikasikan sebagai Interior Gateway Protocol (IGP). Protokol ini menggunakan algoritma Distance-Vector Routing. Pertama kali didefinisikan dalam RFC 1058 (1988). Protokol ini telah dikembangkan beberapa kali, sehingga terciptalah RIP Versi 2 (RFC 2453). Kedua versi ini masih digunakan sampai sekarang, meskipun begitu secara teknis mereka telah dianggap usang oleh teknik-teknik yang lebih maju, seperti Open Shortest Path First (OSPF) dan protokol OSI IS-IS. RIP juga telah diadaptasi untuk digunakan dalam jaringan IPv6, yang dikenal sebagai standar RIPng (RIP Next Generation / RIP generasi berikutnya), yang diterbitkan dalam RFC 2080 (1997).



Gambar 2.6 RIP Routing

Algoritma routing yang digunakan dalam RIP, algoritma Bellman-Ford, pertama kali digunakan dalam jaringan komputer pada tahun 1968, sebagai awal dari algoritma routing ARPANET. Versi paling awal protokol khusus yang menjadi RIP adalah Gateway Information Protocol, sebagai bagian dari PARC Universal Packet internetworking protocol suite, yang dikembangkan di Xerox Parc. Sebuah versi yang bernama Routing Information Protocol, adalah bagian dari Xerox Network Services. Sebuah versi dari RIP yang mendukung Internet Protocol (IP) kemudian dimasukkan dalam Berkeley Software Distribution (BSD) dari sistem operasi Unix. Ini dikenal sebagai daemon routed. Berbagai vendor lainnya membuat protokol routing yang diimplementasikan sendiri. Akhirnya, RFC 1058 menyatukan berbagai implementasi di bawah satu standar.

RIP adalah routing vektor jarak-protokol, yang mempekerjakan hop sebagai metrik routing. Palka down time adalah 180 detik. RIP mencegah routing loop dengan menerapkan batasan pada jumlah hop diperbolehkan dalam path dari sumber ke tempat tujuan. Jumlah maksimum hop diperbolehkan untuk RIP adalah 15. Batas hop ini, bagaimanapun, juga membatasi ukuran jaringan yang dapat mendukung RIP. Sebuah hop 16 adalah dianggap jarak yang tak terbatas dan digunakan untuk mencela tidak dapat diakses, bisa dioperasi, atau rute yang tidak diinginkan dalam proses seleksi.

Awalnya setiap router RIP mentransmisikan / menyebarkan pembaruan(update) penuh setiap 30 detik. Pada awal penyebaran, tabel routing cukup kecil bahwa lalu lintas tidak signifikan. Seperti jaringan tumbuh dalam ukuran, bagaimanapun, itu menjadi nyata mungkin ada lalu lintas besar-besaran meledak setiap 30 detik, bahkan jika router sudah diinisialisasi secara acak kali. Diperkirakan, sebagai akibat dari inisialisasi acak, routing

update akan menyebar dalam waktu, tetapi ini tidak benar dalam praktiknya. Sally Floyd dan Van Jacobson menunjukkan pada tahun 1994 bahwa, tanpa sedikit pengacakan dari update timer, penghitung waktu disinkronkan sepanjang waktu dan mengirimkan update pada waktu yang sama. Implementasi RIP modern disengaja memperkenalkan variasi ke update timer interval dari setiap router. RIP mengimplementasikan split horizon, rute holddown keracunan dan mekanisme untuk mencegah informasi routing yang tidak benar dari yang disebarkan. Ini adalah beberapa fitur stabilitas RIP.

Dalam kebanyakan lingkungan jaringan saat ini, RIP bukanlah pilihan yang lebih disukai untuk routing sebagai waktu untuk menyatu dan skalabilitas miskin dibandingkan dengan EIGRP, OSPF, atau IS-IS (dua terakhir yang link-state routing protocol), dan batas hop parah membatasi ukuran jaringan itu dapat digunakan. Namun, mudah untuk mengkonfigurasi, karena RIP tidak memerlukan parameter pada sebuah router dalam protokol lain oposisi. RIP dilaksanakan di atas User Datagram Protocol sebagai protokol transport. Ini adalah menugaskan dilindungi undang-undang nomor port 520.

Ada tiga versi dari Routing Information Protocol: RIPv1, RIPv2, dan RIPng.

1. RIP versi 1

   Spesifikasi asli RIP, didefinisikan dalam RFC 1058, classful menggunakan routing. Update routing periodik tidak membawa informasi subnet, kurang dukungan untuk Variable Length Subnet Mask (VLSM). Keterbatasan ini tidak memungkinkan untuk memiliki subnet berukuran berbeda dalam kelas jaringan yang sama. Dengan kata lain, semua subnet dalam kelas jaringan harus memiliki ukuran yang sama. Juga tidak ada dukungan untuk router otentikasi, membuat RIP rentan terhadap berbagai serangan.

2. RIP versi 2

   Karena kekurangan RIP asli spesifikasi, RIP versi 2 (RIPv2) dikembangkan pada tahun 1993 dan standar terakhir pada tahun 1998. Ini termasuk kemampuan untuk membawa informasi subnet, sehingga mendukung Classless Inter-Domain Routing (CIDR). Untuk menjaga kompatibilitas, maka batas hop dari 15 tetap. RIPv2 memiliki fasilitas untuk sepenuhnya beroperasi dengan spesifikasi awal jika semua protokol Harus Nol bidang dalam pesan RIPv1 benar ditentukan. Selain itu, aktifkan kompatibilitas fitur memungkinkan interoperabilitas halus penyesuaian. Dalam upaya untuk menghindari beban yang tidak perlu host yang tidak berpartisipasi dalam routing, RIPv2 me-multicast seluruh tabel routing ke semua router yang berdekatan di alamat 224.0.0.9, sebagai lawan dari RIP yang menggunakan siaran unicast. Alamat 224.0.0.9 ini berada pada alamat IP versi 4 kelas D (range 224.0.0.0 - 239.255.255.255). Pengalamatan unicast masih diperbolehkan untuk aplikasi khusus. (MD5) otentikasi RIP diperkenalkan pada tahun 1997. RIPv2 adalah Standar Internet STD-56.

3. RIPng

RIPng (RIP Next Generation / RIP generasi berikutnya), yang didefinisikan dalam RFC 2080, adalah perluasan dari RIPv2 untuk mendukung IPv6, generasi Internet Protocol berikutnya. Perbedaan utama antara RIPv2 dan RIPng adalah:

- Dukungan dari jaringan IPv6
- RIPv2 mendukung otentikasi RIPv1, sedangkan RIPng tidak. IPv6 router pada saat itu, seharusnya menggunakan IP Security (IPsec) untuk otentikasi
- RIPv2 memungkinkan pemberian beragam tag untuk rute , sedangkan RIPng tidak
- RIPv2 meng-encode hop berikutnya (next-hop) ke setiap entry route, RIPng membutuhkan penyandian (encoding) tertentu dari hop berikutnya untuk satu set entry route .
- Hop count tidak dapat melebihi 15, dalam kasus jika melebihi akan dianggap tidak sah. Hop tak hingga direpresentasikan dengan angka 16.
- Sebagian besar jaringan RIP datar. Tidak ada konsep wilayah atau batas-batas dalam jaringan RIP.
- Variabel Length Subnet Masks tidak didukung oleh RIP IPv4 versi 1 (RIPv1).
- RIP memiliki konvergensi lambat dan menghitung sampai tak terhingga masalah.

• IGRP (Interior Gateway Routing Protocol)

Pengertian IGRP (Interior Gateway Routing Protocol) adalah protocol distance vector yang diciptakan oleh perusahaan Cisco untuk mengatasi kekurangan RIP. Jumlah hop maksimum menjadi 255 dan sebagai metric, IGRP menggunakan Bandwidth, MTU, Delay Dan Load. IGRP adalah protocol routing yang menggunakan Autonomous System (AS) yang dapat menentukan routing berdasarkan system, interior atau exterior. Administrative distance untuk IGRP adalah 100.

IGRP merupakan suatu penjaluran jarak antara vektor protokol, bahwa masing-masing penjaluran bertugas untuk mengirimkan semua atau sebagian dari isi table penjaluran dalam penjaluran pesan untuk memperbaharui pada waktu tertentu untuk masing-masing penjaluran. Penjaluran memilih alur yang terbaik antara sumber dan tujuan. Untuk menyediakan fleksibilitas tambahan, IGRP mengijinkan untuk melakukan penjaluran multipath. Bentuk garis equal bandwidth dapat menjalankan arus lalu lintas dalam round robin, dengan melakukan peralihan secara otomatis kepada garis kedua jika sampai garis kesatu turun. Isi dari informasi routing adalah:

- Identifikasi tujuan baru
- Mempelajari apabila terjadi kegagalan

IGRP mengirimkan update routing setiap interval 90 detik. Update ini advertise semua jaringan dalam AS. Kunci desain jaringan IGRP adalah:

- Secara otomatis dapat menangani topologi yang komplek
- Kemampuan ke segmen dengan bandwidth dan delay yang berbeda
- Skalabilitas, untuk fungsi jaringan yang besar

Secara default, IGRP menggunakan bandwidth dan delay sebagai metric. Untuk konfigurasi tambahan, IGRP dapat dikonfigurasi menggunakan kombinasi semua varibel atau yang disebut dengan Composite Metric. Variabel-variabel itu misalnya: bandwidth, delay, load, reliability.

Operasi IGRP

Masing-masing penjaluran secara rutin mengirimkan masing-masing jaringan lokal kepada suatu pesan yang berisi salinan tabel penjaluran dari tabel lainnya. Pesan ini berisi tentang biaya-biaya dan jaringan yang akan dicapai untuk menjangkau masing-masing jaringan tersebut. Penerima pesan penjaluran dapat menjangkau semua jaringan didalam pesan sepanjang penjaluran yang bisa digunakan untuk mengirimkan pesan.

Tujuan dari IGRP adalah :

– Penjaluran stabil dijaringan kompleks sangat besar dan tidaka ada pengulangan penjaluran.
– Overhead rendah, IGRP sendiri tidak menggunakan bandwidth yang diperlukan untuk tugasnya.
– Pemisahan lalu lintas antar beberapa rute paralel.
– Kemampuan untuk menangani berbagai jenis layanan dengan informasi tunggal.
– Mempertimbangkan menghitung laju kesalahan dan tingkat lalu lintas pada alur yang berbeda.
– Penjaluran stabil dijaringan kompleks sangat besar dan tidaka ada pengulangan penjaluran
– Overhead rendah, IGRP sendiri tidak menggunakan bandwidth yang diperlukan untuk tugasnya

Kemudian setelah melalui proses pembaharuan IGRP kemudian menjadi EIGRP (Enhanced IGRP), persamaannya adalah IGRP dan EIGRP sama-sama kompatibel dan antara router-router yang menjalankan EIGRP dan IGRP dengan autonomous system yang sama akan langsung otomatis terdistribusi. Selain itu EIGRP juga akan memberikan tagging external route untuk setiap route yang berasal dari:

– Routing protocol non EIGRP.
– Routing protocol IGRP dengan AS number yang sama.

- OSPF (Open Shortest Path First)

Teknologi link-state dikembangkan dalam ARPAnet untuk menghasilkan protokol yang terdistribusi yang jauh lebih baik daripada protokol distance-vector. Alih-alih saling bertukar jarak (distance) ke tujuan, setiap router dalam jaringan memiliki peta jaringan yang dapat diperbarui dengan cepat setelah setiap perubahan topologi. Peta ini digunakan untuk menghitung route yang lebih akurat daripada menggunakan protokol distance-vector. Perkembangan teknologi ini akhirnya menghasilkan protokol Open Shortest Path First (OSPF) yang dikembangkan oleh IETF (Internet Engineering Task Force) untuk digunakan di Internet.

Prinsip link-state routing sangat sederhana. Sebagai pengganti menghitung route “terbaik” dengan cara terdistribusi, semua router mempunyai peta jaringan dan menghitung semua route yang terbaik dari peta ini. Peta jaringan tersebut disimpan dalam sebuah basis data dan setiap record dalam basis data tersebut menyatakan sebuah link dalam jaringan. Record-record tersebut dikirimkan oleh router yang terhubung langsung dengan masing-masing link. Karena setiap router perlu memiliki peta jaringan yang menggambarkan kondisi terakhir topologi jaringan yang lengkap, setiap perubahan dalam jaringan harus diikuti oleh perubahan dalam basis data link-state yang terletak di setiap router. Perubahan status link yang dideteksi router akan mengubah basis data link-state router tersebut, kemudian router mengirimkan perubahan tersebut ke router-router lain.

Protokol yang digunakan untuk mengirimkan perubahan ini harus cepat dan dapat diandalkan. Ini dapat dicapai oleh protokol flooding. Dalam protokol flooding, pesan yang dikirim adalah perubahan dari basis data serta nomor urut pesan tersebut. Dengan hanya mengirimkan perubahan basis data, waktu yang diperlukan untuk pengiriman dan pemrosesan pesan tersebut lebih sedikit dibandingdengan mengirim seluruh isi basis data tersebut. Nomor urut pesan diperlukan untuk mengetahui apakah pesan yang diterima lebih baru daripada yang terdapat dalam basis data. Nomor urut ini berguna pada kasus link yang putus menjadi tersambung kembali.

Pada saat terdapat link putus dan jaringan menjadi terpisah, basis data kedua bagian jaringan tersebut menjadi berbeda. Ketika link yang putus tersebut hidup kembali, basis data di semua router harus disamakan. Basis data ini tidak akan kembali sama dengan mengirimkan satu pesan link-state saja. Proses penyamaan basis data pada router yang bertetangga disebut sebagai menghidupkan adjacency. Dua buah router bertetangga disebut sebagai adjacent bila basis data link-state keduanya telah sama. Dalam proses ini kedua router tersebut tidak saling bertukar basis data karena akan membutuhkan waktu yang lama.

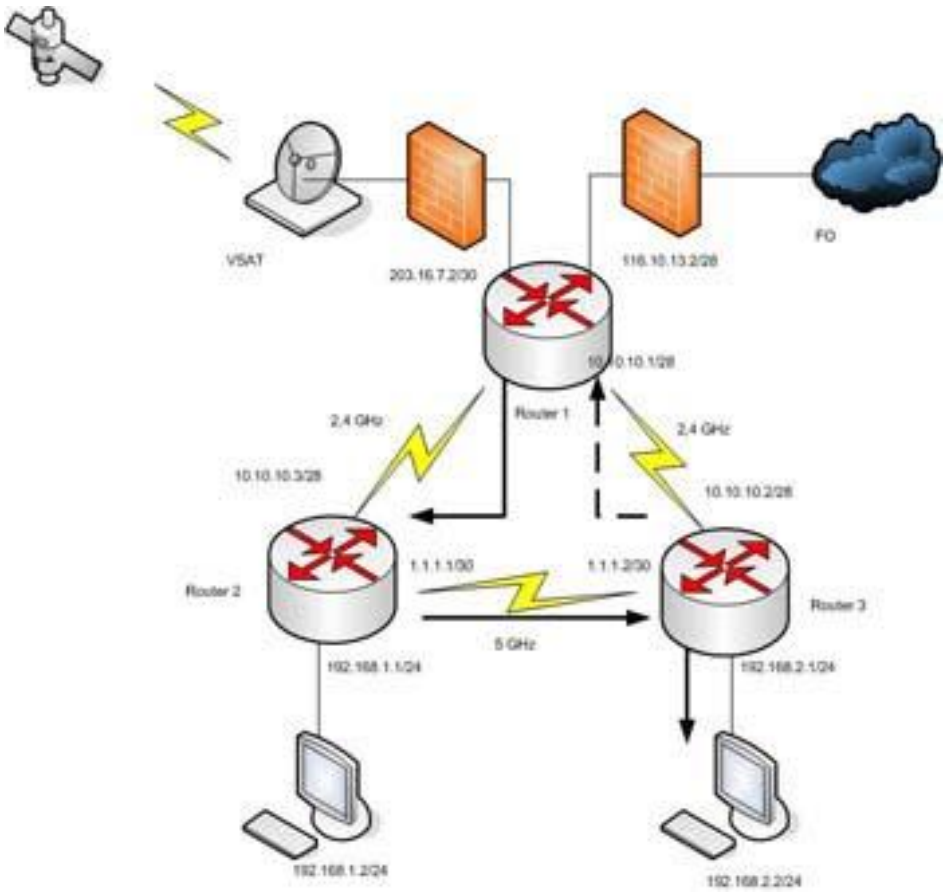
Proses menghidupkan adjacency terdiri dari dua fasa. Fasa pertama, kedua router saling bertukar deskripsi basis data yang merupakan ringkasan dari basis data yang dimiliki setiap router. Setiap router kemudian membandingkan deskripsi basis data yang diterima dengan basis data yang dimilikinya. Pada fasa kedua, setiap router meminta tetangganya untuk mengirimkan record-record basis data yang berbeda, yaitu bila router tidak memiliki record tersebut, atau nomor urut record yang dimiliki lebih kecil daripada yang dikirimkan oleh deskripsi basis data. Setelah proses ini, router memperbarui beberapa record dan ini kemudian dikirimkan ke router-router lain melalui protokol flooding.

Protokol link-state lebih baik daripada protokol distance-vector disebabkan oleh beberapa hal: waktu yang diperlukan untuk konvergen lebih cepat, dan lebih penting lagi protokol ini tidak menghasilkan routing loop. Protokol ini mendukung penggunaan

beberapa metrik sekaligus. Throughput, delay, biaya, dan keandalan adalah metrik-metrik yang umum digunakan dalam jaringan. Di samping itu protokol ini juga dapat menghasilkan banyak jalur ke sebuah tujuan. Misalkan router A memiliki dua buah jalur dengan metrik yang sama ke host B. Protokol dapat memasukkan kedua jalur tersebut ke dalam forwarding table sehingga router mampu membagi beban di antara kedua jalur tersebut. Rancangan OSPF menggunakan protokol link-state dengan beberapa penambahan fungsi. Fungsi-fungsi yang ditambahkan antara lain mendukung jaringan multi-akses, seperti X.25 dan Ethernet, dan membagi jaringan yang besar mejadi beberapa area.

Telah dijelaskan di atas bahwa setiap router dalam protokol link-state perlu membentuk adjacency dengan router tetangganya. Pada jaringan multi-akses, tetangga setiap router dapat lebih dari satu. Dalam situasi seperti ini, setiap router dalam jaringan perlu membentuk adjacency dengan semua router yang lain, dan ini tidak efisien. OSPF mengefisienkan adjacency ini dengan memperkenalkan konsep designated router dan designated router cadangan. Semua router hanya perlu adjacent dengan designated router tersebut, sehingga hanya designated router yang adjacent dengan semua router yang lain. Designated router cadangan akan mengambil alih fungsi designated router yang gagal berfungsi.

Langkah pertama dalam jaringan multi-akses adalah memilih designated router dan cadangannya. Pemilihan ini dimasukkan ke dalam protokol Hello, protokol dalam OSPF untuk mengetahui tetangga-tetangga router dalam setiap link. Setelah pemilihan, baru kemudian router-router membentuk adjacency dengan designated router dan cadangannya. Setiap terjadi perubahan jaringan, router mengirimkan pesan menggunakan protokol flooding ke designated router, dan designated router yang mengirimkan pesan tersebut ke router-router lain dalam link. Dalam jaringan yang besar tentu dibutuhkan basis data yang besar pula untuk menyimpan topologi jaringan. Ini mengarah kepada kebutuhan memori router yang lebih besar serta waktu perhitungan route yang lebih lama. Untuk mengantisipasi hal ini, OSPF menggunakan konsep area dan backbone. Jaringan dibagi menjadi beberapa area yang terhubung ke backbone. Setiap area dianggap sebagai jaringan tersendiri dan router-router di dalamnya hanya perlu memiliki peta topologi jaringan dalam area tersebut. Router-router yang terletak di perbatasan antar area hanya mengirimkan ringkasan dari link-link yang terdapat dalam area dan tidak mengirimkan topologi area satu ke area lain. Dengan demikian, perhitungan route menjadi lebih sederhana.



Gambar 2.7 Open Shortest Path First Routing

Kesederhanaan vs. Kemampuan

Kita sudah lihat sepintas bagaimana RIP dan OSPF bekerja. Setiap protokol routing memiliki kelebihan dan kekurangannya masing-masing. Protokol RIP sangat sederhana dan mudah diimplementasikan tetapi dapat menimbulkan routing loop. Protokol OSPF merupakan protokol yang lebih rumit dan lebih baik daripada RIP tetapi membutuhkan memori dan waktu CPU yang besar.

Di berbagai tempat juga terdapat yang menggunakan gabungan antara routing statik, RIP, RIP-v2, dan OSPF. Hasilnya di jaringan ini menunjukkan bahwa administrasi routing statik jauh lebih memakan waktu dibanding routing dinamik. Pengamatan pada protokol routing dinamik juga menunjukkan bahwa RIP menggunakan bandwidth yang lebih besar daripada OSPF dan semakin besar jaringan, bandwidth yang digunakan RIP bertambah lebih besar pula.

Tahapan dalam membentuk adjacency

Pada saat baru pertama ON, router OSPF tidak tahu apapun tentang tetangganya, router akan mulai mengirimkan paket Hello ke seluruh interface jaringan untuk memperkenalkan dirinya. Jika router yang baru ON ini menerima paket hello yang menyimpan informasi tentang dirinya maka router ini dapat saling berhubungan dua arah dengan router pengirim hello, Default nilai hello pada broadcast multi-access adalah 10 detik dan 40 detik jika tidak ada respon akan

mati, dan pada NBMA hello 30 detik dan akan mati pada 120 detik jika tidak terdapat respon.

- Down : router tidak dapat hello packet dari router manapun
- Attempt : router mengirimkan hello packet tetapi belum mendapat respon, hanya ada pada tipe NT non broadcast multi-access (NBMA) dan tidak ada respon dari router lain.
- Init : router mendapatkan hello packet dari router lain, tetapi belum terbentuk hubungan yang bidirectional (2 way)
- 2 way : pada tahap ini hubungan antar router sudah bi-directional, untuk NT broadcast DR & BDR nya akan melanjutkan ke tahap full, router non DR & BDR akan melanjutkan Full hanya dengan DR & BDR saja
- Exstart : terjadi pemilihan Master dan Slave, master adalah router yang memiliki router id tertinggi
- exchange : terjadi pertukaran Database Descriptor (DBD) paket DBD ini digambarkan dari topologi DB router, proses dimulai oleh master
- Loading : router akan memeriksa DBD dari router lain dan apabila ada entry yang tidak diketahui maka router akan mengira link state request (LSR) , LSR akan dibales dengan link state state ACK dan link state reply, diakhir tahap ini semua router yang di adjacent memiliki topologi DB yang sama
- Full : masing-masing router sudah membentuk hubungan yang adjancent.

OSPF Routing Protocol Untuk Jaringan Lokal

Kekuatan dari OSPF ada pada sistem hirarkinya yang diterapkan dalam sistem area. Penyebaran informasi routing menjadi lebih teratur dan juga mudah untuk di-troubleshooting.

Langkah pertama yang harus dilakukan oleh OSPF adalah membentuk komunikasi dengan para router tetangganya. Tujuannya adalah agar informasi apa yang belum diketahui oleh router tersebut dapat diberi tahu oleh router tetangganya. Begitu pula router tetangga tersebut juga akan menerima informasi dari router lain yang bertindak sebagai tetangganya. Sehingga pada akhirnya seluruh informasi yang ada dalam sebuah jaringan dapat diketahui oleh semua router yang ada dalam jaringan tersebut. Kejadian ini sering disebut dengan istilah Convergence.

Setelah router membentuk komunikasi dengan para tetangganya, maka proses pertukaran informasi routing berlangsung dengan menggunakan bantuan beberapa paket khusus yang bertugas membawa informasi routing tersebut. Paket-paket tersebut sering disebut dengan istilah Link State Advertisement packet (LSA packet). Selain dari hello packet, routing protokol OSPF juga sangat bergantung kepada paket jenis ini untuk dapat bekerja.

OSPF memang memiliki sistem update informasi routing yang cukup teratur dengan rapi. Teknologinya menentukan jalur terpendek dengan algoritma Shortest Path First (SPF) juga sangat hebat. Meskipun terbentang banyak jalan menuju ke sebuah lokasi, namun OSPF dapat menentukan jalan mana yang paling baik dengan sangat tepat.

Sehingga komunikasi data Anda menjadi lancar dan efisien. Namun ada satu lagi keunggulan OSPF, yaitu konsep jaringan hirarki yang membuat proses update informasinya lebih termanajemen dengan baik. Dalam menerapkan konsep hirarki ini, OSPF menggunakan pembagian jaringan berdasarkan konsep area-area. Pembagian berdasarkan area ini yang juga merupakan salah satu kelebihan OSPF.

Konsep Area dalam OSPF

OSPF dibuat dan dirancang untuk melayani jaringan lokal berskala besar. Artinya OSPF haruslah memiliki nilai skalabilitas yang tinggi, tidak mudah habis atau “mentok” karena jaringan yang semakin diperbesar. Namun nyatanya pada penerapan OSPF biasa, beberapa kejadian juga dapat membuat router OSPF kewalahan dalam menangani jaringan yang semakin membesar. Router OSPF akan mencapai titik kewalahan ketika:

– Semakin membesarnya area jaringan yang dilayaninya akan semakin banyak informasi yang saling dipertukarkan. Semakin banyak router yang perlu dilayani untuk menjadi neighbour dan adjacence. Dan semakin banyak pula proses pertukaran informasi routing terjadi. Hal ini akan membuat router OSPF membutuhkan lebih banyak sumber memory dan processor. Jika router tersebut tidak dilengkapi dengan memory dan processor yang tinggi, maka masalah akan terjadi pada router ini.
– Topology table akan semakin membesar dengan semakin besarnya jaringan. Topology table memang harus ada dalam OSPF karena OSPF termasuk routing protocol jenis Link State. Topology table menrupakan tabel kumpulan informasi state seluruh link yang ada dalam jaringan tersebut. Dengan semakin membesarnya jaringan, maka topology table juga semakin membengkak besarnya. Pembengkakan ini akan mengakibatkan router menjadi lama dalam menentukan sebuah jalur terbaik yang akan dimasukkan ke routing table. Dengan demikian, performa forwarding data juga menjadi lamban.
– Topology table yang semakin membesar akan mengakibatkan routing table semakin membesar pula. Routing table merupakan kumpulan informasi rute menuju ke suatu lokasi tertentu. Namun, rute-rute yang ada di dalamnya sudah merupakan rute terbaik yang dipilih menggunakan algoritma Djikstra. Routing table yang panjang dan besar akan mengakibatkan pencarian sebuah jalan ketika ingin digunakan menjadi lambat, sehingga proses forwarding data juga semakin lambat dan menguras tenaga processor dan memory. Performa router menjadi berkurang.

Ketika sebuah jaringan semakin membesar dan membesar terus, routing protokol OSPF tidak efektif lagi jika dijalankan dengan hanya menggunakan satu area saja. Seperti telah Anda ketahui, OSPF merupakan routing protokol berjenis Link State. Maksudnya, routing protokol ini akan mengumpulkan data dari status-status setiap link yang ada dalam jaringan OSPF tersebut. Apa jadinya jika jaringan OSPF tersebut terdiri dari ratusan bahkan ribuan link di

dalamnya? Tentu proses pengumpulannya saja akan memakan waktu lama dan resource processor yang banyak. Setelah itu, proses penentuan jalur terbaik yang dilakukan OSPF juga menjadi sangat lambat. Berdasarkan limitasi inilah konsep area dibuat dalam OSPF. Tujuannya adalah untuk mengurangi jumlah link-link yang dipantau dan dimonitor statusnya agar penyebaran informasinya menjadi cepat dan efisien serta tidak menjadi rakus akan tenaga processing dari perangkat router yang menjalankannya.

Tipe-Tipe Router OSPF

Seperti telah Anda ketahui, OSPF menggunakan konsep area dalam menjamin agar penyebaran informasi tetap teratur baik. Dengan adanya sistem area-area ini, OSPF membedakan lagi tipe-tipe router yang berada di dalam jaringannya. Tipe-tipe router ini dikategorikan berdasarkan letak dan perannya dalam jaringan OSPF yang terdiri dari lebih dari satu area. Di mana letak sebuah router dalam jaringan OSPF juga sangat berpengaruh terhadap fungsinya. Jadi dengan demikian, selain menunjukkan lokasi di mana router tersebut berada, nama-nama tipe router ini juga akan menunjukkan fungsinya. Berikut ini adalah beberapa tipe router OSPF berdasarkan letaknya dan juga sekaligus fungsinya:

- Internal Router

  Router yang digolongkan sebagai internal router adalah router-router yang berada dalam satu area yang sama. Router-router dalam area yang sama akan menanggap router lain yang ada dalam area tersebut adalah internal router. Internal router tidak memiliki koneksi-koneksi dengan area lain, sehingga fungsinya hanya memberikan dan menerima informasi dari dan ke dalam area tersebut. Tugas internal router adalah memelihara database topologi dan routing table yang akurat untuk setiap subnet yang ada dalam areanya. Router jenis ini melakukan flooding LSA informasi yang dimilikinya ini hanya kepada router lain yang dianggapnya sebagai internal router.

- Backbone Router

  Salah satu peraturan yang diterapkan dalam routing protokol OSPF adalah setiap area yang ada dalam jaringan OSPF harus terkoneksi dengan sebuah area yang dianggap sebagai backbone area. Backbone area biasanya ditandai dengan penomoran 0.0.0.0 atau sering disebut dengan istilah Area 0. Router-router yang sepenuhnya berada di dalam Area 0 ini dinamai dengan istilah backbone router. Backbone router memiliki semua informasi topologi dan routing yang ada dalam jaringan OSPF tersebut.

- Area Border Router (ABR)

  Sesuai dengan istilah yang ada di dalam namanya “Border”, router yang tergolong dalam jenis ini adalah router yang bertindak sebagai penghubung atau perbatasan. Yang dihubungkan oleh router jenis ini adalah area-area yang ada dalam jaringan OSPF. Namun karena adanya konsep backbone area dalam OSPF, maka tugas ABR hanyalah melakukan penyatuan antara Area 0 dengan area-area lainnya. Jadi di dalam sebuah router ABR terdapat koneksi ke dua area berbeda, satu koneksi ke area 0

dan satu lagi ke area lain. Router ABR menyimpan dan menjaga informasi setiap area yang terkoneksi dengannya. Tugasnya juga adalah menyebarkan informasi tersebut ke masing-masing areanya. Namun, penyebaran informasi ini dilakukan dengan menggunakan LSA khusus yang isinya adalah summarization dari setiap segment IP yang ada dalam jaringan tersebut. Dengan adanya summary update ini, maka proses pertukaran informasi routing ini tidak terlalu memakan banyak resource processing dari router dan juga tidak memakan banyak bandwidth hanya untuk update ini.

- Autonomous System Boundary Router (ASBR)

  Sekelompok router yang membentuk jaringan yang masih berada dalam satu hak administrasi, satu kepemilikan, satu kepentingan, dan dikonfigurasi menggunakan policy yang sama, dalam dunia jaringan komunikasi data sering disebut dengan istilah Autonomous System (AS). Biasanya dalam satu AS, router-router di dalamnya dapat bebas berkomunikasi dan memberikan informasi. Umumnya, routing protocol yang digunakan untuk bertukar informasi routing adalah sama pada semua router di dalamnya. Jika menggunakan OSPF, maka semuanya tentu juga menggunakan OSPF.

Namun, ada kasus-kasus di mana sebuah segmen jaringan tidak memungkinkan untuk menggunakan OSPF sebagai routing protokolnya. Misalkan kemampuan router yang tidak memadai, atau kekurangan sumber daya manusia yang paham akan OSPF, dan banyak lagi. Oleh sebab itu, untuk segmen ini digunakanlah routing protocol IGP (Interior Gateway Protocol) lain seperti misalnya RIP. Karena menggunakan routing protocol lain, maka oleh jaringan OSPF segmen jaringan ini dianggap sebagai AS lain.

Untuk melayani kepentingan ini, OSPF sudah menyiapkan satu tipe router yang memiliki kemampuan ini. OSPF mengategorikan router yang menjalankan dua routing protokol di dalamnya, yaitu OSPF dengan routing protokol IGP lainnya seperti misalnya RIP, IGRP, EIGRP, dan IS-IS, kemudian keduanya dapat saling bertukar informasi routing, disebut sebagai Autonomous System Border Router (ASBR). Router ASBR dapat diletakkan di mana saja dalam jaringan, namun yang pasti router tersebut haruslah menjadi anggota dari Area 0-nya OSPF. Hal ini dikarenakan data yang meninggalkan jaringan OSPF juga dianggap sebagai meninggalkan sebuah area. Karena adanya peraturan OSPF yang mengharuskan setiap area terkoneksi ke backbone area, maka ASBR harus diletakkan di dalam backbone area.

Jenis Area dalam OSPF

Setelah membagi-bagi jaringan menjadi bersistem area dan membagi router-router di dalamnya menjadi beberapa jenis berdasarkan posisinya dalam sebuah area, OSPF masih membagi lagi jenis-jenis area yang ada di dalamnya. Jenis-jenis area OSPF

ini menunjukkan di mana area tersebut berada dan bagaimana karakteristik area tersebut dalam jaringan. Berikut ini adalah jenis-jenis area dalam OSPF:

- Backbone Area

  Backbone area adalah area tempat bertemunya seluruh area-area lain yang ada dalam jaringan OSPF. Area ini sering ditandai dengan angka 0 atau disebut Area 0. Area ini dapat dilewati oleh semua tipe LSA kecuali LSA tipe 7 yang sudah pasti akan ditransfer menjadi LSA tipe 5 oleh ABR.

- Standar Area

  Area jenis ini merupakan area-area lain selain area 0 dan tanpa disertai dengan konfigurasi apapun. Maksudnya area ini tidak dimodifikasi macam-macam. Semua router yang ada dalam area ini akan mengetahui informasi Link State yang sama karena mereka semua akan saling membentuk adjacent dan saling bertukar informasi secara langsung. Dengan demikian, semua router yang ada dalam area ini akan memiliki topology database yang sama, namun routing table-nya mungkin saja berbeda.

- Stub Area

  Stub dalam arti harafiahnya adalah ujung atau sisi paling akhir. Istilah ini memang digunakan dalam jaringan OSPF untuk menjuluki sebuah area atau lebih yang letaknya berada paling ujung dan tidak ada cabang-cabangnya lagi. Stub area merupakan area tanpa jalan lain lagi untuk dapat menuju ke jaringan dengan segmen lain. Area jenis ini memiliki karakteristik tidak menerima LSA tipe 4 dan 5. Artinya adalah area jenis ini tidak menerima paket LSA yang berasal dari area lain yang dihantarkan oleh router ABR dan tidak menerima paket LSA yang berasal dari routing protokol lain yang keluar dari router ASBR (LSA tipe 4 dan 5). Jadi dengan kata lain, router ini hanya menerima informasi dari router-router lain yang berada dalam satu area, tidak ada informasi routing baru di router. Namun, yang menjadi pertanyaan selanjutnya adalah bagaimana area jenis ini dapat berkomunikasi dengan dunia luar kalau tidak ada informasi routing yang dapat diterimanya dari dunia luar. Jawabannya adalah dengan menggunakan default route yang akan bertugas menerima dan meneruskan semua informasi yang ingin keluar dari area tersebut. Dengan default route, maka seluruh traffic tidak akan dibuang ke mana-mana kecuali ke segmen jaringan di mana IP default route tersebut berada.

- Totally Stub Area

  Mendengar namanya saja, mungkin Anda sudah bisa menangkap artinya bahwa area jenis ini adalah stub area yang lebih diperketat lagi perbatasannya. Totally stub area tidak akan pernah menerima informasi routing apapun dari jaringan di luar jaringan mereka. Area ini akan memblokir LSA tipe 3, 4, dan 5 sehingga tidak ada informasi yang dapat masuk ke area ini. Area jenis ini juga sama dengan stub area, yaitu mengandalkan default route untuk dapat menjangkau dunia luar.

- Not So Stubby Area (NSSA)

  Stub tetapi tidak terlalu stub, itu adalah arti harafiahnya dari area jenis ini. Maksudnya adalah sebuah stub area yang

masih memiliki kemampuan spesial, tidak seperti stub area biasa. Kemampuan spesial ini adalah router ini masih tetap mendapatkan informasi routing namun tidak semuanya. Informasi routing yang didapat oleh area jenis ini adalah hanya external route yang diterimanya bukan dari backbone area. Maksudnya adalah router ini masih dapat menerima informasi yang berasal dari segmen jaringan lain di bawahnya yang tidak terkoneksi ke backbone area. Misalnya Anda memiliki sebuah area yang terdiri dari tiga buah router. Salah satu router terkoneksi dengan backbone area dan koneksinya hanya berjumlah satu buah saja. Area ini sudah dapat disebut sebagai stub area. Namun nyatanya, area ini memiliki satu segmen jaringan lain yang menjalankan routing protokol RIP misalnya. Jika Anda masih mengonfigurasi area ini sebagai Stub area, maka area ini tidak menerima informasi routing yang berasal dari jaringan RIP. Namun konfigurasilah dengan NSSA, maka area ini bisa mengenali segmen jaringan yang dilayani RIP.

Seperti telah dijelaskan di atas, OSPF harus membentuk hubungan dulu dengan router tetangganya untuk dapat saling berkomunikasi seputar informasi routing. Untuk membentuk sebuah hubungan dengan router tetangganya, OSPF mengandalkan Hello protocol. Namun uniknya cara kerja Hello protocol pada OSPF berbeda-beda pada setiap jenis media. Ada beberapa jenis media yang dapat meneruskan informasi OSPF, masing-masing memiliki karakteristik sendiri, sehingga OSPF pun bekerja mengikuti karakteristik mereka. Media tersebut adalah sebagai berikut:

- Broadcast Multiaccess

  Media jenis ini adalah media yang banyak terdapat dalam jaringan lokal atau LAN seperti misalnya ethernet, FDDI, dan token ring. Dalam kondisi media seperti ini, OSPF akan mengirimkan traffic multicast dalam pencarian router-router neighbour-nya. Namun ada yang unik dalam proses pada media ini, yaitu akan terpilih dua buah router yang berfungsi sebagai Designated Router (DR) dan Backup Designated Router (BDR). Apa itu DR dan BDR akan dibahas berikutnya.

- Point-to-Point

  Teknologi Point-to-Point digunakan pada kondisi di mana hanya ada satu router lain yang terkoneksi langsung dengan sebuah perangkat router. Contoh dari teknologi ini misalnya link serial. Dalam kondisi Point-to-Point ini, router OSPF tidak perlu membuat Designated Router dan Back-up-nya karena hanya ada satu router yang perlu dijadikan sebagai neighbour. Dalam proses pencarian neighbour ini, router OSPF juga akan melakukan pengiriman Hello packet dan pesan-pesan lainnya menggunakan alamat multicast bernama AllSPFRouters 224.0.0.5.

- Point-to-Multipoint

  Media jenis ini adalah media yang memiliki satu interface yang menghubungkannya dengan banyak tujuan. Jaringan-jaringan yang ada di bawahnya dianggap sebagai serangkaian jaringan Point-to-Point yang saling terkoneksi langsung ke

perangkat utamanya. Pesan-pesan routing protocol OSPF akan direplikasikan ke seluruh jaringan Point-to-Point tersebut. Pada jaringan jenis ini, traffic OSPF juga dikirimkan menggunakan alamat IP multicast. Tetapi yang membedakannya dengan media berjenis broadcast multi-access adalah tidak adanya pemilihan Designated dan Backup Designated Router karena sifatnya yang tidak meneruskan broadcast.

- Nonbroadcast Multiaccess (NBMA)

  Media berjenis Nonbroadcast multi-access ini secara fisik merupakan sebuah serial line biasa yang sering ditemui pada media jenis Point-to-Point. Namun secara faktanya, media ini dapat menyediakan koneksi ke banyak tujuan, tidak hanya ke satu titik saja. Contoh dari media ini adalah X.25 dan frame relay yang sudah sangat terkenal dalam menyediakan solusi bagi kantor-kantor yang terpencar lokasinya. Di dalam penggunaan media ini pun dikenal dua jenis penggunaan, yaitu jaringan partial mesh dan fully mesh. OSPF melihat media jenis ini sebagai media broadcast multiaccess. Namun pada kenyataannya, media ini tidak bisa meneruskan broadcast ke titik-titik yang ada di dalamnya. Maka dari itu untuk penerapan OSPF dalam media ini, dibutuhkan konfigurasi DR dan BDR yang dilakukan secara manual. Setelah DR dan BDR terpilih, router DR akan mengenerate LSA untuk seluruh jaringan. Dalam media jenis ini yang menjadi DR dan BDR adalah router yang memiliki koneksi langsung ke seluruh router tetangganya. Semua traffic yang dikirimkan dari router-router neighbour akan direplikasikan oleh DR dan BDR untuk masing-masing router dan dikirim dengan menggunakan alamat unicast atau seperti layaknya proses OSPF pada media Point-to-Point.

Perbandingan RIP dan OSPF

Tabel 2.1 Tabel Perbandingan Fitur Routing RIP & OSPF

Feature	***RIP***	***OSPF***
Algorithm	vector-distance	link-state
Maximum Hops	15. 16 hops is considered to be infinity, implying that the destination is unreachable	Limited only by size of routing tables within routers
Subsystem Segmentation	Treats the autonomous system as a single subsystem	Breaks the autonomous system into one or more areas with two levels of routing algorithms, intra-area, and inter-area.
Metric	destination/hop	destination/cost/link identifier
Integrity	no authentication in RIP-1, Authentication has been added to RIP-2	Supports Authentication. Several authentication algorithms are available ranging from simple password operations to more complex cryptographic algorithms.
Complexity	Relatively Simple - Each router	More Complex. Several more PDUs and exchanges are defined in the protocol. Routing tables are large and include not only destinations, but also a tree representation of local network.
Acceptance	Widely Available, BSD routed supports RIP	newer, published in RFCs
Route Options	Identifies a single route to a destination	Supports multiple routes to a single destination. Facilitates load-balancing traffic distribution
Types of Routes	host, network. RIP-2 adds the ability to transfer subnetwork route entries	Host, network, and subnetwork routes

Tabel 2.2 Tabel Perbandingan Karakteristik Routing RIP & OSPF

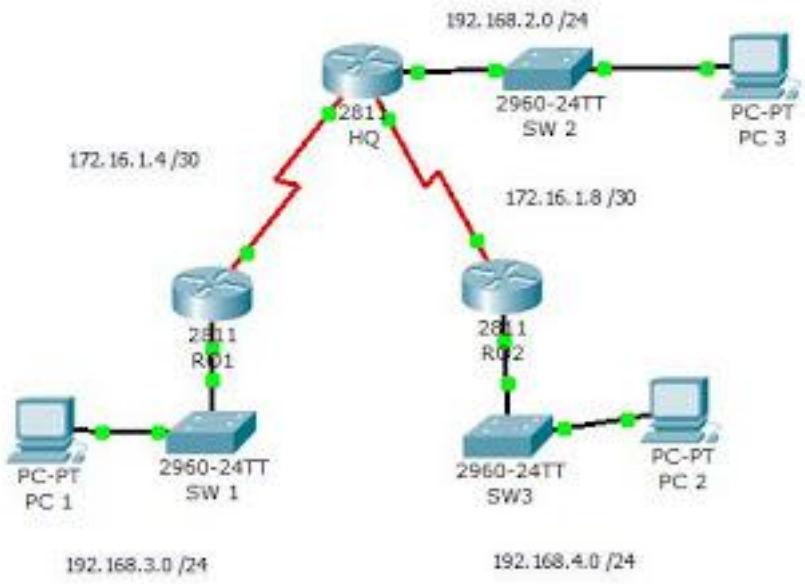
Karakteristik	RIP	OSPF
Update Timer	30 detik	30 menit
Invalid Timer	90 detik	40 detik
Flush Timer	180 detik	-
Count To Infinity	X	
Split Horizon	X	
I-Fold Down Timer	180 detik	10 detik
konvergensi	240/270 detik	5 detik
Route Poisonning	X	
Keseimbangan jalur yang sama	X	X
Keseimbangan Beban Jalur tidak Sama		-
VLSM		X
Alg. Routing	Bellman-Ford	Dijkstra
Metric	Lompatan	Biaya
Batasan Lompatan tak tercapai	15	200

- EIGRP (Enhanced Internal Gateway Routing Protocol)

Pengertian EIGRP (Enhanced Interior Gateway Routing Protocol) merupakan hasil pengembangan dari routing ptotokol pendahulunya yaitu IGRP yang keduanya adalah routing pengembangan dari CISCO. Pengembangan itu dihasilkan oleh perubahan dan bermacam-macam tuntutan dalam jaringan Skala jaringan yang besar. EIGRP menggabungkan kemampuan dari Link-State Protokol dan Distance Vector Protokol, terlebih lagi EIGRP memuat beberapa protocol penting yang secara baik meningkatkan efisiensi penggunaannya ke routing protocol lain.

EIGRP (Enhanced Interior Gateway Routing Protocol) adalah routing protocol yang hanya di adopsi oleh router cisco atau sering disebut sebagai proprietary protocol pada CISCO. Dimana EIGRP ini hanya bisa digunakan sesama router CISCO saja dan routing ini tidak didukung dalam jenis router yang lain. EIGRP sering disebut juga Hybrid-Distance-Vector Routing Protocol, karena cara kerjanya menggunakan dua tipe routing

protocol, yaitu Distance Vector Protocol dan Link State Protocol. Dalam pengertian bahwa routing EIGRP sebenarnya merupakan distance vector protocol tetapi prinsip kerjanya menggunakan links-states protocol, sehingga EIGRP disebut sebagai hybrid-distance-vector, mengapa dikatakan demikian karena prinsip kerjanya sama dengan links-states protocol yaitu mengirimkan semacam hello packet.



Gambar 2.8 EIGRP Routing

Fitur-fitur EIGRP

- Mendukung IP, IPX, dan AppleTalk melalui modul-modul yang bersifat protocol dependent
- Pencarian network tetangga yang dilakukan dengan efisien
- Komunikasi melalui Reliable Transport Protocol (RTP)
- Pemilihan jalur terbaik melalui Diffusing update Algoritma (DUAL)

EIGRP memiliki sistem pembangunan routing protocol dengan membuat sebuah algoritma yang dikenal dengan nama DUAL. Dual digunakan untuk mengkalkulasi dan membangun sebuah routing table. DUAL digunakan untuk memastikan sebuah jalur untuk sebuah network dan menyediakan sebuah loopless routing environment agar membantu mengirimkan sebuah packet ke sebuah jaringan, DUAL mengirimkan sebuah packet query kepada network yang berseberangan dengannya maupun router yang terkoneksi langsung dengan dia.

Selama mengirimkan query packet ,setiap router akan melanjutkan untuk meneruskan query packet tersebut sampai sebuah router akan mengirimkan sebuah replay packet sebagai informasi bagaimana caranya untuk menuju ke sebuah jaringan tertentu. Ketika replay paket telah diterima oleh router yang mengirimkan query packet,

DUAL akan mengkalkulasi dan menentukan router yang mana yang akan menjadi successor dan router yang mana yang akan menjadi feasible successor. Successor akan menjadi jalur yang utama, dan jalur yang terdekat, yang paling efissien yang untuk menuju kesebuah network yang dapat di jangkau oleh DUAL. Jalur successor router dikalkulasikan dengan menggunakan delay, bandwidth, dan factor-faktor yang lain. Sedangkan feasible successor adalah jalur backup atau jalur cadangan yang akan digunakan ketika router tidak memilih jalur successornya dan tidak diharuskan sebuah router yang menggunakan protocol EIGRP menentukan feasible successor.

Ketika successor atupun feasible successor jatuh, maka DUAL akan mengirimkan kembali query packet ke masing-masing router dan meletakkan jalur yang telah ia pelajari dari pengiriman query paket akan disimpan dalam sebuah routing table. DUAL memungkinkan router EIGRP untuk menentukan apakah jalur yang diberikan oleh router tetangga looped atau free-loop dan mengizinkan router yang menggunakan protocol EIGRP untuk menemukan jalur alternatif tanpa harus menunggu update dari router lain.

Perbandingan antar IGRP dan EIGRP

Tabel 2.3 Tabel Perbandingan IGRP & EIGRP

Kategori	IGRP	EIGRP
Compability Mode	Tidak mendukung multi protokol	Mendukung multiprotokol
Metric Calculation	Perhitungan dengan metrik paling efisien menuju ke network tujuan	Perhitungan dengan metrik paling efisien menuju ke network tujuan
HopCount	maksimal 255	maksimal 224
Automatic Protocol Redistribution	Tidak mendistribusikan secara otomatis	mendistribusikan secara otomatis ke routing protokol yang lain
Routing Tagging	Tidak ada	Ada, route tagging yang berfungsi untuk mengecek external routing ,sehingga EIGRP akan mengetahui routing protocol yang digunakan oleh router tetangganya

Struktur Data EIGRP

EIGRP menggunakan beberapa tipe packet :

- *Hello packet* dikirim secara multicast ke IP Address 224.0.0.10. EIGRP akan mengirimkan hello packet untuk mengetahui apakah router-router tetangganya masih hidup ataukah dalam keadaan mati. Pengiriman hello packet tersebut bersifat simultant, dalam hello packet tersebut mempunyai hold time, bila dalam jangka waktu hold time router tetangga tidak membalas hello paket tadi maka router tersebut akan dianggap dalam keadaan mati. Biasanya hold time itu 3x waktunya hello packet, hello packet defaultnya 15 second. Lalu DUAL akan meng-kalkulasi ulang untuk pathnya.
- *Update packets* digunakan untuk menyampaikan tujuan yang dapat dijangkau oleh router. Ketika sebuah router baru ditemukan Update packets dikirim secara unicast sehingga router dapat membangun topologi table.dalam kasus lain, Update packets dikirim secara multicast untuk perubahan link-cost.
- *Acknowledgement packet* adalah Hello packet yang tidak berisikan data, packet Acknowledgement memuat non zero acknowledgement number dan selalu dikirimkan dengan mengunakan unicast address, acknowledgement merupakan sebuah pemberitahuan bahwa paket datanya telah diterima.
- *Query packets* adalah sebuah request atau permintaan yang dilakukan secara multicast yang akan meminta sebuah route. Selama mengirimkan query packet, setiap router akan melanjutkan untuk meneruskan query packet tersebut sampai sebuah router akan mengirimkan sebuah replay packet sebagai informasi bagaimana caranya untuk menuju ke sebuah jaringan tertentu.
- *Reply packets* dikirim apabila router tujuan tidak memiliki feasible successors. Reply packets dikirim untuk merespon Query packet yang menginstrusikan bahwa router pengirim tidak memperhitunghkan ulang jalurnya karena feasible successors masih tetap ada. Reply packets adalah packet unicast yang dikirim ke router yang mengirimkan Query packet.

Teknologi EIGRP

Untuk menyediakan proses routing yang handal EIGRP menggunakan 4 teknologi yang dikombinasikan dan membedakannya dengan routing protocol yang lain.

- Neighbor discovery/recovery, Mekanisme neighbor discovery/recovery mengijinkan router secara dinamis mempelajari router lain yang secara langsung terhubung ke jaringan mereka. Routers juga harus mengetahui ketika router tetangganya tidak dapat lagi dijangkau. Proses ini dicapai dengan low-overhead yang secara periodik mengirimkan hello packet yang kecil. Selama router menerima Hello packet dari router tetangga, router tersebut menganggap bahwa router tetangga tersebut masih berfungsi. Dan keduanya masih bisa melakukan pertukaran informasi.

– Reliable Tansport Protocol (RTP) bertanggung jawab untuk menjamin pengiriman dan penerimaan packet EIGRP ke semua router. RTP juga mendukung perpaduan pengiriman packet secara unicast ataupun multicast. Untuk efisiensi hanya beberapa packet EIGRP yang dikirimkan. Pada jaringan multi access yang mempunyai kemampuan untuk mengirimkan packet secara multicast seperti Ethernet, tidak perlu mengirimkan Hello packet ke semua router tetangga secara individu. Untuk alasan tersebut, EIGRP mengirimkan single multicast hello packet yang berisi sebuah indicator yang menginformasikan si penerima bahwa packet tidak perlu dibalas. Tipe packet yang lain seperti update packet mengindikasikan bahwa balasan terhadap packet tersebut diperlukan. RTP memuat sebuah ketentuan untuk mengirimkan packet multicast secara cepat ketika balasan terhadap packet sedang ditunda, yang membantu memastikan sisa waktu untuk convergence rendah didalam keberadaan bermacam-macam kecepatan links.
– DUAL finite-state machine menaruh keputusan proses untuk semua perhitungan jalur dengan mengikuti semua jalur yang telah dinyatakan oleh semua router tetangga. DUAL menggunakan informasi tentang jarak untuk memilih jalur yang efisien, jalur loop-free dan memilih jalur untuk penempatan di dalam tabel routing berdasarkan successors yang telah dibuat oleh DUAL, successor adalah router yang berdekatan yang digunakan untuk meneruskan packet yang mempunyai nilai cost paling sedikit dengan router tujuan dan dijamin tidak menjadi bagian dari routing loop. ketika perubahan topologi terjadi, DUAL mencoba mencari successors. Jika ditemukan, DUAL menggunakannya untuk menghindari penghitungan jalur yang tidak diperlukan. DUAL juga membuat route backup (jalur cadangan) yang disebut fesible successor.
– Potocol-dependent modules bertanggung jawab pada layer network yang memerlukan protocol khusus. Misalnya IP-EIGRP module yang bertanggung jawab untuk mengirim dan menerima packet EIGRP yang telah dienkapsulasi di dalam protocol IP. IP-EIGRP juga bertanggung jawab untuk menguraikan packet EIGRP dan memberitahukan pada DUAL tentang informasi yang baru saja diterima.

BGP (Border Gateway Protocol)

Border Gateway Protocol atau yang sering disingkat BGP merupakan salah satu jenis routing protocol yang ada di dunia komunikasi data. Sebagai sebuah routing protocol, BGP memiliki kemampuan melakukan pengumpulan rute, pertukaran rute dan menentukan rute terbaik menuju ke sebuah lokasi dalam jaringan. Routing protocol juga pasti dilengkapi dengan algoritma yang pintar dalam mencari jalan terbaik. Namun yang membedakan BGP dengan routing protocol lain seperti misalnya OSPF dan IS-IS ialah, BGP termasuk dalam kategori routing protocol jenis Exterior Gateway Protocol (EGP).

Sesuai dengan namanya, Exterior, routing protocol jenis ini memiliki kemampuan melakukan pertukaran rute dari dan ke luar

jaringan lokal sebuah organisasi atau kelompok tertentu. Organisasi atau kelompok tertentu diluar organisasi pribadi sering disebut dengan istilah autonomous system (AS). Maksudnya rute-rute yang dimiliki oleh sebuah AS dapat juga dimiliki oleh AS lain yang berbeda kepentingan dan otoritas. Begitu juga dengan AS tersebut dapat memiliki rute-rute yang dipunya organisasi lain. Apa untungnya organisasi lain memiliki rute milik organisasi Anda dan sebaliknya? Keuntungannya adalah organisasi Anda bisa dikenal oleh organisasi-organisasi lain yang Anda kirimi rute. Setelah dikenali rute-rute menuju lokasi Anda, banyak orang yang dapat berkomunikasi dengan Anda. Selain itu, Anda juga menerima rute-rute menuju ke organisasi lain, sehingga Anda juga dapat membangun komunikasi dengan para pengguna yang tergabung di organisasi lain. Dengan demikian, komunikasi dapat semakin luas menyebar.

BGP dikenal sebagai routing protocol yang sangat kompleks dan rumit karena kemampuannya yang luar biasa ini, yaitu melayani pertukaran rute antarorganisasi yang besar. Routing protocol ini memiliki tingkat skalabilitas yang tinggi karena beberapa organisasi besar dapat dilayaninya dalam melakukan pertukaran routing, sehingga luas sekali jangkauan BGP dalam melayani para pengguna jaringan. Apa yang akan terjadi jika banyak organisasi di dunia ini yang saling berkumpul dan bertukar informasi routing? Yang akan dihasilkan dari kejadian ini adalah INTERNET. Maka dari itu, tidak salah jika BGP mendapat julukan sebagai inti dari eksisnya dunia Internet.

Analogi Autonomous System atau sering disingkat AS adalah bagaikan sebuah perusahaan tempat Anda bekerja. Sebuah perusahaan memiliki peraturannya sendiri, memiliki struktur organisasi sendiri, memiliki produknya sendiri, memiliki gayanya sendiri dalam berbisnis dan memiliki privasinya sendiri. Semua itu, tidak perlu diketahui oleh orang lain di luar perusahaan Anda, bukan? Namun, apa jadinya jika perusahaan tersebut menghasilkan sebuah produk yang harus dijual ke masyarakat? Tentu pertama-tama produk itu haruslah diketahui orang lain di luar perusahaan tersebut. Produk hasilnya diketahui orang lain bukan berarti seluruh isi perut perusahaan tersebut bisa diketahui oleh pihak lain, bukan? Kira-kira analogi Autonomous System dalam BGP sama seperti ini.

Jaringan internal sebuah organisasi bisa terdiri dari berpuluh-puluh bahkan ratusan perangkat jaringan dan server. Semuanya bertugas melayani kepentingan organisasi tersebut, sehingga otoritas dan kontrolnya hanya boleh diatur oleh organisasi tersebut. Autonomous System biasanya ditentukan dengan sistem penomoran. Sistem penomoran AS di dunia Internet diatur oleh organisasi Internet bernama IANA.

Analogi Untuk BGP

Jika AS diumpamakan sebagai sebuah perusahaan, routing protocol BGP dapat diumpamakan sebagai divisi marketing dan promosi dalam sebuah perusahaan. Divisi marketing memiliki tugas menginformasikan dan memasarkan produk

perusahaan tersebut. Divisi marketing memiliki tugas menyebarkan informasi seputar produk yang akan dijualnya. Dengan berbagai siasat dan algoritma di dalamnya, informasi tersebut disebarkan ke seluruh pihak yang menjadi target pasarnya. Tujuannya adalah agar mereka mengetahui apa produk tersebut dan di mana mereka bisa mendapatkannya.

Selain itu, divisi marketing juga memiliki tugas melakukan survai pasar yang menjadi target penjualan produknya. Para pembeli dan pengecer produk juga akan memberikan informasi seputar keinginan dan kebutuhan mereka terhadap produk yang dijual perusahaan tersebut. Divisi marketing juga perlu mengetahui bagaimana kondisi, prosepek, rute perjalanan, karakteristik tertentu dari suatu daerah target penjualannya. Jika semua informasi tersebut sudah diketahui, maka akan diolah menjadi sebuah strategi marketing yang hebat.

BGP memiliki tugas yang kurang lebih sama dengan divisi marketing dan promosi pada sebuah perusahaan. Tugas utama dari BGP adalah memberikan informasi tentang apa yang dimiliki oleh sebuah organisasi ke dunia di luar. Tujuannya adalah untuk memperkenalkan pada dunia luar alamat-alamat IP apa saja yang ada dalam jaringan tersebut. Setelah dikenal dari luar, server-server, perangkat jaringan, PC-PC dan perangkat komputer lainnya yang ada dalam jaringan tersebut juga dapat dijangkau dari dunia luar. Selain itu, informasi dari luar juga dikumpulkannya untuk keperluan organisasi tersebut berkomunikasi dengan dunia luar.

Dengan mengenal alamat-alamat IP yang ada di jaringan lain, maka para pengguna dalam jaringan Anda juga dapat menjangkau jaringan mereka. Sehingga terbukalah halaman web Yahoo, search engine Google, toko buku Amazon, dan banyak lagi.

BGP merupakan satu-satunya routing protocol yang dapat digunakan untuk menghubungkan dua organisasi besar yang berbeda kepentingan. Meskipun routing protocol jenis EGP bukan hanya BGP saja, namun tampaknya BGP sudah menjadi standar internasional untuk keperluan ini. Hal ini dikarenakan BGP memiliki fitur-fitur yang luar biasa banyak dan fleksibel. Mulai dari pengaturan frekuensi routing update, sistem pembangunan hubungan dengan AS tetangga, sistem hello, policy-policy penyebaran informasi routing, dan banyak lagi fitur lain yang dapat Anda modifikasi dan utak-atik sendiri sesuai dengan selera. Maka dari itu BGP merupakan routing protocol yang dapat dikontrol sebebas-bebasnya oleh pengguna. Dengan demikian, banyak sekali kebutuhan yang dapat terpenuhi dengan menggunakan BGP. BGP juga sangat tepat jika sebuah perusahaan memiliki jalur menuju internet yang berjumlah lebih dari satu. Kondisi jaringan dimana memiliki jalur keluar lebih dari satu buah ini sering disebut dengan istilah multihoming. Jaringan multihoming pada umumnya adalah jaringan berskala sedang sampai besar seperti misalnya ISP, bank, perusahaan minyak multinasional, dan banyak lagi. Biasanya jaringan ini memiliki blok IP dan nomor AS sendiri.

Peranan BGP dalam jaringan multihoming ini sangat besar. Pertama, BGP akan berperan sebagai routing protocol yang melakukan pertukaran routing dengan ISP atau NAP yang berada di atas jaringan ini. Kedua, BGP dengan dipadukan oleh pengaturan policy-policynya yang sangat fleksibel dapat membuat sistem load balancing traffic yang keluar masuk. Selain itu, BGP juga merupakan routing protocol yang sangat reliable kerjanya. Hal ini dikarenakan BGP menggunakan protokol TCP untuk berkomunikasi dengan tetangganya dalam melakukan pertukaran informasi. TCP merupakan protokol yang menganut sistem reliable service, di mana setiap sesi komunikasi yang dibangun berdasarkan protokol ini harus dipastikan sampai tidaknya. Pemastian ini dilakukan menggunakan sistem Acknowledge terhadap setiap sesi komunikasi yang terjadi. Dengan demikian, hampir tidak ada informasi routing dari BGP yang tidak sampai ke perangkat tujuannya. Routing protocol BGP yang sekarang banyak digunakan adalah BGP versi 4 atau lebih sering disingkat sebagai BGP-4.

Kecanggihan dan kerumitan BGP sebenarnya dapat diperjelas intinya dengan beberapa karakteristik kunci. Berikut ini adalah karakteristik routing protokol BGP yang menandakan ciri khasnya, yaitu :

– BGP adalah Path Vector routing protocol yang dalam proses menentukan rute-rute terbaiknya selalu mengacu kepada path yang terbaik dan terpilih yang didapatnya dari router BGP yang lainnya.
– Routing table akan dikirim secara penuh pada awal dari sesi BGP, update selanjutnya hanya bersifat incremental atau menambahi dan mengurangi routing yang sudah ada saja.
– Router BGP membangun dan menjaga koneksi antar-peer menggunakan port TCP nomor 179.
– Koneksi antar-peer dijaga dengan menggunakan sinyal keepalive secara periodik.
– Kegagalan menemukan sinyal keepalive, routing update, atau sinyal-sinyal notifikasi lainnya pada sebuah router BGP dapat memicu perubahan status BGP peer dengan router lain, sehingga mungkin saja akan memicu update-update baru ke router yang lain.
– Metrik yang digunakan BGP untuk menentukan rute terbaik sangat kompleks dan dapat dimodifikasi dengan sangat fleksibel. Ini merupakan sumber kekuatan BGP yang sebenarnya. Metrik-metrik tersebut sering disebut dengan istilah Attribute.
– Penggunaan sistem pengalamatan hirarki dan kemampuannya untuk melakukan manipulasi aliran traffic membuat routing protokol BGP sangat skalabel untuk perkembangan jaringan dimasa mendatang.
– BGP memiliki routing table sendiri yang biasanya memuat informasi prefix-prefix routing yang diterimanya dari router BGP lain. Prefixprefix ini juga disertai dengan informasi atributnya yang dicantumkan secara spesifik di dalamnya.
– BGP memungkinkan Anda memanipulasi traffic menggunakan attribute-attributenya yang cukup banyak. Attribute ini memiliki tingkat prioritas untuk dijadikan sebagai

acuan.

Seperti dijelaskan di atas, BGP merupakan routing protocol yang kompleks dan sulit untuk dirawat. Dengan demikian, penggunaannya diperlukan keahlian khusus dan juga perangkat router berkemampuan proses yang tinggi. Untuk itu, perencanaan yang baik sangat diperlukan untuk menggunakan BGP. Ada kalanya Anda tidak perlu menggunakan routing protocol ini dalam berhubungan dengan AS lain. Jangan gunakan BGP untuk jaringan dengan situasi seperti berikut ini :

– Hanya ada satu buah koneksi yang menuju ke Internet atau ke AS lain. Jaringan ini sering disebut dengan istilah singlehoming.
– Policy routing untuk ke Internet dan pemilihan jalur terbaik tidak terlalu diperlukan dalam sebuah AS.
– Perangkat router yang akan digunakan untuk menjalankan BGP tidak memiliki cukup memory dan tenaga processing untuk menangani update informasi dalam jumlah besar dan konstan.
– Keterbatasan pengetahuan dan kemampuan para administrator jaringannya dalam hal policy routing dan karakteristik BGP lainnya.
– Bandwidth yang kecil yang menghubungkan AS yang satu dengan lainnya.

Untuk membentuk dan mempertahankan sebuah sesi BGP dengan router tetangganya, BGP mempunyai mekanismenya sendiri yang unik. Pembentukan sesi BGP ini mengandalkan paket-paket pesan yang terdiri dari empat macam. Paket-paket tersebut adalah sebagai berikut:

- Open Message

  Sesuai dengan namanya, paket pesan jenis ini merupakan paket pembuka sebuah sesi BGP. Paket inilah yang pertama dikirimkan ke router tetangga untuk membangun sebuah sesi komunikasi. Paket ini berisikan informasi mengenai BGP version number, AS number, hold time, dan router ID.

- Keepalive Message

  Paket Keepalive message bertugas untuk menjaga hubungan yang telah terbentuk antarkedua router BGP. Paket jenis ini dikirimkan secara periodik oleh kedua buah router yang bertetangga. Paket ini berukuran 19 byte dan tidak berisikan data sama sekali.

- Notification Message

  Paket pesan ini adalah paket yang bertugas menginformasikan error yang terjadi terhadap sebuah sesi BGP. Paket ini berisikan field-field yang berisi jenis error apa yang telah terjadi, sehingga sangat memudahkan penggunanya untuk melakukan troubleshooting.

- Update Message

  Paket update merupakan paket pesan utama yang akan membawa informasi rute-rute yang ada. Paket ini berisikan semua informasi rute BGP yang ada dalam jaringan tersebut. Ada tiga komponen utama dalam paket pesan ini, yaitu Network-Layer Reachability Information (NLRI), path attribut, dan withdrawn routes.

- Atribut-atribut Protocol BGP

Atribut – atribut yang diberikan protocol bgp terdiri dari 10 atribute akan tetapi ada satu atribute keluaran cisco dan khusus dipakai untuk produk/router cisco. Masing-masing atribute memiliki sifat dan karakteristik yang berbeda-beda sehingga untuk dapat mengatur sesi komunikasi keluar maupun masuknya suatu routing update dan packet data, kita harus mengerti atribute mana yang sesuai dengan hal yang akan kita manage. Atribut-atribut yang dimaksud adalah sebagai berikut :

– Origin
  Atribut BGP yang satu ini merupakan atribut yang termasuk dalam jenis Well known mandatory. Jika sumbernya berasal router BGP dalam jaringan lokal atau menggunakan asnumber yag sama dengan yang sudah ada, maka indicator atribut ini adalah huruf “i” untuk interior. Apabila sumber rute berasal dari luar jaringan lokal, maka tandanya adalah huruf “e” untuk exterior. Sedangkan apabila rute didapat dari hasil redistribusi dari routing protokol lain, maka tandanya adalah “?” yang artinya adalah incomplete.

– AS_Path
  Atribut ini harus ada pada setiap rute yang dipertukarkan menggunakan BGP. Atribut ini menunjukkan perjalanan paket dari awal hingga berakhir di tempat Anda. Perjalanan paket ini ditunjukkan secara berurut dan ditunjukkan dengan menggunakan nomor-nomor AS. Dengan demikian, akan tampak melalui mana saja sebuah paket data berjalan ke tempat Anda.

– Next Hop
  Next hop sesuai dengan namanya, merupakan atribut yang menjelaskan ke mana selanjutnya sebuah paket data akan dilemparkan untuk menuju ke suatu lokasi. Dalam EBGP-4, yang menjadi next hop dari sebuah rute adalah alamat asal (source address) dari sebuah router yang mengirimkan prefix tersebut dari luar AS. Dalam IBGP-4, alamat yang menjadi parameter next hop adalah alamat dari router yang terakhir mengirimkan rute dari prefix tersebut. Atribut ini juga bersifat Wellknown Mandatory.

– Multiple Exit Discriminator (MED)
  Atribut ini berfungsi untuk menginformasikan router yang berada di luar AS untuk mengambil jalan tertentu untuk mencapat si pengirimnya. Atribut ini dikenal sebagai metrik eksternal dari sebuah rute. Meskipun dikirimkan ke AS lain, atribut ini tidak dikirimkan lagi ke AS ketiga oleh AS lain tersebut. Atribut ini bersifat Optional Nontransitive.

– Local Preference
  Atribut ini bersifat Wellknown Discretionary, di mana sering digunakan untuk memberitahukan router-router BGP lain dalam satu AS ke mana jalan keluar yang di-prefer jika ada dua atau lebih jalan keluar dalam router tersebut. Atribut ini merupakan kebalikan dari MED, di mana hanya didistribusikan antar-router-router dalam satu AS saja atau router IBGP lain.

– Atomic Agregate
  Atribut ini bertugas untuk memberitahukan bahwa sebuah rute telah diaggregate (disingkat menjadi pecahan yang lebih besar) dan ini menyebabkan sebagian informasi ada

yang hilang. Atribut ini bersifat Wellknown Discretionary.

– Agregator
  Atribut yang satu ini berfungsi untuk memberikan informasi mengenai Router ID dan nomor Autonomous System dari sebuah router yang melakukan aggregate terhadap satu atau lebih rute. Parameter ini bersifat Optional Transitive.

– Community
  Community merupakan fasilitas yang ada dalam routing protokol BGP-4 yang memiliki kemampuan memberikan tag pada rute-rute tertentu yang memiliki satu atau lebih persamaan. Dengan diselipkannya sebuah atribut community, maka akan terbentuk sebuah persatuan rute dengan tag tertentu yang akan dikenali oleh router yang akan menerimanya nanti. Setelah router penerima membaca atribut ini, maka dengan sendirinya router tersebut mengetahui apa maksud dari tag tersebut dan melakukan proses sesuai dengan yang diperintahkan. Atribut ini bersifat Optional Transitive.

– Originator ID
  Atribut ini akan banyak berguna untuk mencegah terjadinya routing loop dalam sebuah jaringan. Atribut ini membawa informasi mengenai router ID dari sebuah router yang telah melakukan pengiriman routing. Jadi dengan adanya informasi ini, routing yang telah dikirim oleh router tersebut tidak dikirim kembali ke router itu. Biasanya atribut ini digunakan dalam implementasi route reflector. Atribut ini bersifat Optional Nontransitive.

– Cluster List
  Cluster list merupakan atribut yang berguna untuk mengidentifikasi router-router mana saja yang tergabung dalam proses route reflector. Cluster list akan menunjukkan path-path atau jalur mana yang telah direfleksikan, sehingga masalah routing loop dapat dicegah. Atribut ini bersifat Optional Nontransitive.

– Weight
  Atribut yang satu ini adalah merupakan atribut yang diciptakan khusus untuk penggunaan di router keluaran vendor Cisco. Atribut ini merupakan atribut dengan priority tertinggi dan sering digunakan dalam proses path selection. Atribut ini bersifat lokal hanya untuk digunakan pada router tersebut dan tidak diteruskan ke router lain karena belum tentu router lain yang bukan bermerk Cisco dapat mengenalinya. Fungsi dari atribut ini adalah untuk memilih salah satu jalan yang diprioritaskan dalam sebuah router. Apabila terdapat dua atau lebih jalur keluar maka dengan mengkonfigurasi atribut weight router dapat menetukan salah satu path terbaik yang diprioriataskan sebagai jalur keluar dengan menentukan priority tertinggi.

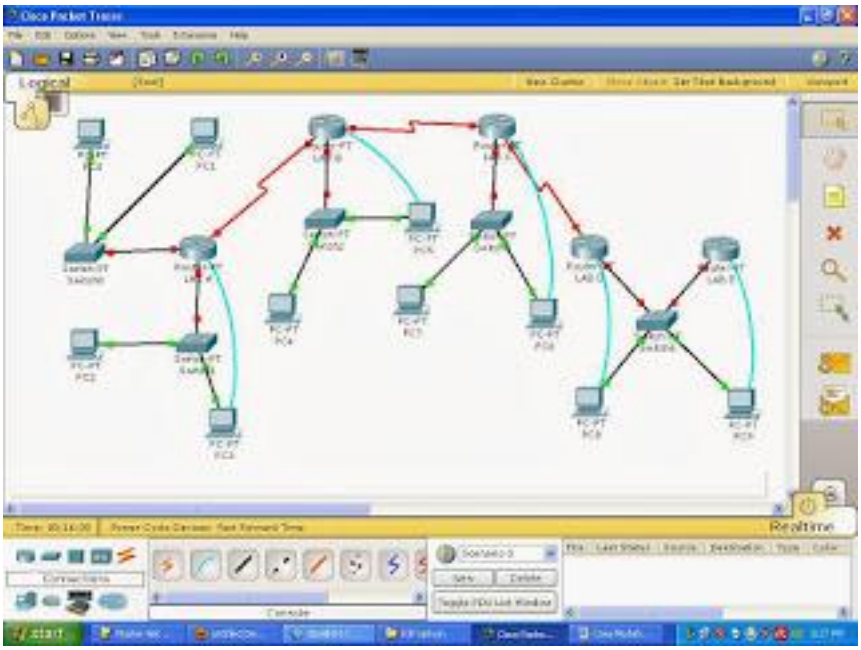
Konfigurasi Dan Verifikasi RIP

Routing protocol yang menggunakan algoritma distance vector, yaitu algoritma Bellman-Ford. Pertama kali dikenalkan pada tahun 1969 dan merupakan algoritma routing yang pertama pada ARPANET. RIP yang merupakan routing protokol dengan algoritma distance vector, yang menghitung jumlah hop (count hop) sebagai routing metric. Jumlah maksimum dari hop yang diperbolehkan

adalah 15 hop. Tiap RIP router saling tukar informasi routing tiap 30 detik, melalui UDP port 520. Untuk menghindari loop routing, digunakan teknik split horizon withpoison reverse. RIP merupakan routing protocol yang paling mudah untuk dikonfigurasi.

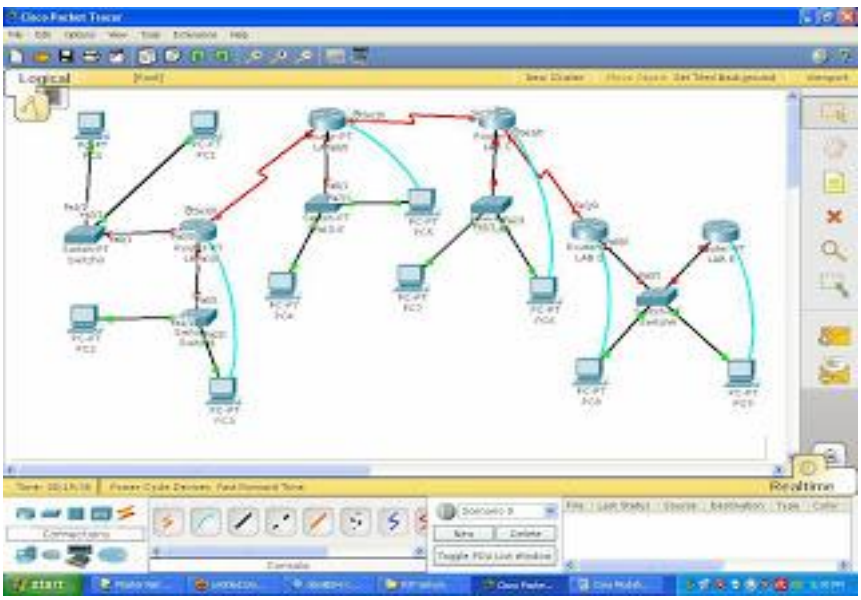
Di bawah ini akan diberikan contoh routing dengan menggunakan RIP dengan aplikasi Packet Tracer versi gratis.

- Buat desain jaringan terlebih dahulu pada Packet Tracer. Seperti gambar dibawah ini



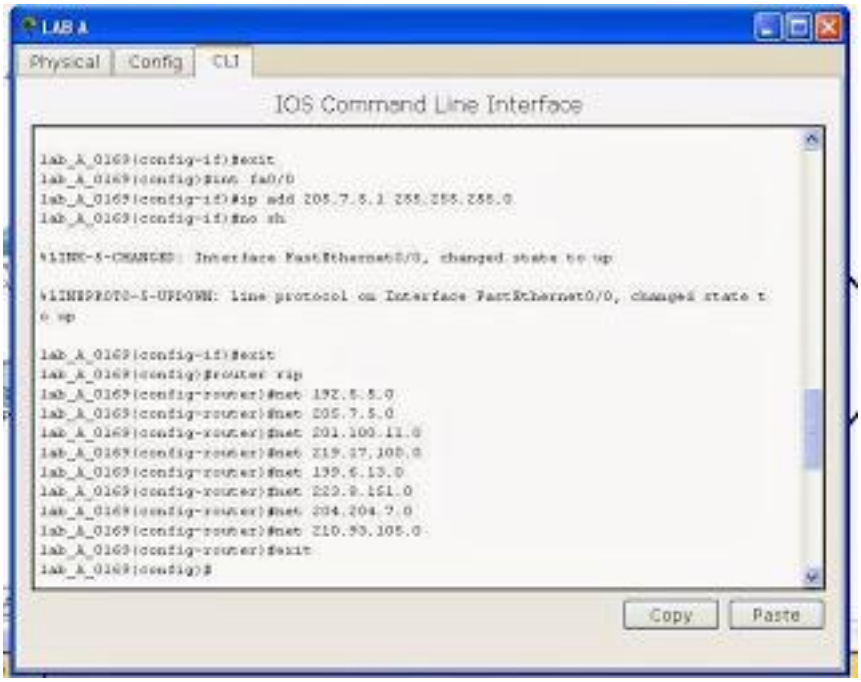
Gambar 2.9 Desain Jaringan Yang Akan Dibuat

- Harus mengetahui letak – letak pengkabelan. Hal ini berguna disaat mengisikan IP address. Seperti gambar dibawah ini :



Gambar 2.10 Hubungan Antar Node Dalam Jaringan

- Mengisikan konfigurasi dan IP address yang sesuai.
- Banyak cara untuk mengkonfigurasi dan mengisikan IP address dari atas ke bawah atau dari bawah ke atas. Mengkonfigurasi dan mengisikan IP address dari atas ke bawah maksudnya adalah mengkonfigurasi dan mengisikan IP address dimulai dari server (router) terlebih dahulu kemudian terus sampai ke klien. Sedangkan mengkonfigurasi dan mengisikan IP address dari bawah ke atas maksudnya adalah mengkonfigurasi dan mengisikan IP address dimulai dari klien terlebih dahulu kemudian terus sampai ke server (router). Pada contoh ini akan menggunakan cara dari atas kebawah karena di dunia nyata konfigurasi dimulai dari server terlebih dahulu.
- Mengkonfigurasikan router A.



Gambar 2.11 Konfigurasi Router A

Dibawah ini adalah sintax router A :

System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)

Copyright (c) 2000 by cisco Systems, Inc.

PT 1001 (PTSC2005) processor (revision 0x200) with 60416K/5120K bytes of memory

Self decompressing the image :

##
############################## [OK]

Restricted Rights Legend

Use, duplication, or disclosure by the Government is

subject to restrictions as set forth in subparagraph

(c) of the Commercial Computer Software -

Restricted

Rights clause at FAR sec. 52.227-19 and subparagraph

(c) (1) (ii) of the Rights in Technical Data and Computer

Software clause at DFARS sec. 252.227-7013.

cisco Systems, Inc.

170 West Tasman Drive

San Jose, California 95134-1706

Cisco Internetwork Operating System Software

IOS (tm) PT1000 Software (PT1000-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5)

Technical Support: http://www.cisco.com/techsupport

Copyright (c) 1986-2005 by cisco Systems, Inc.

Compiled Wed 27-Apr-04 19:01 by miwang

PT 1001 (PTSC2005) processor (revision 0x200) with 60416K/5120K bytes of memory

.Processor board ID PT0123 (0123)

PT2005 processor: part number 0, mask 01

Bridging software.

X.25 software, Version 3.0.0.

4 FastEthernet/IEEE 802.3 interface(s)

2 Low-speed serial(sync/async) network interface(s)

32K bytes of non-volatile configuration memory.

63488K bytes of ATA CompactFlash (Read/Write)

--- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]: n

Press RETURN to get started!

Router>en

Router#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#hostname lab_A_0169

lab_A_0169(config)#int s3/0

lab_A_0169(config-if)#ip add 201.100.11.1 255.255.255.0

lab_A_0169(config-if)#no sh

%LINK-5-CHANGED: Interface Serial3/0, changed state to down

lab_A_0169(config-if)#clock rate 9600

lab_A_0169(config-if)#exit

lab_A_0169(config)#int fa1/0

lab_A_0169(config-if)#ip add 192.5.5.1 255.255.255.0

lab_A_0169(config-if)#no sh

%LINK-5-CHANGED: Interface FastEthernet1/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to up

lab_A_0169(config-if)#exit

lab_A_0169(config)#int fa0/0

lab_A_0169(config-if)#ip add 205.7.5.1 255.255.255.0

lab_A_0169(config-if)#no sh

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

lab_A_0169(config-if)#exit

lab_A_0169(config)#router rip

lab_A_0169(config-router)#net 192.5.5.0

lab_A_0169(config-router)#net 205.7.5.0

lab_A_0169(config-router)#net 201.100.11.0

lab_A_0169(config-router)#net 219.17.100.0

lab_A_0169(config-router)#net 199.6.13.0

lab_A_0169(config-router)#net 223.8.151.0

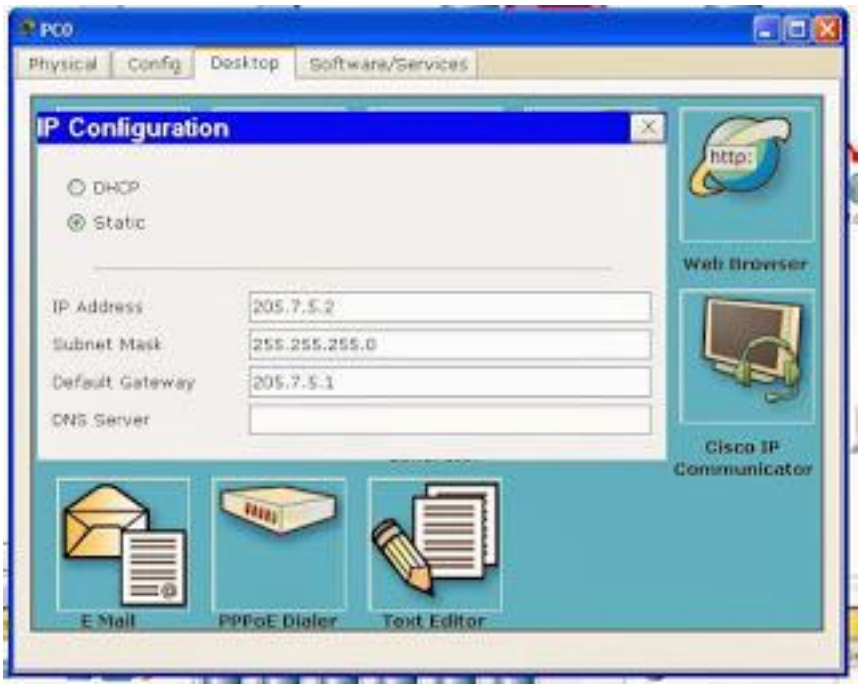
lab_A_0169(config-router)#net 204.204.7.0

lab_A_0169(config-router)#net 210.93.105.0

lab_A_0169(config-router)#exit

lab_A_0169(config)#

- Kemudian mengkonfigurasi PC0 dan PC1



Gambar 2.12 Konfigurasi PC2

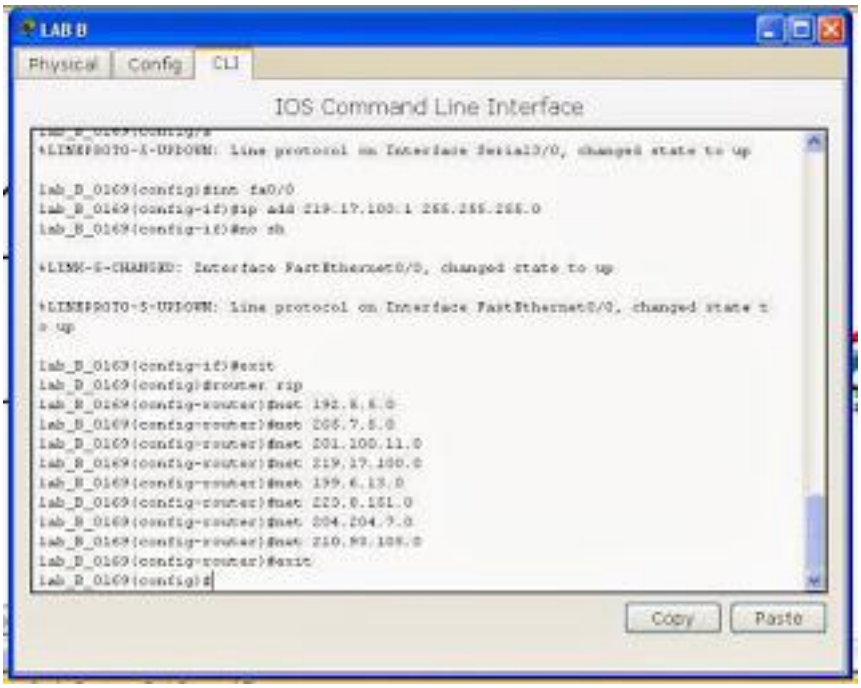
Gambar 2.13 Konfigurasi PC1

- Seteleh itu mengkonfigurasikan PC2 dan PC3

Gambar 2.14 Konfigurasi PC2

Gambar 2.15 Konfigurasi PC3

- Kemudian mengkonfigurasi router B



Gambar 2.16 Konfigurasi Router B

Dibawah ini adalah sintax router B :

System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)

Copyright (c) 2000 by cisco Systems, Inc.

PT 1001 (PTSC2005) processor (revision 0x200) with 60416K/5120K bytes of memory

Self decompressing the image :

##

############################## [OK]

Restricted Rights Legend

Use, duplication, or disclosure by the Government is

subject to restrictions as set forth in subparagraph

(c) of the Commercial Computer Software - Restricted

Rights clause at FAR sec. 52.227-19 and subparagraph

(c) (1) (ii) of the Rights in Technical Data and Computer

Software clause at DFARS sec. 252.227-7013.

cisco Systems, Inc.

170 West Tasman Drive

San Jose, California 95134-1706

Cisco Internetwork Operating System Software

IOS (tm) PT1000 Software (PT1000-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5)

Technical Support: http://www.cisco.com/techsupport

Copyright (c) 1986-2005 by cisco Systems, Inc.

Compiled Wed 27-Apr-04 19:01 by miwang

PT 1001 (PTSC2005) processor (revision 0x200) with 60416K/5120K bytes of memory

.Processor board ID PT0123 (0123)

PT2005 processor: part number 0, mask 01

Bridging software.

X.25 software, Version 3.0.0.

4 FastEthernet/IEEE 802.3 interface(s)

2 Low-speed serial(sync/async) network interface(s)

32K bytes of non-volatile configuration memory.

63488K bytes of ATA CompactFlash (Read/Write)

--- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]: n

Press RETURN to get started!

Router>en

Router#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#hostname lab_B_0169

lab_B_0169(config)#

lab_B_0169(config)#int s2/0

lab_B_0169(config-if)#ip add 199.6.13.1 255.255.255.0

lab_B_0169(config-if)#no sh

%LINK-5-CHANGED: Interface Serial2/0, changed state to down

lab_B_0169(config-if)#clock rate 9600

lab_B_0169(config-if)#exit

lab_B_0169(config)#int s3/0

lab_B_0169(config-if)#ip add 201.100.11.2

255.255.255.0

lab_B_0169(config-if)#no sh

%LINK-5-CHANGED: Interface Serial3/0, changed state to up

lab_B_0169(config-if)#exit

lab_B_0169(config)#

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial3/0, changed state to up

lab_B_0169(config)#int fa0/0

lab_B_0169(config-if)#ip add 219.17.100.1 255.255.255.0

lab_B_0169(config-if)#no sh

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

lab_B_0169(config-if)#exit

lab_B_0169(config)#router rip

lab_B_0169(config-router)#net 192.5.5.0

lab_B_0169(config-router)#net 205.7.5.0

lab_B_0169(config-router)#net 201.100.11.0

lab_B_0169(config-router)#net 219.17.100.0

lab_B_0169(config-router)#net 199.6.13.0

lab_B_0169(config-router)#net 223.8.151.0

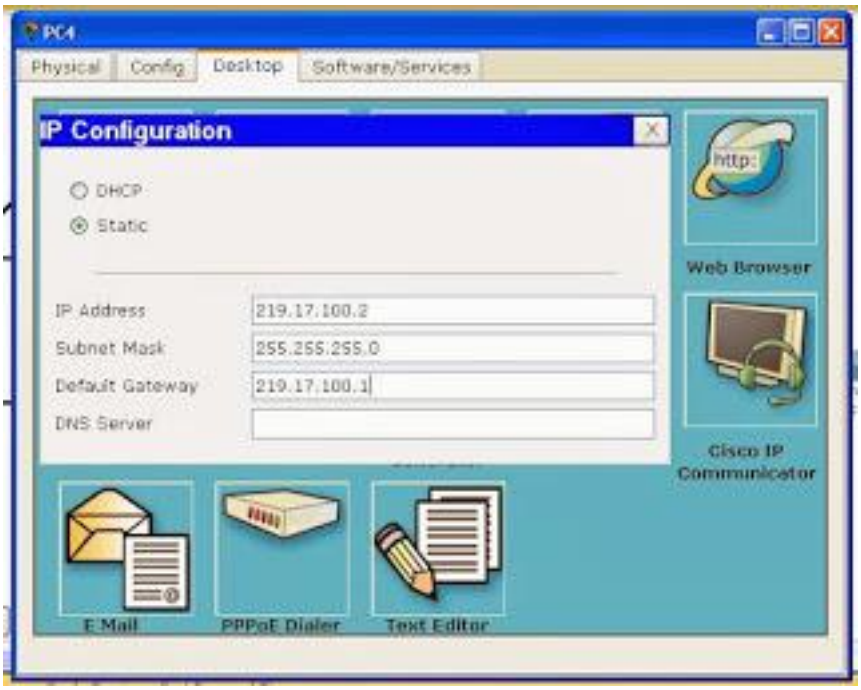
lab_B_0169(config-router)#net 204.204.7.0

lab_B_0169(config-router)#net 210.93.105.0

lab_B_0169(config-router)#exit

lab_B_0169(config)#

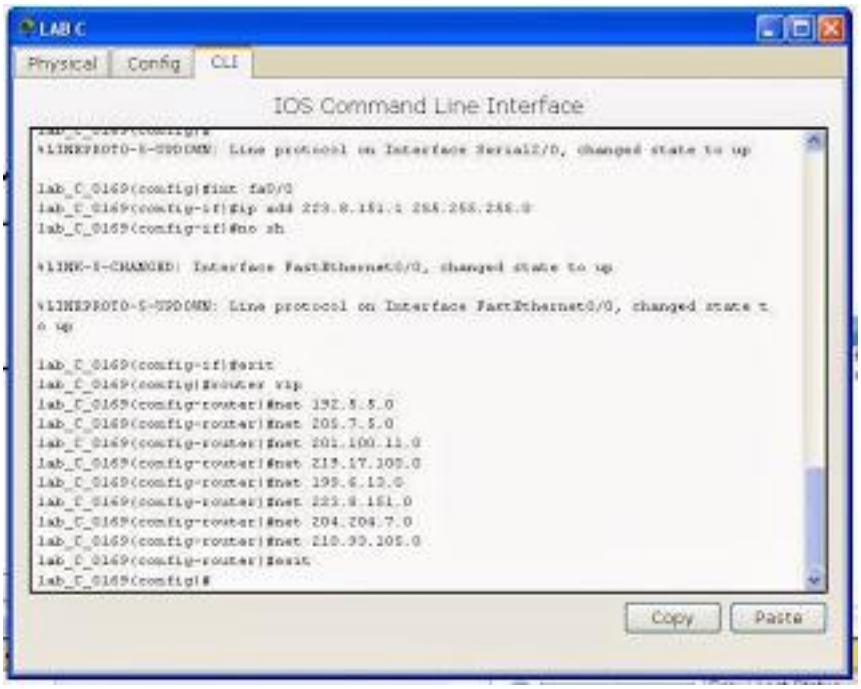
- Setelah itu mengkonfigurasikan PC4 dan PC5



Gambar 2.17 Konfigurasi PC4

Gambar 2.18 Konfigurasi PC5

- Kemudian mengkonfigurasikan router C



Gambar 2.19 Konfigurasi Router C

Dibawah ini adalah sintax router C :

System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)

Copyright (c) 2000 by cisco Systems, Inc.

PT 1001 (PTSC2005) processor (revision 0x200) with 60416K/5120K bytes of memory

Self decompressing the image :

##

############################## [OK]

Restricted Rights Legend

Use, duplication, or disclosure by the Government is

subject to restrictions as set forth in subparagraph

(c) of the Commercial Computer Software - Restricted

Rights clause at FAR sec. 52.227-19 and subparagraph

(c) (1) (ii) of the Rights in Technical Data and Computer

Software clause at DFARS sec. 252.227-7013.

cisco Systems, Inc.

170 West Tasman Drive

San Jose, California 95134-1706

Cisco Internetwork Operating System Software

IOS (tm) PT1000 Software (PT1000-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5)

Technical Support: http://www.cisco.com/techsupport

Copyright (c) 1986-2005 by cisco Systems, Inc.

Compiled Wed 27-Apr-04 19:01 by miwang

PT 1001 (PTSC2005) processor (revision 0x200) with 60416K/5120K bytes of memory

.Processor board ID PT0123 (0123)

PT2005 processor: part number 0, mask 01

Bridging software.

X.25 software, Version 3.0.0.

4 FastEthernet/IEEE 802.3 interface(s)

2 Low-speed serial(sync/async) network interface(s)

32K bytes of non-volatile configuration memory.

63488K bytes of ATA CompactFlash (Read/Write)

--- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]: n

Press RETURN to get started!

Router>en

Router#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#hostname lab_C_0169

lab_C_0169(config)#int s3/0

lab_C_0169(config-if)#ip add 204.204.7.1 255.255.255.0

lab_C_0169(config-if)#clock rate 9600

lab_C_0169(config-if)#no sh

%LINK-5-CHANGED: Interface Serial3/0, changed state to down

lab_C_0169(config-if)#exit

lab_C_0169(config)#int s2/0

lab_C_0169(config-if)#ip add 199.6.13.2

255.255.255.0

lab_C_0169(config-if)#no sh

%LINK-5-CHANGED: Interface Serial2/0, changed state to up

lab_C_0169(config-if)#exit

lab_C_0169(config)#

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up

lab_C_0169(config)#int fa0/0

lab_C_0169(config-if)#ip add 223.8.151.1 255.255.255.0

lab_C_0169(config-if)#no sh

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

lab_C_0169(config-if)#exit

lab_C_0169(config)#router rip

lab_C_0169(config-router)#net 192.5.5.0

lab_C_0169(config-router)#net 205.7.5.0

lab_C_0169(config-router)#net 201.100.11.0

lab_C_0169(config-router)#net 219.17.100.0

lab_C_0169(config-router)#net 199.6.13.0

lab_C_0169(config-router)#net 223.8.151.0

lab_C_0169(config-router)#net 204.204.7.0

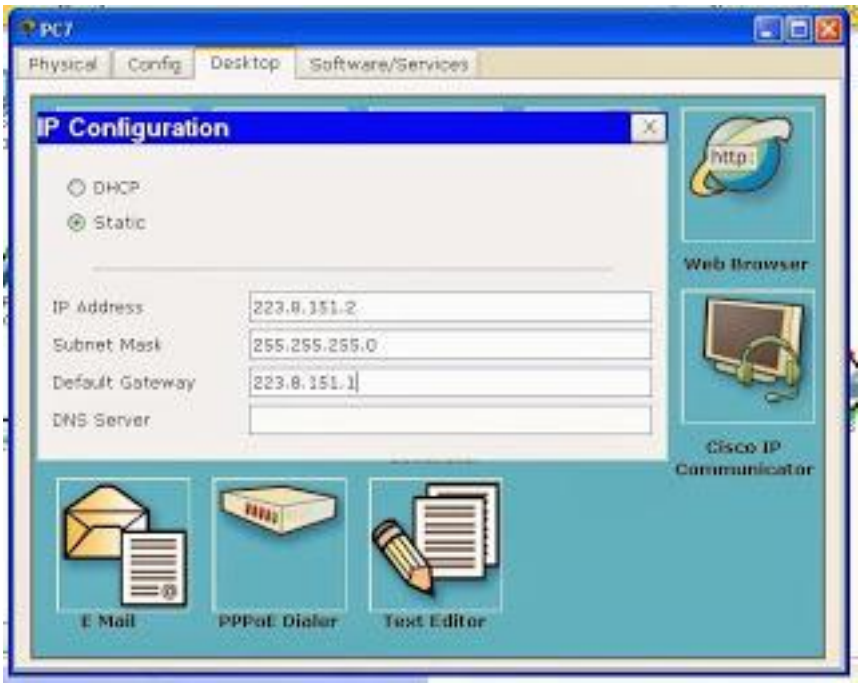
lab_C_0169(config-router)#net 210.93.105.0

lab_C_0169(config-router)#exit

lab_C_0169(config)#

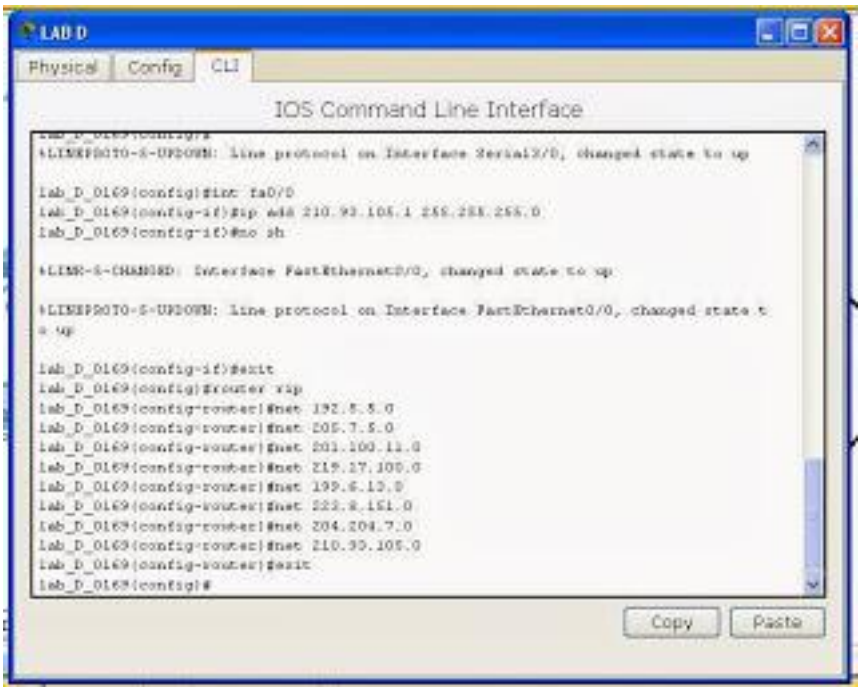
- Setelah itu mengkonfigurasikan PC6 dan PC7

Gambar 2.20 Konfigurasi PC6



Gambar 2.21 Konfigurasi PC7

- Kemudian mengkonfigurasikan router D



Gambar 2.22 Konfigurasi Router D

Dibawah ini adalah sintax router D : System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)

Copyright (c) 2000 by cisco Systems, Inc.

PT 1001 (PTSC2005) processor (revision 0x200) with 60416K/5120K bytes of memory

Self decompressing the image :

##
############################## [OK]

Restricted Rights Legend

Use, duplication, or disclosure by the Government is

subject to restrictions as set forth in subparagraph

(c) of the Commercial Computer Software - Restricted

Rights clause at FAR sec. 52.227-19 and subparagraph

(c) (1) (ii) of the Rights in Technical Data and Computer

Software clause at DFARS sec. 252.227-7013.

cisco Systems, Inc.

170 West Tasman Drive

San Jose, California 95134-1706

Cisco Internetwork Operating System Software

IOS (tm) PT1000 Software (PT1000-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5)

Technical Support: http://www.cisco.com/techsupport

Copyright (c) 1986-2005 by cisco Systems, Inc.

Compiled Wed 27-Apr-04 19:01 by miwang

PT 1001 (PTSC2005) processor (revision 0x200) with 60416K/5120K bytes of memory

.Processor board ID PT0123 (0123)

PT2005 processor: part number 0, mask 01

Bridging software.

X.25 software, Version 3.0.0.

4 FastEthernet/IEEE 802.3 interface(s)

2 Low-speed serial(sync/async) network interface(s)

32K bytes of non-volatile configuration memory.

63488K bytes of ATA CompactFlash (Read/Write)

--- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]: n

Press RETURN to get started!

Router>en

Router#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#hostname lab_D_0169

lab_D_0169(config)#int s3/0

lab_D_0169(config-if)#ip add 204.204.7.2 255.255.255.0

lab_D_0169(config-if)#no sh

%LINK-5-CHANGED: Interface Serial3/0, changed state to up

lab_D_0169(config-if)#exit

lab_D_0169(config)#

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial3/0, changed state to up

lab_D_0169(config)#int fa0/0

lab_D_0169(config-if)#ip add 210.93.105.1 255.255.255.0

lab_D_0169(config-if)#no sh

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

lab_D_0169(config-if)#exit

lab_D_0169(config)#router rip

lab_D_0169(config-router)#net 192.5.5.0

lab_D_0169(config-router)#net 205.7.5.0

lab_D_0169(config-router)#net 201.100.11.0

lab_D_0169(config-router)#net 219.17.100.0

lab_D_0169(config-router)#net 199.6.13.0

lab_D_0169(config-router)#net 223.8.151.0

lab_D_0169(config-router)#net 204.204.7.0

lab_D_0169(config-router)#net 210.93.105.0

lab_D_0169(config-router)#exit

lab_D_0169(config)#

13. Setelah itu mengkonfigurasikan router LAB E

System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)

Copyright (c) 2000 by cisco Systems, Inc.

PT 1001 (PTSC2005) processor (revision 0x200) with 60416K/5120K bytes of memory

Self decompressing the image :

[OK]

Restricted Rights Legend

Use, duplication, or disclosure by the Government is

subject to restrictions as set forth in subparagraph

(c) of the Commercial Computer Software - Restricted

Rights clause at FAR sec. 52.227-19 and subparagraph

(c) (1) (ii) of the Rights in Technical Data and Computer

Software clause at DFARS sec. 252.227-7013.

cisco Systems, Inc.

170 West Tasman Drive

San Jose, California 95134-1706

Cisco Internetwork Operating System Software

IOS (tm) PT1000 Software (PT1000-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5)

Technical Support: http://www.cisco.com/techsupport

Copyright (c) 1986-2005 by cisco Systems, Inc.

Compiled Wed 27-Apr-04 19:01 by miwang

PT 1001 (PTSC2005) processor (revision 0x200) with 60416K/5120K bytes of memory

.Processor board ID PT0123 (0123)

PT2005 processor: part number 0, mask 01

Bridging software.

X.25 software, Version 3.0.0.

4 FastEthernet/IEEE 802.3 interface(s)

2 Low-speed serial(sync/async) network interface(s)

32K bytes of non-volatile configuration memory.

63488K bytes of ATA CompactFlash (Read/Write)

--- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]: n

Press RETURN to get started!

Router>en

Router#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#hostname lab_E_0169

lab_E_0169(config)#int fa0/0

lab_E_0169(config-if)#ip add 210.93.105.2 255.255.255.0

lab_E_0169(config-if)#no sh

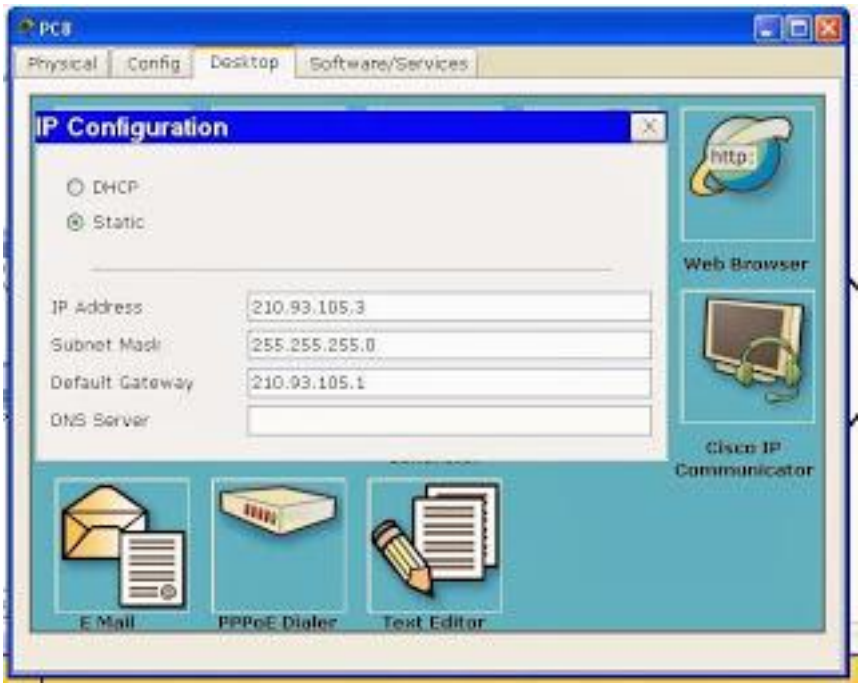
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

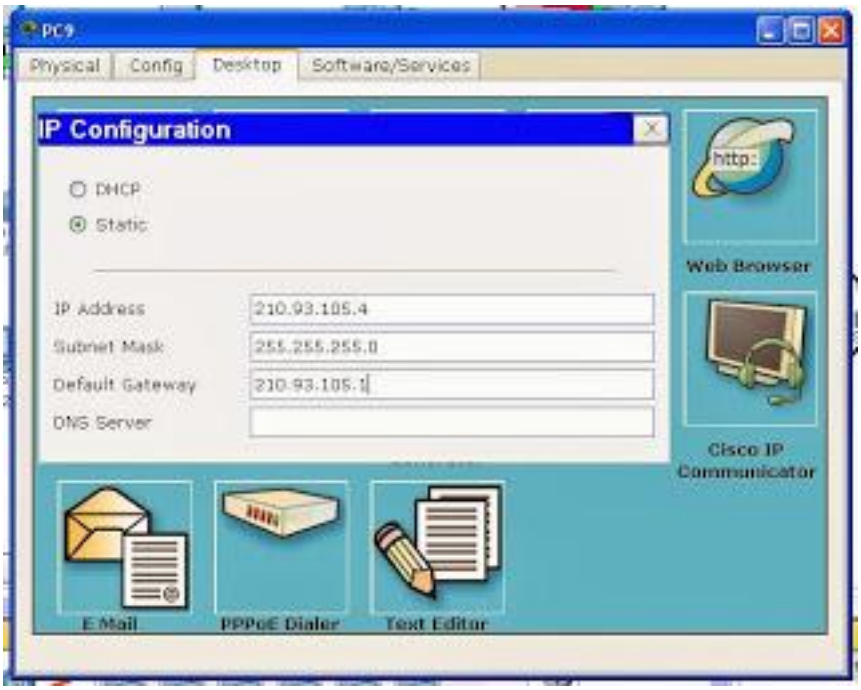
lab_E_0169(config-if)#exit

lab_E_0169(config)#

- Setelah itu mengkonfigurasikan PC8 dan PC9

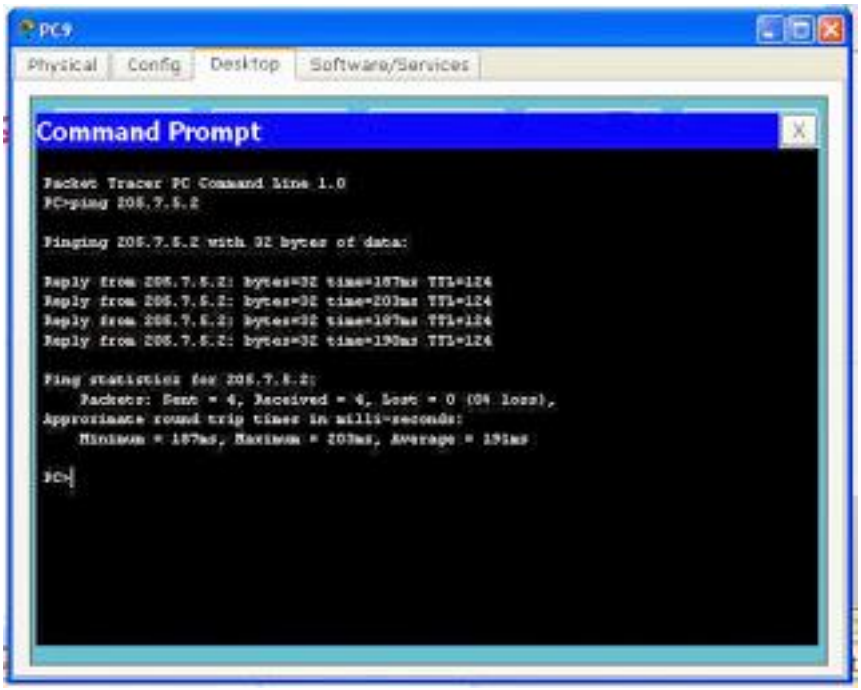


Gambar 2.23 Konfigurasi PC8



Gambar 2.24 Konfigurasi PC9

- Lakukan tes jaringan menggunakan perintah PING.



Gambar 2.25 Hasil Tes Jaringan Dengan Perintah PING

Protocol Routing Eksterior

Semua routing protokol bertujuan mencari rute tersingkat untuk mencapai tujuan. Dan masing-masing protokol mempunyai cara dan metodenya sendiri-sendiri. Secara garis besar, routing protokol dibagi menjadi Interior Routing Protocol dan Exterior Routing Protocol. Keduanya akan diterangkan sebagai berikut :

Interior Routing Protocol

Sesuai namanya, interior berarti bagian dalam. Dan interior routing protocol digunakan dalam sebuah network yang dinamakan autonomus systems (AS) . AS dapat diartikan sebagai sebuah network (bisa besar atau pun kecil) yang berada dalam satu kendali teknik. AS bisa terdiri dari beberapa sub network yang masing-masingnya mempunyai gateway untuk saling berhubungan. Interior routing protocol mempunyai beberapa macam implementasi protokol, yaitu :

- RIP (Routing Information Protocol)

  Merupakan protokol routing yang paling umum dijumpai karena biasanya sudah included dalam sebuah sistem operasi, biasanya Unix atau Novell. RIP memakai metode distance-vector algoritma. Algoritma ini bekerja dengan menambahkan satu angka metrik kepada ruting apabila melewati satu gateway. Satu kali data melewati satu gateway maka angka metriknya bertambah satu (atau dengan kata lain naik satu hop). RIP hanya bisa menangani 15 hop, jika lebih maka host tujuan dianggap tidak dapat dijangkau.

  Oleh karena alasan tadi maka RIP tidak mungkin untuk diterapkan di sebuah AS yang besar. Selain itu RIP juga mempunyai kekurangan dalam hal network masking.

Namun kabar baiknya, implementasi RIP tidak terlalu sulit jika dibandingkan dengan jenis protokol lain.

- OSPF (Open Shortest Path First)

  Merupakan protokol routing yang kompleks dan memakan resource komputer. Dengan protokol ini, route dapat dapat dibagi menjadi beberapa jalan. Maksudnya untuk mencapai host tujuan dimungkinkan untuk mecapainya melalui dua atau lebih rute secara paralel.

Lebih jauh tentang RIP dan OSPF akan diterangkan lebih lanjut.

Exterior Protocol

AS merupakan sebuah jaringan dengan sistem policy yang berperan dalam satu pusat kendali. Internet terdiri dari ribuan AS yang saling terhubung. Untuk bisa saling berhubungan antara AS, maka tiap-tiap AS menggunakan exterior protocol untuk pertukaran informasi routingnya. Informasi routing yang dipertukarkan bernama reachability information (informasi keterjangkauan). Tidak banyak router yang menjalankan routing protokol ini. Hanya router utama dari sebuah AS yang menjalankannya. Dan untuk terhubung ke internet setiap AS harus mempunyai nomor sendiri. Protokol yang mengimplementasikan exterior :

- EGP (Exterior Gateway Protocol)

  Protokol ini mengumumkan ke AS lainnya tentang network yang berada di bawahnya. Pengumumannya kira-kira berbunyi : ” Kalau hendak pergi ke AS nomor sekian dengan nomor network sekian, maka silahkan melewati saya”. Router utama menerima routing dari router-router AS yang lain tanpa mengevaluasinya. Maksudnya, rute untuk ke sebuah AS bisa jadi lebih dari satu rute dan EGP menerima semuanya tanpa mempertimbangkan rute terbaik.

- BGP (Border Gateway Protocol)

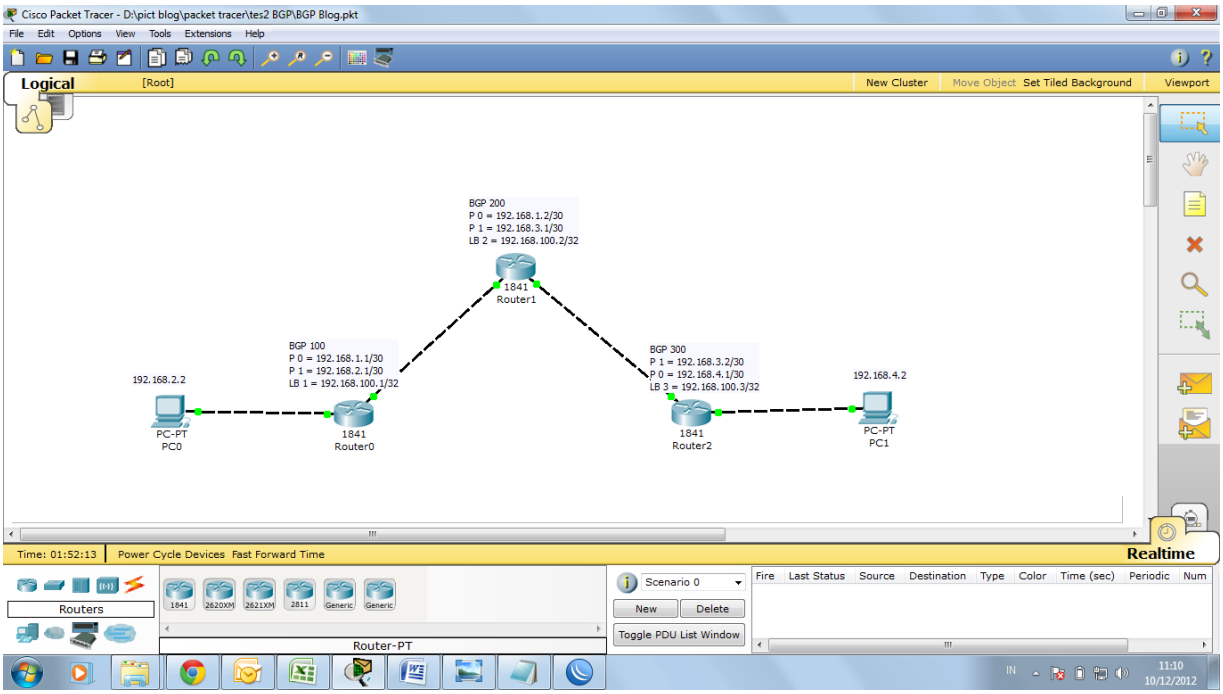
  BGP sudah mempertimbangkan rute terbaik untuk dipilih. Seperti EGP, BGP juga mepertukarkan reachability information.

Konfigurasi Dan Verifikasi BGP

BGP (Border Gateway Protokol) adalah merupakan salah satu jenis routing protokol yang digunakan untuk koneksi antar Autonomous System (AS), dan salah satu jenis routing protokol yang banyak digunakan oleh ISP besar ataupun untuk perbankan. BGP termasuk dalam kategori routing protokol jenis Exterior Gateway Protokol (EGP). Dengan adanya EGP, router dapat melakukan pertukaran rute dari dan ke luar jaringan lokal Auotonomous System (AS). BGP mempunyai skalabilitas yang tinggi karena dapat melayani pertukaran routing pada beberapa organisasi besar. Oleh karena itu BGP dikenal dengan routing protokol yang sangat rumit dan kompleks. Jadi biar jelas, BGP ini digunakan untuk koneksi internet antar client yang beda ISP, beda halnya dengan OSPF yang koneksinya dipakai masih di dalam 1 ISP. Kelebihan dari BGP ini yaitu sangat sederhana dalam instalasi dan kekurangannya yaitu sangat minim untuk

dikembangkan di dalam topologi.

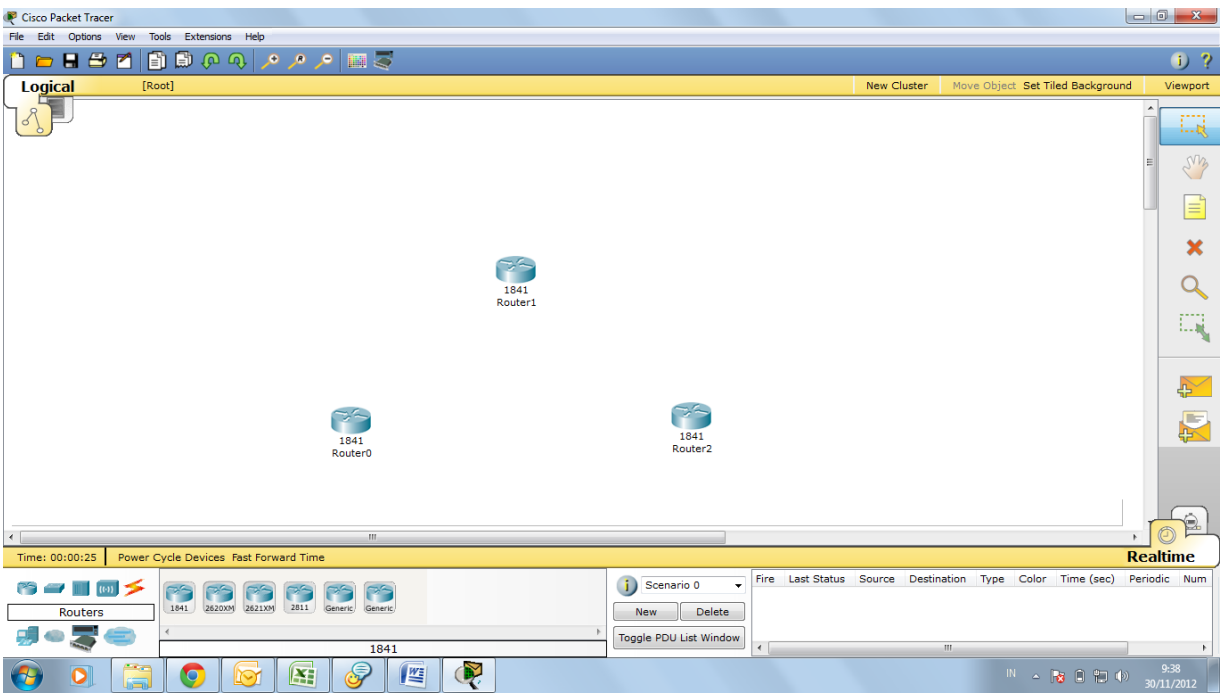
Berikut tampilan skema keseluruhan jaringan yang akan dibuat seperti gambar dibawah ini.



Gambar 2.26 Keseluruhan Skema Jaringan Dengan BGP

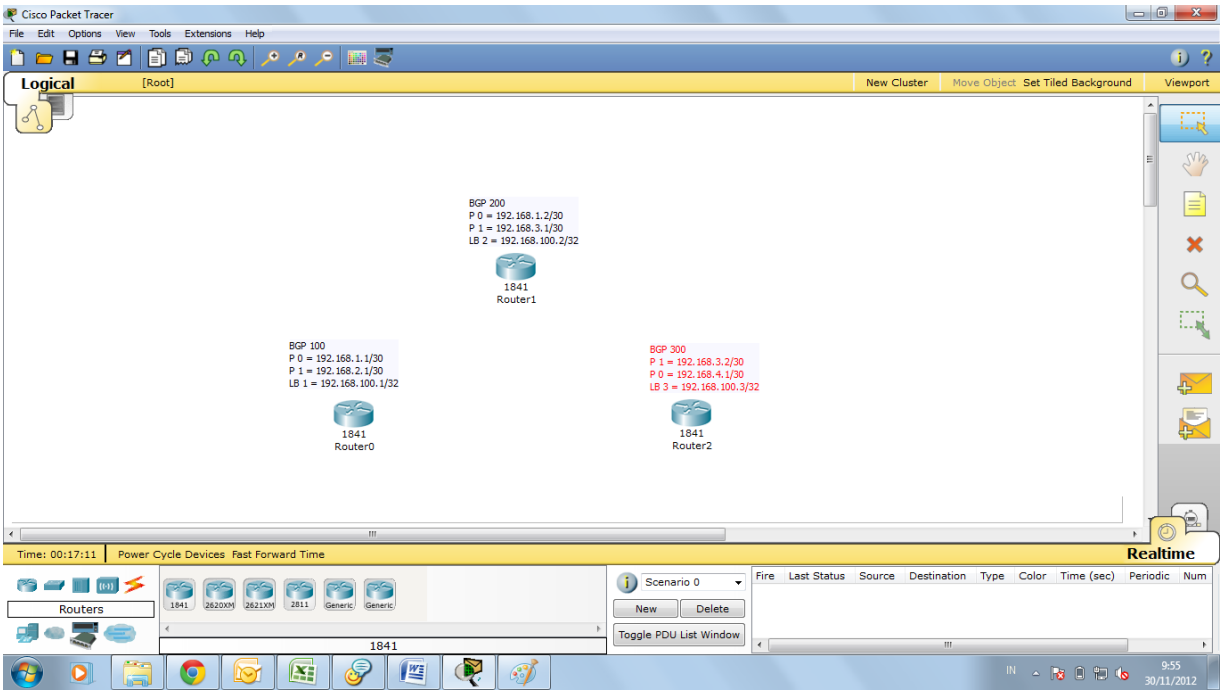
Langkah-langkah yang harus dibuat agar rangkaian di atas dapat terbentuk yaitu:

- *Tempatkan 3 router seperti di bawah ini*

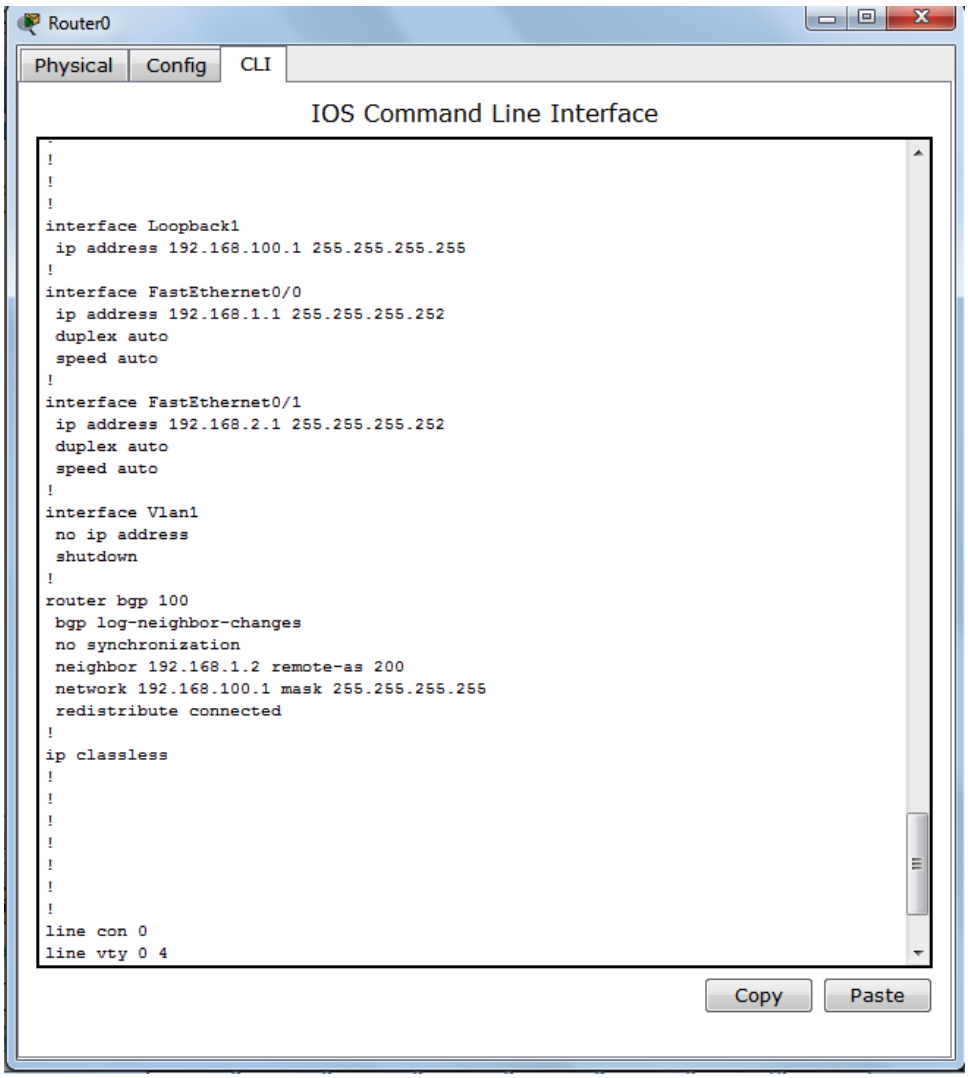


Gambar 2.27 Menempatkan 3 Router

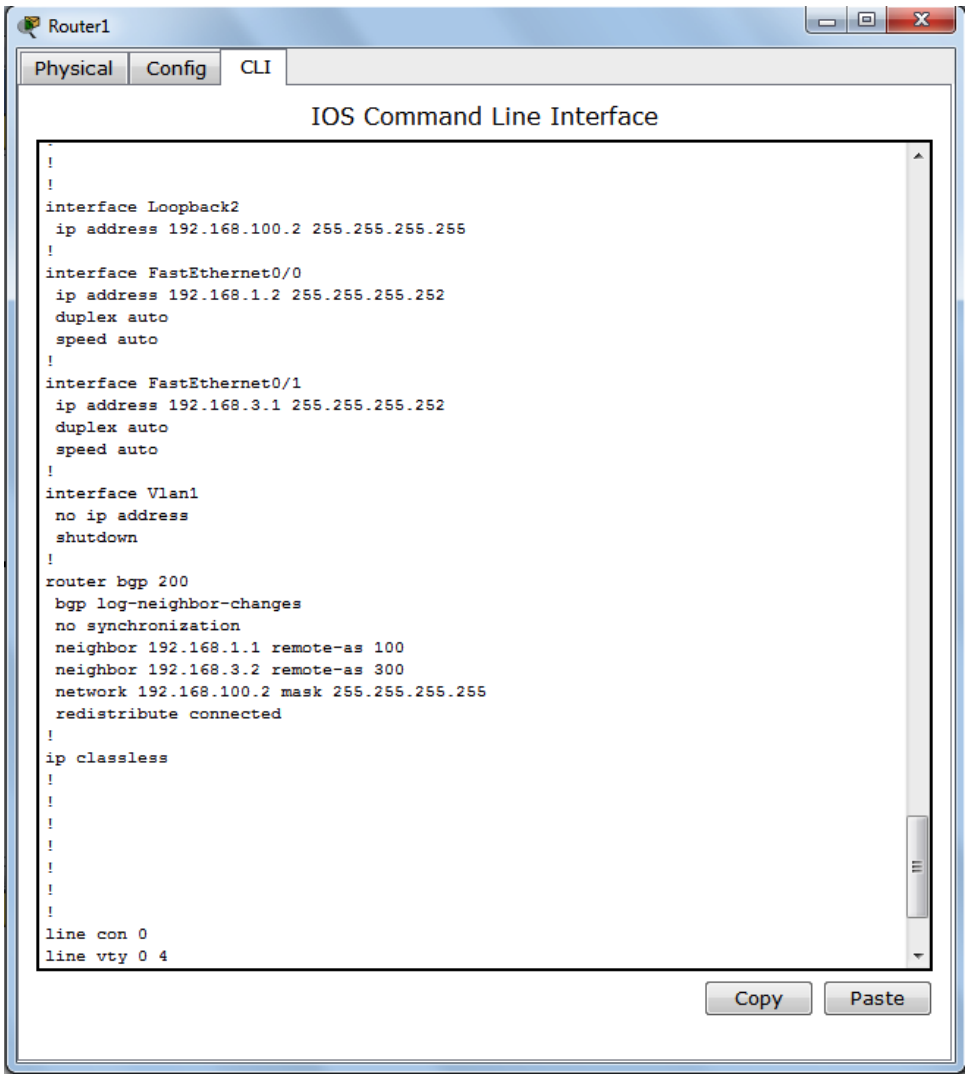
- Setelah kita menempatkan 3 router, diset IP di masing-masing port tiap router



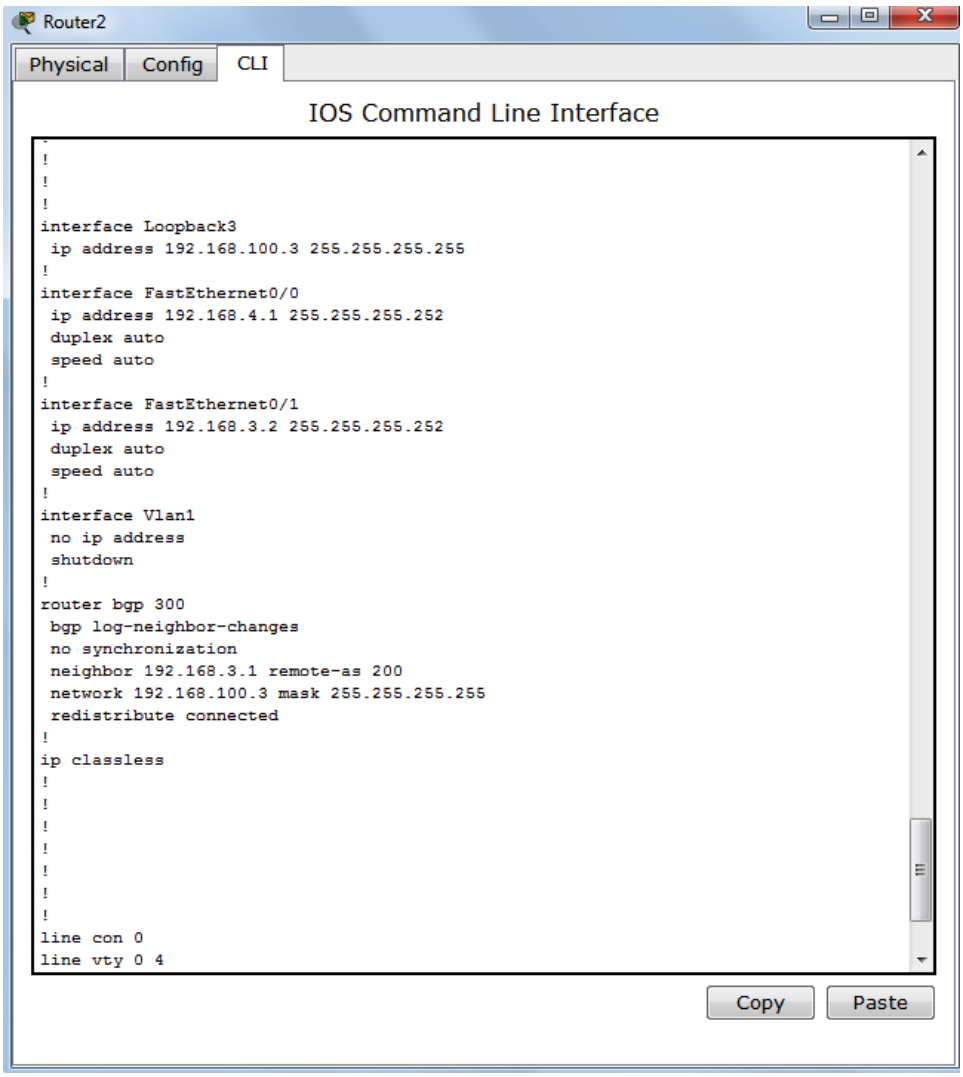
Gambar 2.28 Pemberian IP Untuk Setiap Router



Gambar 2.29 Konfigurasi IP Di Router2



Gambar 2.30 Konfigurasi IP Di Router1



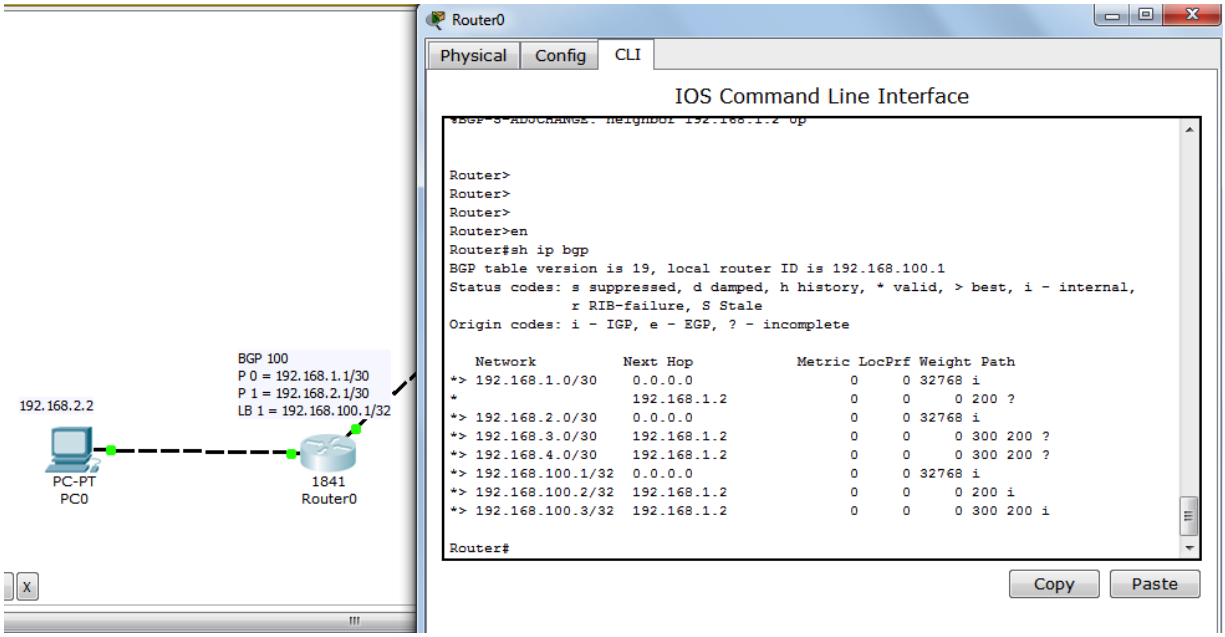
Gambar 2.31 Konfigurasi IP Di Router2

- Setelah kita set IP, maka sekarang kita set untuk router BGP-nya.

– Command-command set router BGP yaitu (pengetesan untuk router0) :

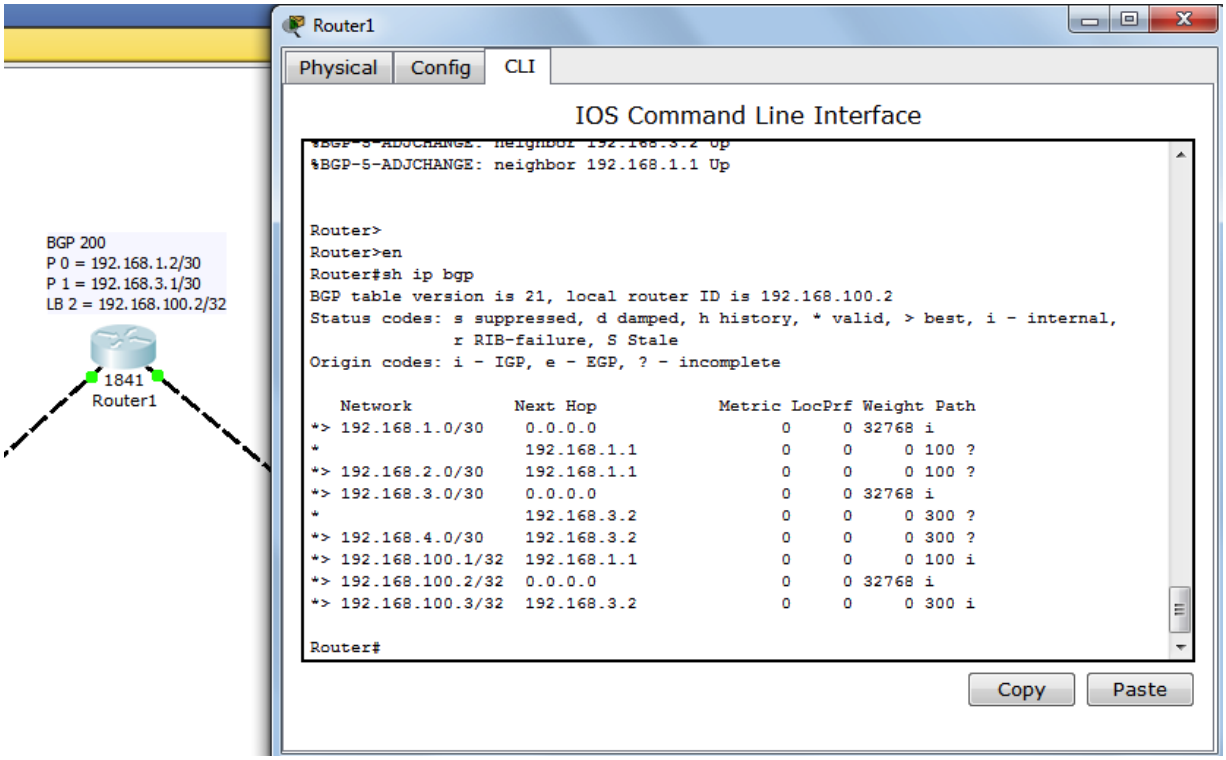
  - Router (config) # router bgp 100
    Maksud dari 100 ini adalah AS number dari router, tiap router hanya bisa dipasang 1 AS number.
  - Router (config-router) # neighbor 192.168.1.2 remote-as 200
    Jadi IP di sini adalah IP tetangga yang berhubungan langsung dengan router ini. Dan untuk remote-as adalah AS number dari router tetangga ini.
  - Router (config-router) # network 192.168.100.1 mask 255.255.255.255
    Untuk IP diatas adalah IP loopback dari router0. IP Loopback adalah IP yang digunakan sebagai router id dalam interface-interface loopback. Interface loopback sendiri adalah interface logikal, artinya interface ini secara nyata tidak ada atau virtual
  - Router (config-router) # Redistribute connected
    Redistribute adalah untuk menyebarkan network antar routing protocol yang berbeda atau sebuah router yang mengambil informasi yang telah ada dalam satu routing

- Dan akhirnya telah dibuat set router BGP di router0. Selanjutnya tinggal menset di router 1 dan 2. Dan berikut gambar hasil dari router BGP apabila semua router sudah kita set router BGP.

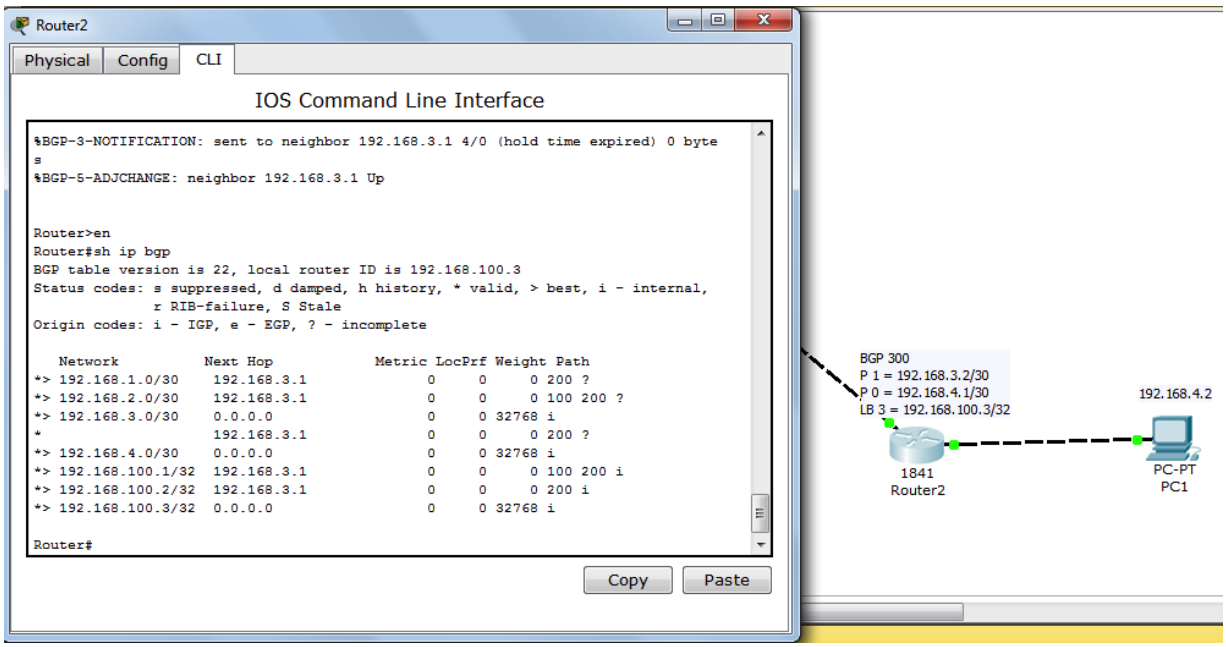


Gambar 2.32 Daftar IP BGP Di Router2

- Jadi dari gambar di atas, dapat kita lihat bahwa untuk sampai ke network 192.168.4.0, link dari router ini akan dilempar (next hope) ke IP 192.168.1.2 yang berada di port 0 router1 dan BGP 200. Dan di sana ada beberapa langkah yang akan dilalui (path) untuk sampai di tujuan, yaitu melalui AS number 200 dan 300. Jadi sederhananya untuk sampai ke network 192.168.4.0, link melewati AS number 200 dan 300.

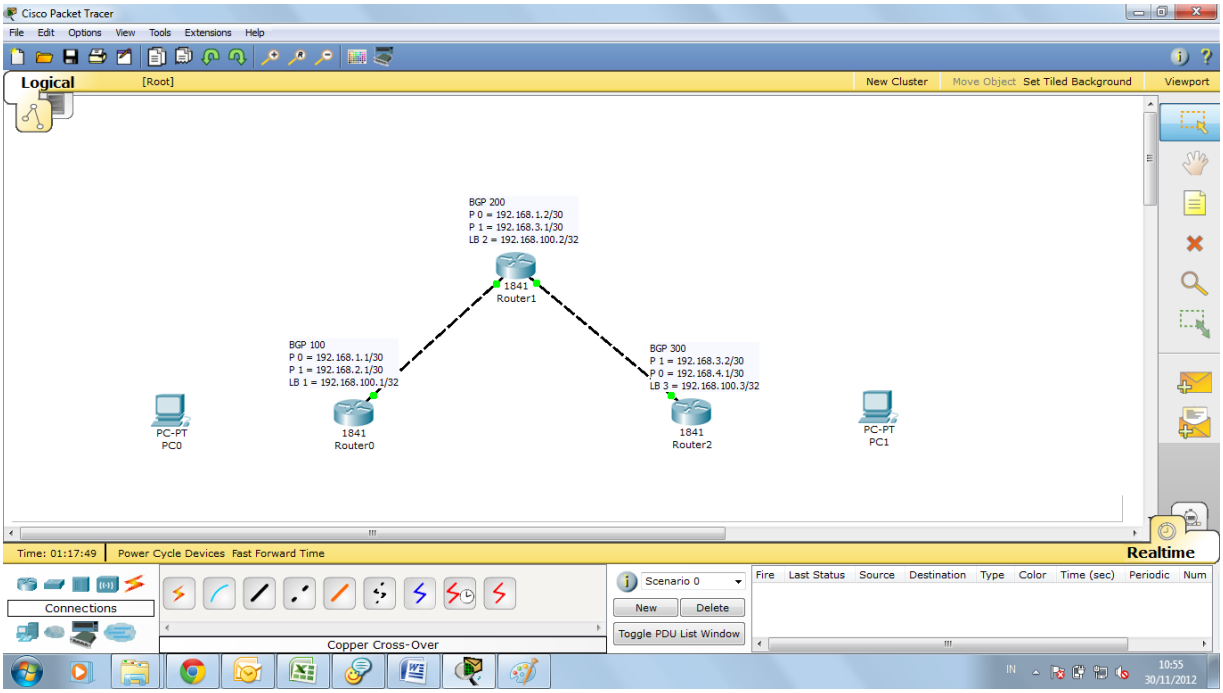


Gambar 2.33 Daftar IP BGP Di Router1



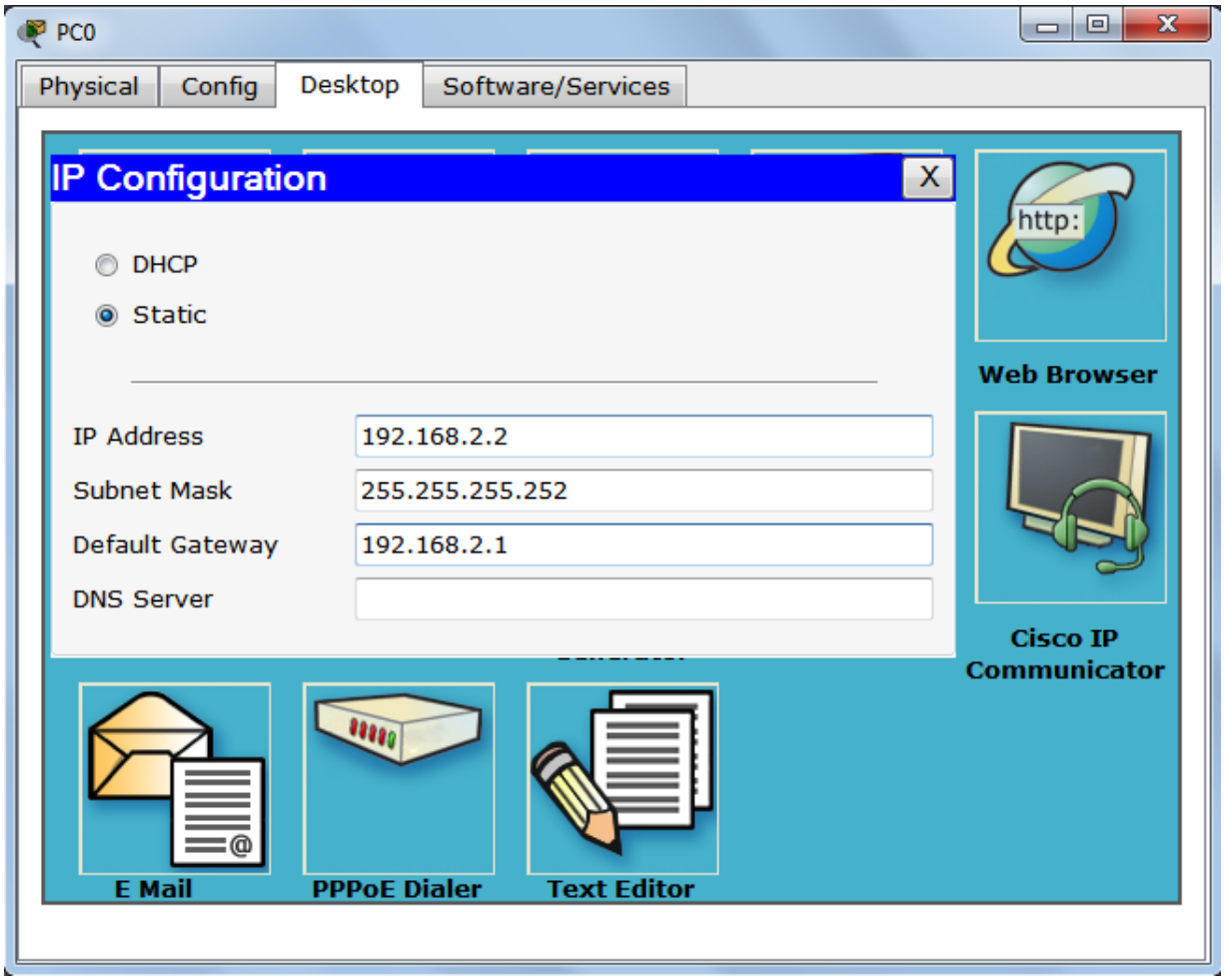
Gambar 2.34 Daftar IP BGP Di Router2

- Setelah semua router sudah diset IP dan BGP nya, sekarang tinggal ditambahkan 2 buah user (PC) pada jaringan ini.

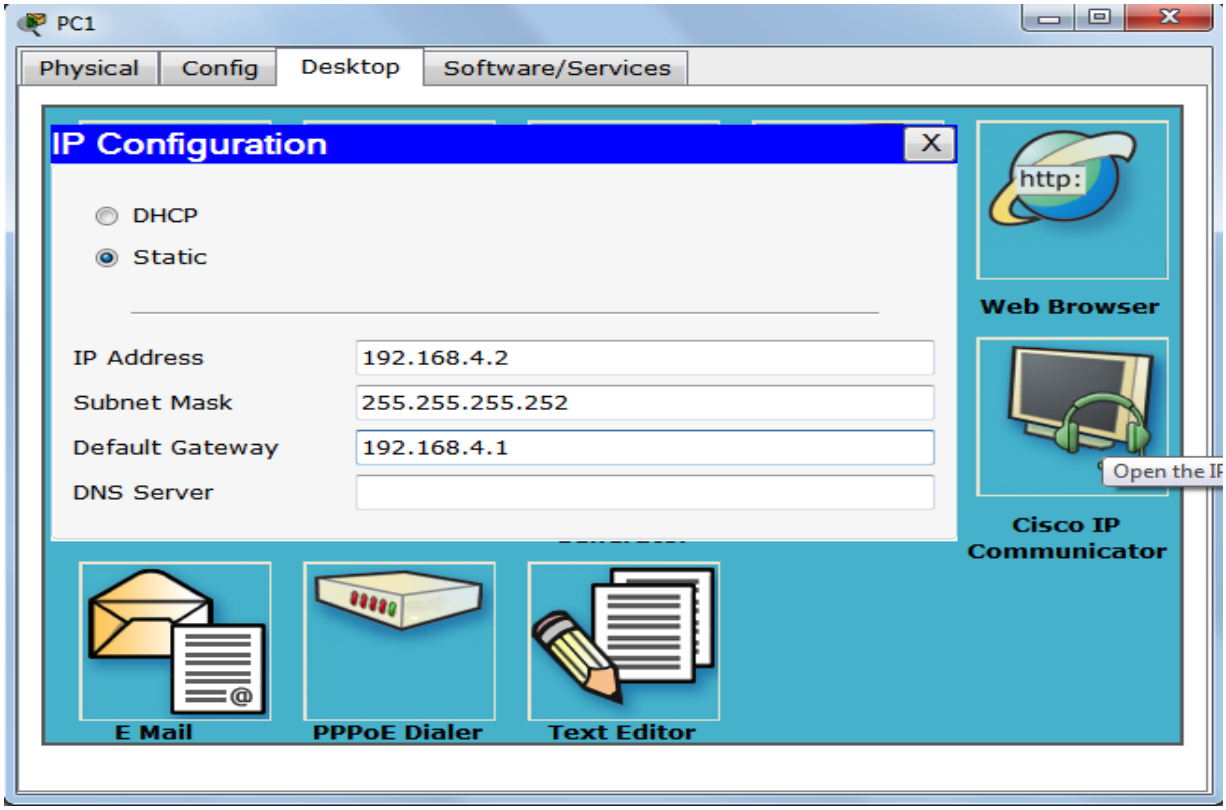


Gambar 2.35 Penempatan PC Sebagai Pengguna

- *Setelah itu diset IP static di kedua PC.*

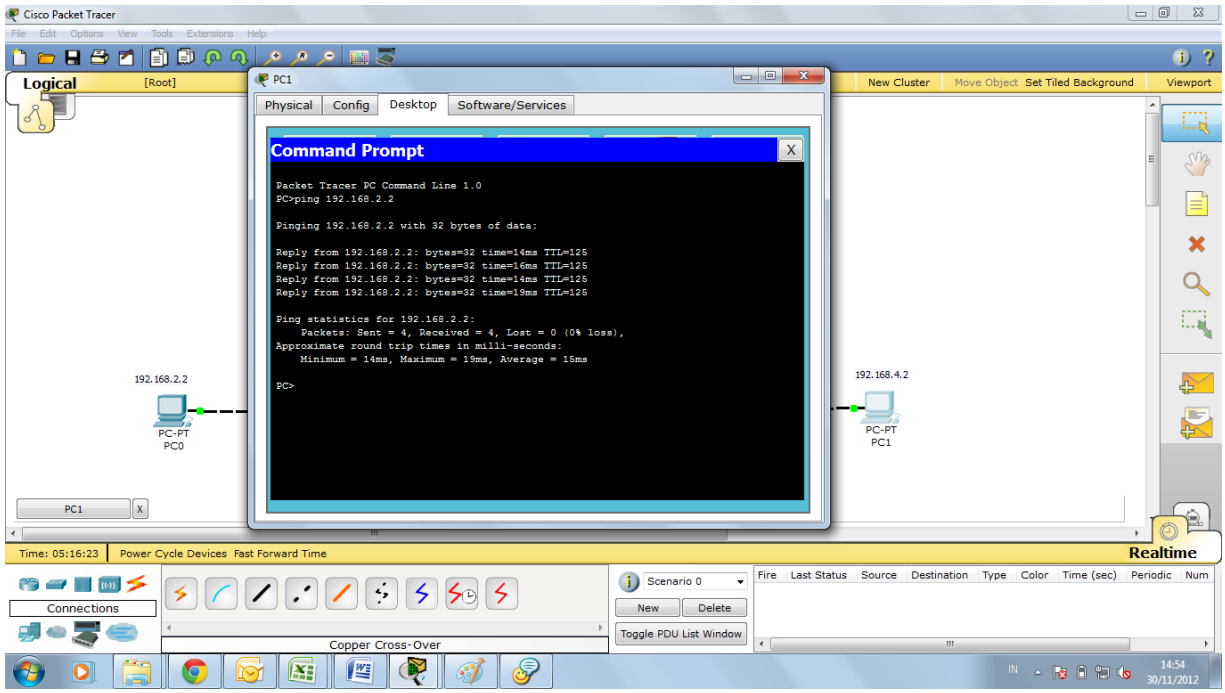


Gambar 2.36 Pengaturan IP Di PC2



Gambar 2.37 Pengaturan IP Di PC1

- Dan sekarang untuk pengecekan terakhir, apakah semua bagian sudah terkoneksi dengan baik, maka untuk itu dilakukan tes PING dari PC0 ke PC1.



Gambar 2.38 Pengetesan Ping Antar Kedua PC

2.1.2.4. Mengasosiasi

Setelah mengikuti kegiatan belajar 2 ini siswa diharapkan dapat menyimpulkan pelbagai hasil percobaan dan pengamatan terkait dengan dasar-dasar routing, protocol routing interior umum, pengaturan routing dalam sebuah jaringan organisasi, konfigurasi dan verifikasi RIP, protocol routing eksterior, protocol routing eksterior yang ada pada ISP, dan Konfigurasi dan verifikasi BGP.

2.1.3 Rangkuman

Routing protocol adalah suatu aturan yang mempertukarkan informasi routing yang akan membentuk sebuah tabel routing sehingga pengalamatan pada paket data yang akan dikirim menjadi lebih jelas dan routing protocol mencari rute tersingkat untuk mengirimkan paket data menuju alamat yang dituju. Routing protocol dibagi menjadi 2, yakni:

- Interior Routing Protocol
  Interior Routing Protocol biasanya digunakan pada jaringan yang bernama Autonomous System, yaitu sebuah jaringan yang berada hanya dalam satu kendali teknik yang terdiri dari beberapa subnetwork dan gateway yang saling berhubungan satu sama lain. Interior routing diimplementasikan melalui:

– Routing Information Protocol (RIP), biasanya terdapat pada sistem operasi UNIX dan Novell yang menggunakan metode distance vector algoritma yang bekerja dengan menambahkan satu angka matrik jika melewati 1 gateway, sehingga jika melewati beberapa gateway maka metriknya juga akan bertambah.

– Open Shortest Path First (OSPF), routing ini memakan banyak resource komputer dibanding Routing Information Protocol (RIP), akan tetapi pada routing ini rute dapat dibagi menjadi beberapa jalan sehinggga data dapat melewati dua atau lebih rute secara pararel.

- Exterior Routing Protocol
  Pada dasarnya internet terdiri dari beberapa Autonomous System yang saling berhubungan satu sama lain dan untuk menghubungkan Autonomous System dengan Autonomous System yang lainnya maka Autonomous System menggunakan exterior routing protocol sebagai pertukaran informasi routingnya.

– Exterior Gateway Protocol (EGP) merupakan protokol yang mengumumkan kepada Autonomous System yang lain tentang jaringan yang berada dibawahnya maka jika sebuah Autonomous System ingin berhubungan dengan jaringan yang ada dibawahnya maka mereka harus melaluinya sebagai router utama. Akan tetapi kelemahan protokol ini tidak bisa memberikan rute terbaik untuk pengiriman paket data.

– Border Gateway Protocol (BGP) merupakan protokol yang sudah dapat memilih rute terbaik yang digunakan pada ISP besar yang akan dipilih.

2.1.4 Tugas

Buatlah kelompok terdiri atas 2-3 orang. Masing-masing kelompok membuat ringkasan tentang routing jaringan komputer, kemudian secara bergantian masing-masing kelompok mempresentasikan hasilnya didepan kelas.

1. Bacalah uraian materi diatas dengan teliti dan cermat.
2. Buatlah ringkasan materi menggunakan aplikasi pengolah presentasi.
3. Presentasikan hasil ringkasan di depan kelas.

2.1.5. Penilaian Diri

Setelah mengikuti kegiatan belajar 2 ini diharapkan siswa memiliki wawasan pengetahuan dan dapat menjawab pelbagai hal terkait dengan dasar-dasar routing, protokol routing interior umum, pengaturan routing dalam sebuah jaringan organisasi, konfigurasi dan verifikasi RIP, protocol routing eksterior, protocol routing eksterior yang ada pada ISP, dan konfigurasi dan verifikasi BGP.

BAB III

3.1 Kegiatan Belajar 3 : Layanan-layanan ISP

3.1.1 Tujuan Pembelajaran

Setelah mengikuti kegiatan belajar 3 ini siswa diharapkan dapat memahami tentang layanan-layanan ISP.

3.1.2 Aktivitas Belajar Siswa

3.1.2.1 Mengamati

Melalui kegiatan belajar 3 ini siswa diharapkan dapat melakukan pengamatan mengenai :

- Protokol-protokol pendukung suatu ISP
- Protokol-protokol lapisan transport
- TCP dan UDP
- Hirarki dan resolusi DNS
- Layanan HTTP dan HTTPS
- Layanan FTP
- Layanan SMTP, POP3 dan IMAP4

3.1.2.2 Menanya

Melalui kegiatan belajar ini siswa dapat melakukan :

- Mendiskusikan protokol-protokol pendukung suatu ISP
- Mendiskusikan protocol-protokol lapisan transport
- Mendiskusikan TCP dan UDP
- Mendiskusikan hirarki dan resolusi DNS
- Mendiskusikan layanan HTTP dan HTTPS
- Mendiskusikan layanan FTP
- Mendiskusikan layanan SMTP, POP3 dan IMAP4

3.1.2.3 Mengumpulkan Informasi

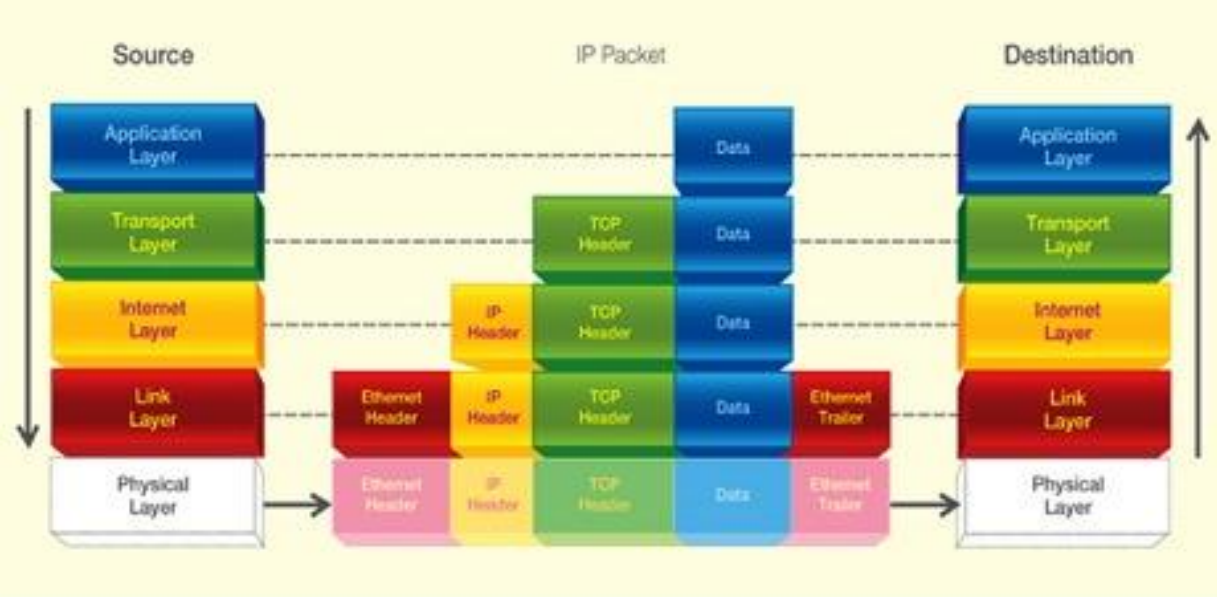
Protokol TCP/IP

Protokol TCP/IP dikembangkan pada akhir dekade 1970-an hingga awal 1980-an sebagai sebuah protokol standar untuk menghubungkan komputer-komputer dan jaringan untuk membentuk sebuah jaringan yang luas (WAN). TCP/IP merupakan sebuah standar jaringan terbuka yang bersifat independen terhadap mekanisme transport jaringan fisik yang digunakan, sehingga dapat digunakan di mana saja. Protokol ini menggunakan skema pengalamatan yang sederhana yang disebut sebagai alamat IP (IP Address) yang mengizinkan hingga beberapa ratus juta komputer untuk dapat saling berhubungan satu sama lainnya di Internet. Protokol ini juga bersifat routable yang berarti protokol ini cocok untuk menghubungkan sistem-sistem berbeda (seperti Microsoft Windows dan keluarga UNIX) untuk membentuk jaringan yang heterogen.

Protokol TCP/IP selalu berevolusi seiring dengan waktu, mengingat semakin banyaknya kebutuhan terhadap jaringan komputer dan Internet. Pengembangan ini dilakukan oleh beberapa badan, seperti halnya Internet Society (ISOC), Internet Architecture Board (IAB), dan Internet Engineering Task Force (IETF). Macam-macam protokol yang berjalan di atas TCP/IP, skema pengalamatan, dan konsep TCP/IP didefinisikan dalam dokumen yang disebut sebagai Permintaan for Comments

(RFC) yang dikeluarkan oleh IETF.

Peranannya sangat penting pada sistem operasi Windows dan juga karena protokol TCP/IP merupakan protokol pilihan (default) dari Windows. Protokol TCP berada pada lapisan Transport model OSI (Open System Interconnection), sedangkan IP berada pada lapisan Jaringan mode OSI.



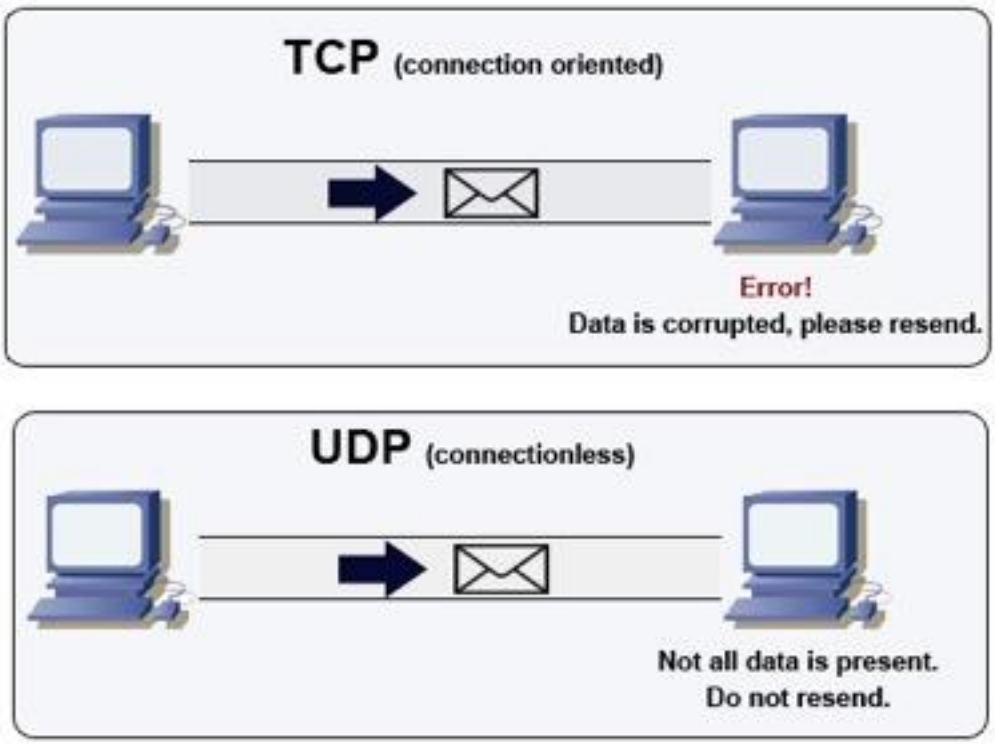
Gambar 3.1 Pro3tokol TCP/IP

Protokol UDP

User Datagram Protocol (UDP) adalah salah satu protokol lapisan transpor TCP/IP yang mendukung komunikasi yang tidak andal (unreliable), tanpa koneksi (connectionless) antara host-host dalam jaringan yang menggunakan TCP/IP. UDP memiliki karakteristik-karakteristik berikut:

- Connectionless (tanpa koneksi): Pesan-pesan UDP akan dikirimkan tanpa harus dilakukan proses negosiasi koneksi antara dua host yang hendak berukar informasi.
- Unreliable (tidak andal): Pesan-pesan UDP akan dikirimkan sebagai datagram tanpa adanya nomor urut atau pesan acknowledgment. Protokol lapisan aplikasi yang berjalan di atas UDP harus melakukan pemulihan terhadap pesan-pesan yang hilang selama transmisi. Umumnya, protokol lapisan aplikasi yang berjalan di atas UDP mengimplementasikan layanan keandalan mereka masing-masing, atau mengirim pesan secara periodik atau dengan menggunakan waktu yang telah didefinisikan.
- UDP menyediakan mekanisme untuk mengirim pesan-pesan ke sebuah protokol lapisan aplikasi atau proses tertentu di dalam sebuah host dalam jaringan yang menggunakan TCP/IP. Header UDP berisi field Source Process Identification dan Destination Process Identification.

- UDP menyediakan penghitungan checksum berukuran 16-bit terhadap keseluruhan pesan UDP.



Gambar 3.2 Perbandingan Protokol UDP Dan TCP/IP Dalam Mengirimkan Data

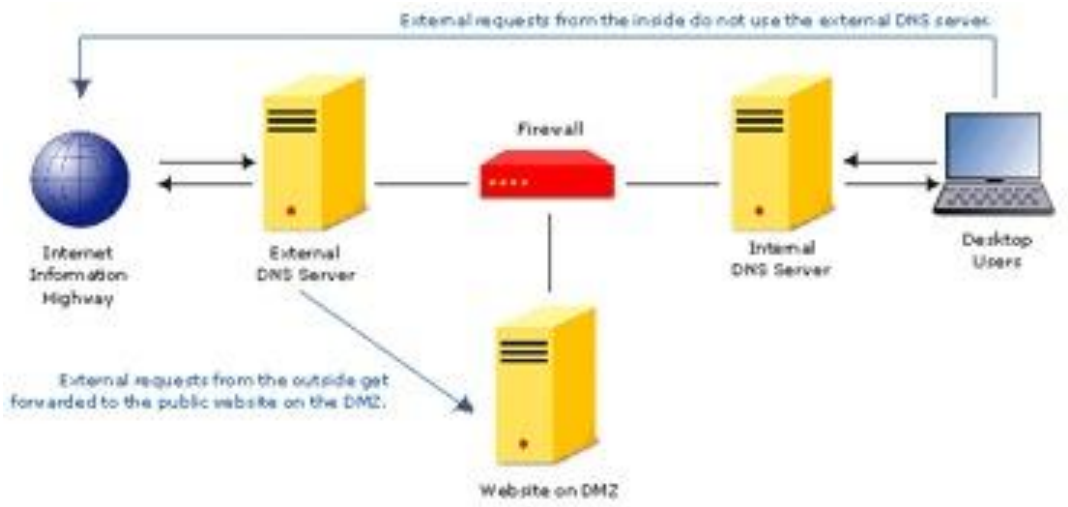
Hirarki Dan Resolusi DNS

Domain Name System (DNS) adalah Distribute Database System yang digunakan untuk pencarian nama komputer (name resolution) di jaringan yang menggunakan TCP/IP. DNS merupakan sebuah aplikasi service yang biasa digunakan di internet seperti web browser atau e-mail yang menerjemahkan sebuah domain ke IP address. Domain Name System (DNS) adalah sebuah aplikasi service di internet yang berguna menerjemahkan sebuah domain name ke IP address dan salah satu jenis system yang melayani permintaan pemetaan IP address ke FQPN (Fany Qualified Domain Name) dan dari FQDN ke IP address. DNS biasanya digunakan pada aplikasi yang berhubungan ke internet sererti Web Browser atau e-mail, dimana DNS membantu memetakan host name sebuah computer ke IP address. Selain digunakan di internet DNS juga dapat di implementasikan ke private jaringan atau internet.

Domain Name System (DNS) adalah suatu sistem yang memungkinkan nama suatu host pada jaringan komputer atau internet ditranslasikan menjadi IP address. Dalam pemberian nama, DNS menggunakan arsitektur hierarki sebagai berikut :

- Root-level domain: merupakan tingkat teratas yang ditampilkan sebagai tanda titik (.)

- Top level domain: kode kategori organisasi atau negara misalnya: .com untuk dipakai oleh perusahaan; .edu untuk dipakai oleh perguruan tinggi; .gov untuk dipakai oleh badan pemerintahan. Selain itu untuk membedakan pemakaian nama oleh suatu negara dengan negara lain digunakan tanda misalnya .id untuk Indonesia atau .au untuk australia
- *Second level domain: merupakan nama untuk organisasi atau perusahaan, misalnya: microsoft.com; yahoo.com, dan lain-lain*



Gambar 3.3 Diagram Server DNS

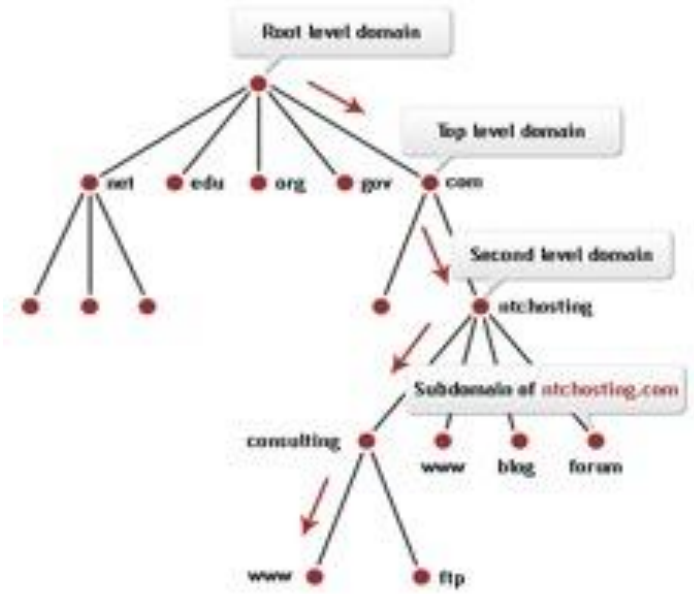
- Fungsi Server DNS
  - *Menerjemahkan nama komputer ke IP address (memetakan nama komputer menjadi IP address).*
  - *Kerangka Peraturan pengiriman secara kontroversi menggunakan keuntungan jenis rekod DNS, dikenal sebagai rekod TXT.*
  - *Menyediakan keluwesan untuk kegagalan computer, beberapa server DNS memberikan perlindungan untuk setiap domain. Tepatnya, tiga belas server akar (root server) digunakan oleh seluruh dunia.*

- Kelebihan Server DNS
  - Mudah, DNS sangat mudah karena pengguna tidak lagi direpotkan untuk mengingat IP address sebuah komputer, cukup host name.
  - Konsisten, IP address sebuah komputer bisa saja berubah, tapi host name tidak harus berubah.
  - Simple, DNS server mudah untuk dikonfigurasikan (bagi admin).
  - DNS mudah untuk di implementasikan di protocol TCP/IP.

- Kekurangan Server DNS
  - Pengguna tidak dapat menggunakan nama banyak untuk mencari nama domain baik di internet maupun di intranet.
  - DNS tidak mudah untuk di

implementasikan.
  – Tidak konsisten.
  – Tidak bisa membuat banyak nama domain.

- Cara Kerja Server DNS
  – Ketika kita melakukan permintaan suatu alamat, misalnya www.google.com dari host kita (misal : 10.121.222.54), maka host kita akan menghubungi name server lokal untuk menanyakan dimanakah www.google.com berada.
  – Name server (misal : 10.121.222.54), akan mengirimkan permintaan tersebut di database lokal kita. Karena tidak ada, maka name server akan menghubungi root DNS servernya, siapa yang memegang domain untuk (.com)
  – Beberapa daftar Top Level Domain (TLD) yang ada sekarang adalah: com, net, org, biz, info, name, museum, dan tv. Sedangkan Country Code Top Level Domain (ccTLD) adalah: us, uk, fr, es, de, it, jp, ie, dll.
  – *Root server akan memberitahu IP address dari server DNS dari www.google.com. Kemudian DNS server lokal akan mengontak server DNS yang mengelola www.google.com. Kemudian DNS server tersebut akan memberitahu IP address dari www.google.com. Kemudian host kita (misal : 10.121.222.54) akan dapat permintaan www.google.com dengan IP address tersebut.*

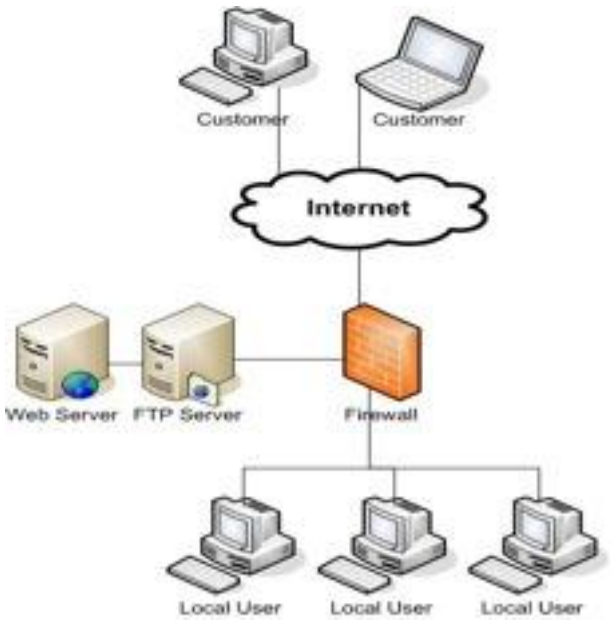


Gambar 3.4 Hirarki Kerja DNS

Layanan FTP

FTP merupakan singkatan dari File Transfer Protocol adalah suatu protokol yang berfungsi untuk pertukaran file dalam suatu

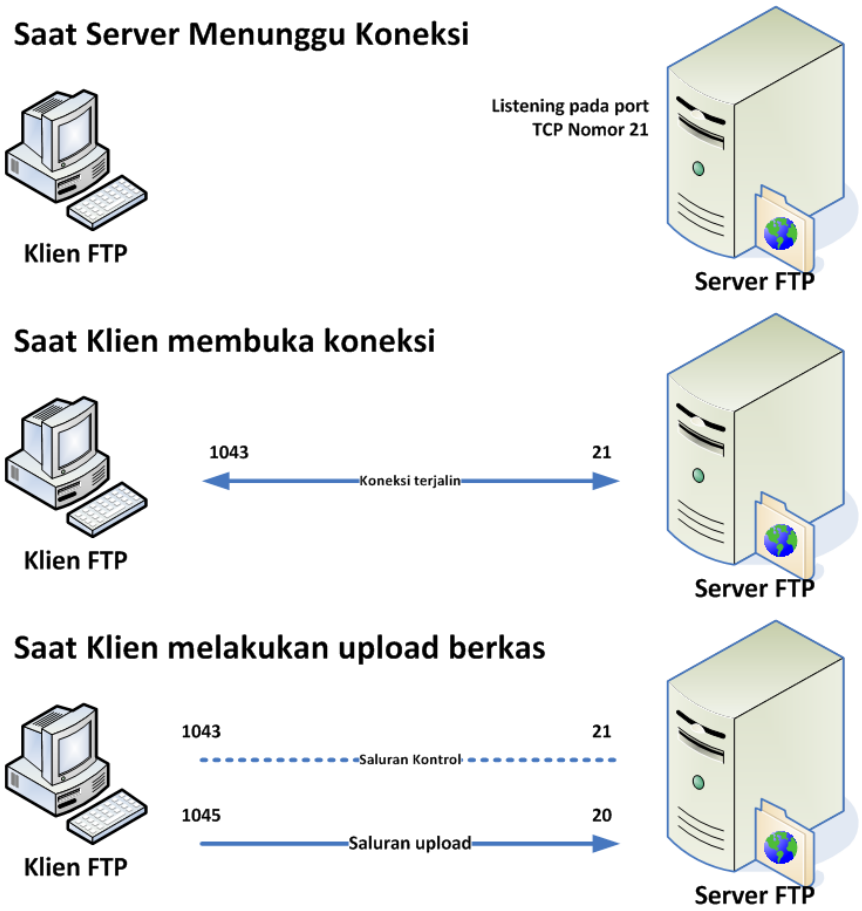
jaringan komputer yang mendukung protokol TCP/IP. FTP terdiri dari sebuah client dan sebuah server yang merupakan aplikasi yang memberikan akses/pertukaran transfer data antara dua komputer (client dan server).



Gambar 3.5 Diagram Server FTP

Transfer file/data ini dapat terjadi antara komputer yang berbentuk mainframe dan sebuah komputer di jaringan lokal atau transfer data dapat terjadi dari komputer kita ke server FTP melalui internet. FTP merupakan aplikasi yang sangat berguna (powerful) karena aplikasi ini menyediakan akses kepada pengunjung atau pengguna untuk mengakses data yang tersimpan pada server tersebut, dan dapat diakses oleh sejumlah besar komputer secara bersamaan.

Fungsi FTP Server adalah menjalankan perangkat lunak yang digunakan untuk pertukaran file (File Exchange), yang selalu siap memberikan layanan FTP apabila mendapatkan permintaan atau permintaan dari FTP Client. FTP Client adalah komputer yang meminta koneksi ke FTP Server untuk tujuan tukar menukar file (Upload dan Download File).



Gambar 3.6 Proses Layanan FTP

Layanan Surat Elektronik

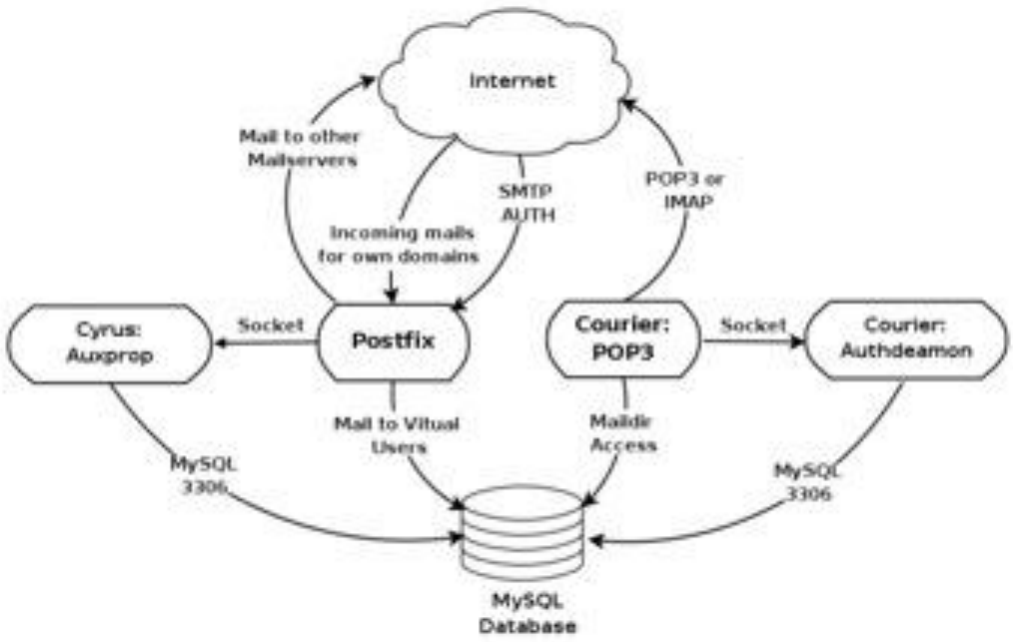
Mail server adalah aplikasi yang digunakan untuk mengirimkan e-mail. Sesuai dengan namanya sever mail yang merupakan pusan kendali e-mail, mail server senantiasa menerima pesan dari e-mail client yang berasal dari client, atau bahkan dari server e-mail lain. Mail server biasanya dikelola oleh seorang yang biasanya dipanggil postmaster. Tugas dari postmaster adalah mengelola account, memonitor kinerja server, dan tugas administratif lainnya.

Proses pengiriman e-mail malalui tahapan yang sedikit panjang. Saat e-mail di kirim, maka e-mail tersebut disimpan pada mail server menjadi satu file berdasarkan tujuan e-mail. File ini berisi informasi sumber dan tujuan, serta dilengkapi tanggal dan waktu pengiriman. Pada saat pengguna membaca e-mail berarti pengguna telah mengakses server e-mail dan membaca file yang tersimpan dalam server yang di tampilkan melalui browser pengguna.

Gambar 3.7 Layanan Surat Elektronik

Pada mail server terdapat dua server yang berbeda yaitu incoming dan outgoing server. Server yang biasa menangani outgoing e-mail adalah server SMTP(Simple Mail Transfer Protocol) pada port 25 sedangkan untuk menangani e-mail adalah POP3(Post Office Protocol) pada port 110. Saat e-mail dikirim maka akan langsung ditangani oleh SMTP server dan akan dikiriM ke SMTP tujuan, baik secara langsung maupun melalui beberapa SMTP server yang ada pada jalur tujuannya. Apabila server terkoneksi ke jaringan maka pesan akan langsung di kirim, tapi apa bila server tidak terkoneksi ke jaringan maka pesan akan dimasukkan ke dalam queue dan di resend setiap 15 menit. Apabila dalam 5 hari server tidak juga terkoneksi jaringan maka akan muncul pemberitahuan undeliver notice ke inbox pengirim.

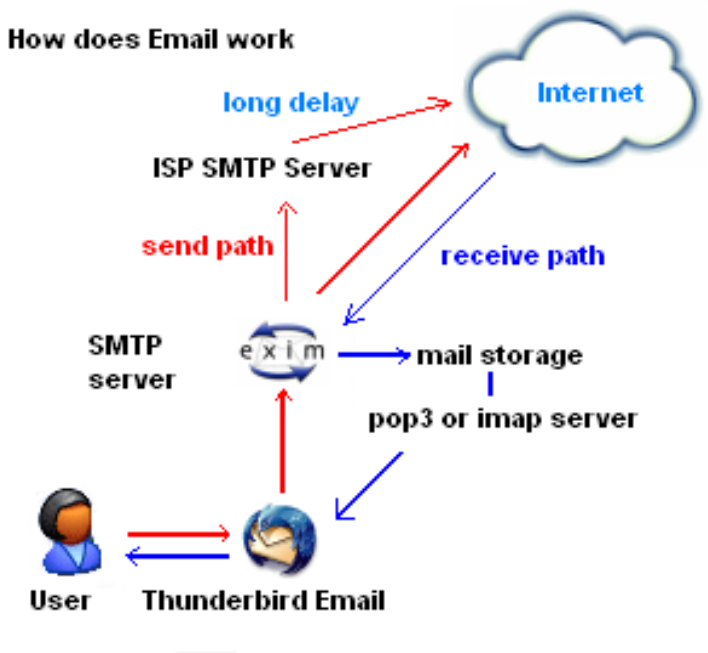
Apabila e-mail terkirim maka akan masuk pada POP3 server atau IMAP server. Jika menggunakan POP3 server pengguna akan membaca file pesan maka komputer pengguna akan mendownload file pesan dari server sehingga file tersebun hanya akan ada pada komputer pengguna tersebut. Sehingga pengguna dapat membaca pesan yang telah di download tersebut. Berbeda dengan IMAP server yang mempertahankan e-mail pada server sehigga e-mail dapat di buka kembali pada device yang berbeda.



Gambar 3.8 Diagram Alur Layanan Surat Elektronik

Simple Mail Transfer Protocol (SMTP)

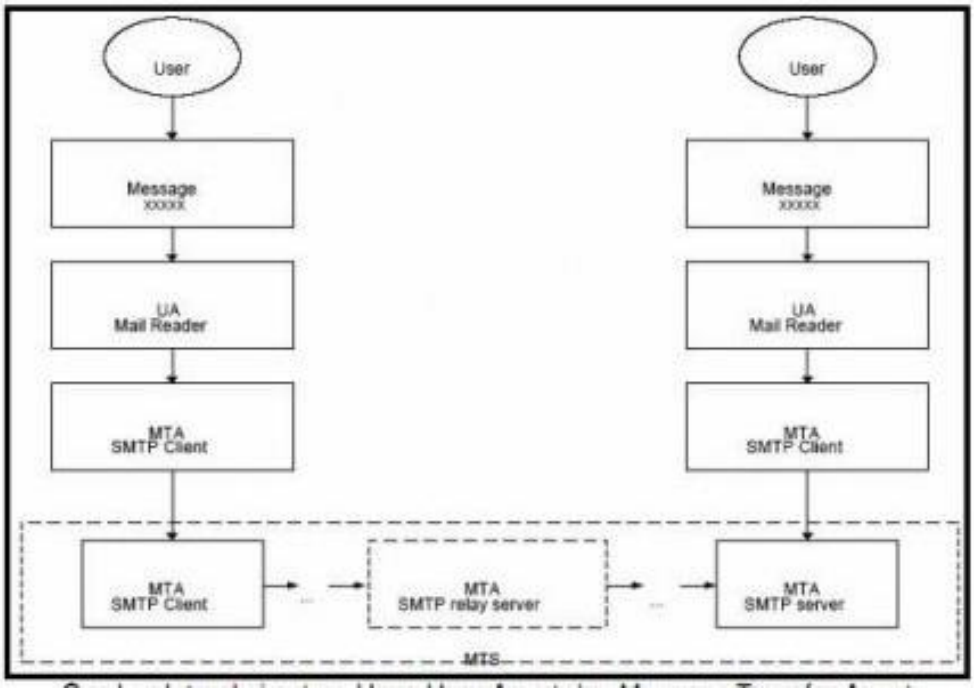
Simple Mail Transfer Protocol (SMTP) adalah suatu standar internet untuk transmisi email melalui Jaringan Internet Protocol (IP). Ketika server surat elektronik dan MTA lain menggunakan SMTP untuk mengirim dan menerima email, aplikasi email client di sisi pengguna, secara umum mneggunakan SMTP hanya untuk mengirim pesan ke sebuah server email untuk dilanjutkan/relaying. Untuk menerima email, aplikasi email client umumnya menggunakan Post Office Protocol (POP) atau Internet Message Access Protocol (IMAP) atau sebuah sistem proprietary (semacam Microsoft Exchange atau Lotus Notes/Domino) untuk mengakses akun kotak email mereka di server mail.



Gambar 3.9 Alur Layanan Surat Elektronik Dengan SMTP

Cara Kerja SMTP

Simple Mail Transfer Protocol (SMTP) didefinisikan dan digunakan dalam Internet untuk mengirimkan electonic mail (E-mail). Cara kerja SMTP mirip yang dilakukan oleh FTP. SMTP menggunakan beberapa spool dan queue. Pesan yang dikirim oleh SMTP akan dikirimkan dalam queue. SMTP akan menghindari membalas pesan dari queue jika dihubungkan ke remote machine. Jika pesan tidak dapat dibalas dengan waktu yang telah ditentukan maka pesan akan dikembalikan ke pengirim atau dipindahkan. Interaksi antara message ke User Agent dan ke Message Transfer Agent hingga diterima oleh Penerima.



Gambar 3.10 Alur Kerja Layanan SMTP

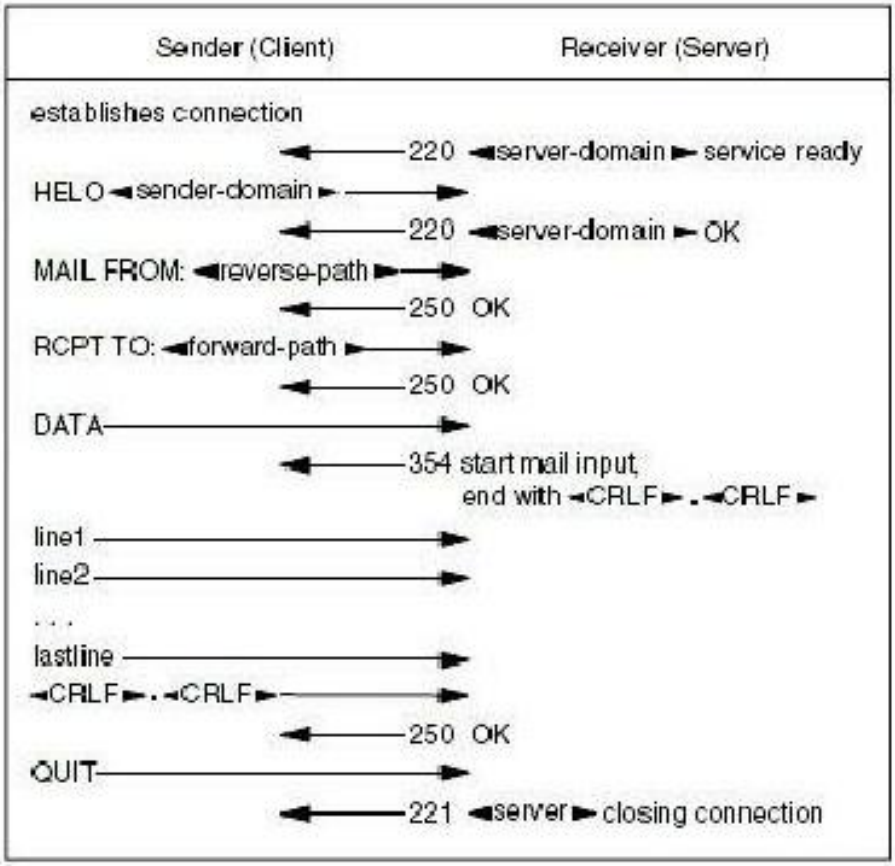
SMTP bekerja berdasarkan pengiriman end-to-end, dimana SMTP client (pengirim) akan menghubungi SMTP server (penerima) untuk segera mengirimkan email. SMTP server melayani pengguna melalui port 25. Dimana setiap pesan yang dikirimkan melaui SMTP harus memiliki :

- Header atau amplop, yang dijabarkan pada RFC 822.

Tabel 3.1 Header Surat Elektronik

Kata kunci	Nilai
to	Tujuan dari email
cc	Tujuan kedua dari email (carbon-copy)
from	Pengirim email
reply-to	Alamat pengembalian email
return-path	Alamat host untuk pengembalian email
Subject	Subjek tentang email yang diisikan oleh pengguna

- Konten atau isi, yang berisi tentang isi dari surat yang akan dikirimkan



Gambar 3.11 Diagram Alir Pertukaran Surat SMTP

1. SMTP Pengirim melakukan koneksi TCP/IP dengan SMTP penerima dan menunggu server untuk mengirim pesan 220 yang menandakan pelayanan terhadap pesan sudah siap atau pesan 421 pelayanan tidak siap.
2. HELO (kependekan dari hello) dikirim oleh server dengan menunjukkan nama domain
3. Pengirim akan memulai memberikan perintah kepada SMTP dimana apabila SMTP mendukung perintah tersebut akan membalas dengan pesan 250 OK
4. Memberikan informasi kepada SMTP tentang tujuan dari email dengan perintah RCPT TO dilanjutkan dengan alamat email yang dituju
5. Setelah tujuan diset, dilanjutkan dengan perintah DATA yang menunjukkan bahwa baris berikutnya adalah isi dari email dengan diakhiri dengan CRLF
6. Client mengisikan data sesuai dengan pesan yang akan dikirimkan hingga mengisikan CRLF kembali untuk menandakan berakhirnya data
7. Pengirimkan akan menghentikan kegiatan dengan memberi perintah QUIT

Post Office Protocol (POP)/ Internet Messages Address Protocol (IMAP)

IMAP adalah satu dari dua protokol standar internet yang paling umum digunakan untuk menerima email. Satu lagi adalah Post Office Protocol (POP). Secara virtual semua klien email modern dan server mail mendukung kedua protokol tersebut sebagai sarana untuk mentransfer pesan surat elektronik dari suatu server.Internet Message Access Protocol (seringkali dikenal sebagai IMAP) adalah Protokol Internet Layer Aplikasi yang email-client dapat mengakses email dari sebuah remote mail server (server mail jarak jauh).

IMAP mendukung mode operasi online maupun offline. email-client yang menggunakan IMAP umumnya meninggalkan pesan di server hingga pengguna jelas-jelas menghapus email tersebut. Karakter ini dan karakter operasi IMAP yang lain memperkenankan banyak klien untuk melakukan manajemen pada inbox yang sama.

Sedikitnya ada 6 perbedaan yang mencolok antara POP3 dan IMAP, yaitu :

- POP (Post Office Protocol) 3
  - Email harus didownload terlebih dahulu sebelum ditampilkan sehingga memiliki beberapa kelemahan seperti : Anda harus mendownload lagi dari awal secara berulang – ulang jika menggunakan komputer yang berbeda.
  - Email yang sudah didownload ke komputer akan terhapus dari server tergantung dari setting Email client. Jika hal ini terjadi, maka saat Anda menggunakan komputer lainnya, Anda tidak bisa lagi membaca semua email anda secara penuh.
  - Semua email dan file attachment akan terdownload secara menyeluruh saat melakukan cek email dari email client.

  - Outgoing Email hanya akan tersimpan secara lokal di komputer (email client).
  - Anda hanya bisa mengatur email di komputer lokal saja. Saat anda menghapus sebuah email, maka hanya email di komputer Anda saja yang terhapus, sedangkan di email server tetap ada dan harus anda hapus secara manual.
  - Butuh waktu yang lama untuk reload email dari email server ke komputer Anda.
- IMAP (Internet Messages Address Protocol)
  - Email masih tersimpan di server email sehingga tidak perlu mendownload semua email dari awal jika diakses menggunakan komputer lain. Perubahan yang dilakukan di komputer satu akan berdampak pada email server dan komputer yang lain tentunya.
  - Sangat mudah dalam mengidentifikasi Email yang belum terbaca.
  - Pesan yang didownload hanya pesan yang anda akses saat itu untuk ditampilkan di komputer remote. Lebih praktis, cepat dan hemat waktu.
  - Outgoing Email bisa tersimpan secara realtime di email server dan bisa diakses oleh komputer manapun yang menggunakan IMAP.
  - Anda bisa mengatur email server dari komputer secara real time. Saat anda mengapus email di komputer remote, maka anda juga telah menghapusnya dari Email server. Sinkronisasi antara server email dan komputer akan selalu terjadi secara otomatis sehingga yang kita akses di komputer adalah kondisi email secara real time yang ada di email server.
  - Waktu reload email jauh lebih cepat dari POP dan sinkronisasi antara email server dan komputer remote akan selalu terjadi secara otomatis saat anda melakukan aktivitas di komputer remote anda.

Dari perbedaan diatas dapat Anda lihat bahwa IMAP jauh lebih baik daripada POP3 dalam melakukan sinkronisi folder dan rule terhadap email server (webmail). Untuk Anda yang menggunakan HP atau smartphone, jelas lebih cocok jika memilih IMAP.

3.1.2.4 Mengasosiasi

Setelah mengikuti kegiatan belajar 3 ini siswa diharapkan dapat menyimpulkan pelbagai hasil percobaan dan pengamatan terkait dengan protocol-protokol pendukung suatu ISP, protocol-protokol lapisan transport, TCP dan UDP, hirarki dan resolusi DNS, layanan HTTP dan HTTPS, layanan FTP, layanan SMTP, POP3 dan IMAP4.

3.1.3 Rangkuman

Sebuah ISP menyediakan layanan koneksi internet kepada pelanggannya. Layanan-layanan ini mencakup :

- Electronic mail

Email istilah Indonesia adalah surat elektronik, adalah aplikasi yang memungkinkan para pengguna internet untuk

saling berkirim pesan melalui alamat elektronik di internet. Para pengguna email memilki sebuah mailbox (kotak surat) elektronik yang tersimpan dalam suatumailserver.

Suatu Mailbox memiliki sebuah alamat sebagai pengenal agar dapat berhubungan dengan mailbox lainnya, baik dalam bentuk penerimaan maupun pengiriman pesan. Pesan yang diterima akan ditampung dalam mailbox, selanjutnya pemilik mailbox sewaktu-waktu dapat mengecek isinya, menjawab pesan, menghapus, atau menyunting dan mengirimkan pesan email.

Layanan email biasanya dikelompokkan dalam dua basis, yaitu email berbasis client dan email berbasis web. Bagi pengguna email berbasis client, aktifitas emailnya dilakukan dengan menggunakan perangkat lunak email client, misalnya Eudora atau Outlook Express.

Perangkat lunak ini menyediakan fungsi-fungsi penyuntingan dan pembacaan email secara offline (tidak tersambung ke internet), dengan demikian, biaya koneksi ke internet dapat dihemat. Koneksi hanya diperlukan untuk melakukan pengiriman (send) atau menerima (recieve) email dari mailbox.

Sebaliknya, bagi pengguna email berbasis web, seluruh kegiatan email harus dilakukan melalui suatu situs web. Dengan demikian, untuk menggunakannya haruslah dalam keadaan online. Alamat email dari ISP (Internet Service Provider) umumnya berbasis client, sedangkan email berbasis web biasanya disediakan oleh penyelenggara layanan email gratis seperti Hotmail (www.hotmail.com) atau YahooMail (mail.yahoo.com).

- File Transfer Protocol

Fasilitas ini memungkinkan para pengguna internet untuk melakukan pengiriman (upload) atau menyalin (download) sebuah file antara komputer lokal dengan komputer lain yang terhubung dalam jaringan internet. Ribuan situs FTP menawarkan banyak file yang dapat di download. File-file yang dapat di download dapat berupa file-file yang berisi game, foto atau gambar-gambar, peta, artikel-artikel, utility-utility program aplikasi dan yang lainnya. Protokol standar yang digunakan untuk keperluan ini disebut sebagai File

Transfer Protocol (FTP). FTP umumnya dimanfaatkan sebagai sarana pendukung untuk kepentingan pertukaran maupun penyebarluasan sebuah file melalui jaringan internet. FTP juga dimanfaatkan untuk melakukan prosesupload suatu halaman web ke webserver agar dapat diakses oleh pengguna internet lainnya.

3.1.4 Tugas

Buatlah kelompok terdiri atas 2-3 orang. Masing-masing kelompok membuat ringkasan tentang layanan-layanan ISP, kemudian secara bergantian masing-masing kelompok mempresentasikan hasilnya di depan kelas.

1. Bacalah uraian materi diatas dengan teliti dan cermat.

2. Buatlah ringkasan materi menggunakan aplikasi pengolah presentasi.
3. Presentasikan hasil ringkasan di depan kelas.

3.1.5 Penilaian Diri

Setelah mengikuti kegiatan belajar 3 ini diharapkan siswa memiliki wawasan pengetahuan dan dapat menjawab pelbagai hal terkait dengan protocol-protokol pendukung suatu ISP, protocol-protokol lapisan transport, TCP dan UDP, hirarki dan resolusi DNS, layanan HTTP dan HTTPS, layanan FTP, layanan SMTP, POP3 dan IMAP4.

BAB IV

4.1 Kegiatan Belajar 4 : Tugas Dan Tanggung Jawab ISP

4.1.1 Tujuan Pembelajaran

Setelah mengikuti kegiatan belajar 4 ini siswa diharapkan dapat memahami tentang tugas dan tanggung jawab ISP.

4.1.2 Aktifitas Belajar Siswa

4.1.2.1 Mengamati

Melalui kegiatan belajar 4 ini siswa diharapkan dapat melakukan pengamatan mengenai :

- Pertimbangan layanan keamanan ISP (enkripsi data)
- Peralatan pengaman pada ISP (ACL, port filtering, firewall, IDS, IPS)
- Monitoring dan pengaturan ISP (Service Level Agreement, SNMP, Syslog) Backup dan recovery (media, file)

4.1.2.2 Menanya

Melalui kegiatan belajar 4 ini siswa diharapkan dapat melakukan :

- Mendiskusikan pertimbangan layanan keamanan ISP (enkripsi data)
- Mendiskusikan peralatan pengaman pada ISP (ACL, port filtering, firewall, IDS, IPS)
- Mendiskusikan monitoring dan pengaturan ISP (SLA, SNMP, Syslog)
- Mendiskusikan backup dan recovery (media, file)

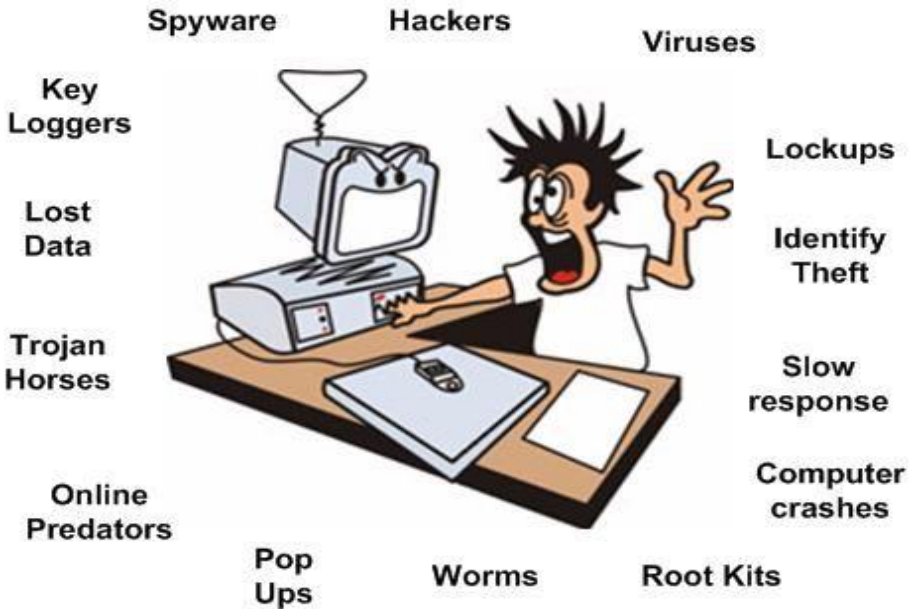
4.1.2.3 Mengumpulkan Informasi

Pertimbangan Layanan Keamanan ISP

Masalah keamanan merupakan salah satu aspek penting dari sebuah sistem informasi. Sayang sekali masalah keamanan ini sering kali kurang mendapat perhatian dari para pemilik dan pengelola sistem informasi. Seringkali masalah keamanan berada di urutan kedua, atau bahkan di urutan terakhir dalam daftar hal-hal yang dianggap penting. Apabila menggangu performansi dari sistem, seringkali keamanan dikurangi atau ditiadakan.

William Stalling (2011) menyatakan bahwa security service adalah sebuah proses atau layanan komunikasi yang disediakan oleh sistem untuk memberikan jenis perlindungan tertentu terhadap sumber daya sistem, layanan keamanan menerapkan kebijakan keamanan dan dilaksanakan oleh mekanisme keamanan.

Garfinkel mengemukakan bahwa keamanan komputer (computer security) melingkupi empat aspek, yaitu privacy, integrity, authentication, dan availability. Selain keempat hal di atas, masih ada dua aspek lain yang juga sering dibahas dalam kaitannya dengan electronic commerce, yaitu access control dan non-repudiation.



Gambar 4.1 Bentuk-bentuk Ancaman Keamanan Jaringan Komputer

- Privacy / Confidentiality

Inti utama aspek privacy atau confidentiality adalah usaha untuk menjaga informasi dari orang yang tidak berhak mengakses. Privacy lebih kearah data-data yang sifatnya privat sedangkan confidentiality biasanya berhubungan dengan data yang diberikan ke pihak lain untuk keperluan tertentu (misalnya sebagai bagian dari pendaftaran sebuah servis) dan hanya diperbolehkan untuk keperluan tertentu tersebut. Contoh hal yang berhubungan dengan privacy adalah e-mail seorang pemakai (user) tidak boleh dibaca oleh administrator. Contoh confidential information adalah data-data yang sifatnya pribadi (seperti nama, tempat tanggal lahir, social security number, agama, status perkawinan, penyakit yang pernah diderita, nomor kartu kredit, dan sebagainya) merupakan data-data yang ingin diproteksi penggunaan dan penyebarannya. Contoh lain dari confidentiality adalah daftar pelanggan dari sebuah Internet Service Provider (ISP).

Untuk mendapatkan kartu kredit, biasanya ditanyakan data-data pribadi. Jika saya mengetahui data-data pribadi anda, termasuk nama ibu anda, maka saya dapat melaporkan melalui telepon (dengan berpura-pura sebagai anda) bahwa kartu kredit anda hilang dan mohon penggunaannya diblokir. Institusi (bank) yang mengeluarkan kartu kredit anda akan percaya bahwa saya adalah anda dan akan menutup kartu kredit anda. Masih banyak lagi kekacauan yang dapat ditimbulkan bila data-data pribadi ini digunakan oleh orang yang tidak berhak.

Confidentiality merupakan aspek yang menjamin kerahasiaan data atau informasi. Sistem yang digunakan untuk mengimplementasikan e-procurement harus dapat menjamin kerahasiaan data yang dikirim, diterima dan disimpan. Bocornya

informasi dapat berakibat batalnya proses pengadaan. Kerahasiaan ini dapat diimplementasikan dengan berbagai cara, seperti misalnya menggunakan teknologi kriptografi dengan melakukan proses enkripsi (penyandian, pengkodean) pada transmisi data, pengolahan data (aplikasi dan database), dan penyimpanan data (storage). Teknologi kriptografi dapat mempersulit pembacaan data tersebut bagi pihak yang tidak berhak.

Seringkali perancang dan implementor dari sistem informasi atau sistem transaksi elektronik lalai dalam menerapkan pengamanan. Umumnya pengamanan ini baru diperhatikan pada tahap akhir saja sehingga pengamanan lebih sulit diintegrasikan dengan sistem yang ada. Penambahan pada tahap akhir ini menyebabkan sistem menjadi tambal sulam. Akibat lain dari hal ini adalah adanya biaya yang lebih mahal daripada jika pengamanan sudah dipikirkan dan diimplementasikan sejak awal. Akses terhadap informasi juga harus dilakukan dengan melalui mekanisme otorisasi (authorization) yang ketat. Tingkat keamanan dari mekanisme otorisasi bergantung kepada tingkat kerahasiaan data yang diinginkan.

- Integrity

Aspek ini menekankan bahwa informasi tidak boleh diubah tanpa seijin pemilik informasi. Adanya virus, trojan horse, atau pemakai lain yang mengubah informasi tanpa ijin merupakan contoh masalah yang harus dihadapi. Sebuah e-mail dapat saja “ditangkap” (intercept) di tengah jalan, diubah isinya (altered, tampered, modified), kemudian diteruskan ke alamat yang dituju. Dengan kata lain, integritas dari informasi sudah tidak terjaga. Penggunaan enkripsi dan digital signature, misalnya, dapat mengatasi masalah ini.

Salah satu contoh kasus trojan horse adalah distribusi paket program TCP Wrapper (yaitu program populer yang dapat digunakan untuk mengatur dan membatasi akses TCP/IP) yang dimodifikasi oleh orang yang tidak bertanggung jawab. Jika anda memasang program yang berisi trojan horse tersebut, maka ketika anda merakit (compile) program tersebut, dia akan mengirimkan eMail kepada orang tertentu yang kemudian memperbolehkan dia masuk ke sistem anda. Informasi ini berasal dari CERT Advisory, “CA- 99-01 Trojan-TCP-Wrappers” yang didistribusikan 21 Januari 1999. Contoh serangan lain adalah yang disebut “man in the middle attack” dimana seseorang menempatkan diri di tengah pembicaraan dan menyamar sebagai orang lain.

Integrity merupakan aspek yang menjamin bahwa data tidak boleh berubah tanpa ijin pihak yang berwenang (authorized). Aspek ini menekankan bahwa informasi tidak boleh diubah tanpa seijin pemilik informasi. Adanya virus, trojan horse, atau pemakai lain yang mengubah informasi tanpa ijin merupakan contoh masalah yang harus dihadapi. Sebuah e-mail dapat saja “ditangkap” (intercept) di tengah jalan, diubah isinya (altered, tampered, modified), kemudian diteruskan ke alamat yang dituju. Dengan kata lain, integritas dari informasi

sudah tidak terjaga. Penggunaan enkripsi dan digital signature, misalnya, dapat mengatasi masalah ini.

Untuk aplikasi e-procurement, aspek integrity ini sangat penting. Data yang telah dikirimkan tidak dapat diubah oleh pihak yang berwenang. Pelanggaran terhadap hal ini akan berakibat tidak berfungsinya sistem e-procurement. Secara teknis ada banyak cara untuk menjamin aspek integrity ini, seperi misalnya dengan menggunakan messange authentication code, hash function, digital signature.

- Authentication

Aspek ini berhubungan dengan metoda untuk menyatakan bahwa informasi betul-betul asli, orang yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud, atau server yang kita hubungi adalah betul-betul server yang asli.

Masalah pertama, membuktikan keaslian dokumen, dapat dilakukan dengan teknologi watermarking dan digital signature. Watermarking juga dapat digunakan untuk menjaga “intelectual property”, yaitu dengan menandai dokumen atau hasil karya dengan “tanda tangan” pembuat. Masalah kedua biasanya berhubungan dengan access control, yaitu berkaitan dengan pembatasan orang yang dapat mengakses informasi. Dalam hal ini pengguna harus menunjukkan bukti bahwa memang dia adalah pengguna yang sah, misalnya dengan menggunakan password, biometric (ciri-ciri khas orang), dan sejenisnya.

Ada tiga hal yang dapat ditanyakan kepada orang untuk menguji siapa dia:

- Dengan apa yang dimilikinya (What you have, misalnya kartu ATM)
- Dengan apa yang diketahuinya (What you know, misalnya PIN atau password)
- Dengan apa yang ada padanya (What you are, misalnya sidik jari atau biometric)

Penggunaan teknologi smart card, saat ini kelihatannya dapat meningkatkan keamanan aspek ini. Secara umum, proteksi authentication dapat menggunakan digital certificates. Authentication biasanya diarahkan kepada orang (pengguna), namun tidak pernah ditujukan kepada server atau mesin. Pernahkan kita bertanya bahwa mesin ATM yang sedang kita gunakan memang benar-benar milik bank yang bersangkutan? Bagaimana jika ada orang nakal yang membuat mesin seperti ATM sebuah bank dan meletakkannya di tempat umum? Dia dapat menyadap data-data (informasi yang ada di magnetic strip) dan PIN dari orang yang tertipu. Memang membuat mesin ATM palsu tidak mudah. Tapi, bisa anda bayangkan betapa mudahnya membuat web site palsu yang menyamar sebagai web site sebuah bank yang memberikan layanan Internet Banking. (Contoh kasus adalah klikBCA.com.)

- Availability

Aspek availability atau ketersediaan berhubungan dengan ketersediaan informasi ketika dibutuhkan. Sistem informasi yang diserang atau dijebol dapat menghambat atau meniadakan akses ke informasi. Contoh hambatan adalah serangan yang sering disebut dengan “denial of service attack”

(DoS attack), dimana server dikirimi permintaan (biasanya palsu) yang bertubi-tubi atau permintaan yang diluar perkiraan sehingga tidak dapat melayani permintaan lain atau bahkan sampai down, hang, crash. Contoh lain adalah adanya mailbomb, dimana seorang pemakai dikirimi e-mail bertubi-tubi (katakan ribuan e-mail) dengan ukuran yang besar sehingga sang pemakai tidak dapat membuka e-mailnya atau kesulitan mengakses e-mailnya (apalagi jika akses dilakukan melalui saluran telepon). Bayangkan apabila anda dikirimi 5000 email dan anda harus mengambil (download) email tersebut melalui telepon dari rumah.

Availability merupakan aspek yang menjamin bahwa data tersedia ketika dibutuhkan. Dapat dibayangkan efek yang terjadi ketika proses penawaran sedang dilangsungkan ternyata sistem tidak dapat diakses sehingga penawaran tidak dapat diterima. Ada kemungkinan pihak-pihak yang dirugikan karena tidak dapat mengirimkan penawaran, misalnya. Hilangnya layanan dapat disebabkan oleh berbagai hal, mulai dari benca alam (kebakaran, banjir, gempa bumi), ke kesalahan sistem (server rusak, disk rusak, jaringan putus), sampai ke upaya pengrusakan yang dilakukan secara sadar (attack). Pengamanan terhadap ancaman ini dapat dilakukan dengan menggunakan sistem backup dan menyediakan disaster recovery center (DRC) yang dilengkapi dengan panduan untuk melakukan pemulihan (disaster recovery plan).

- Access Control

  Aspek ini berhubungan dengan cara pengaturan akses kepada informasi. Hal ini biasanya berhubungan dengan klasifikasi data (public, private, confidential, top secret) & user (guest, admin, top manager, dsb.), mekanisme authentication dan juga privacy. Access control seringkali dilakukan dengan menggunakan kombinasi userid/password atau dengan menggunakan mekanisme lain (seperti kartu, biometrics).

- Non-repudiation

  Aspek ini menjaga agar seseorang tidak dapat menyangkal telah melakukan sebuah transaksi. Sebagai contoh, seseorang yang mengirimkan email untuk memesan barang tidak dapat menyangkal bahwa dia telah mengirimkan email tersebut. Aspek ini sangat penting dalam hal electronic commerce. Penggunaan digital signature, certifiates, dan teknologi kriptografi secara umum dapat menjaga aspek ini. Akan tetapi hal ini masih harus didukung oleh hukum sehingga status dari digital signature itu jelas legal. Hal ini akan dibahas lebih rinci pada bagian tersendiri.

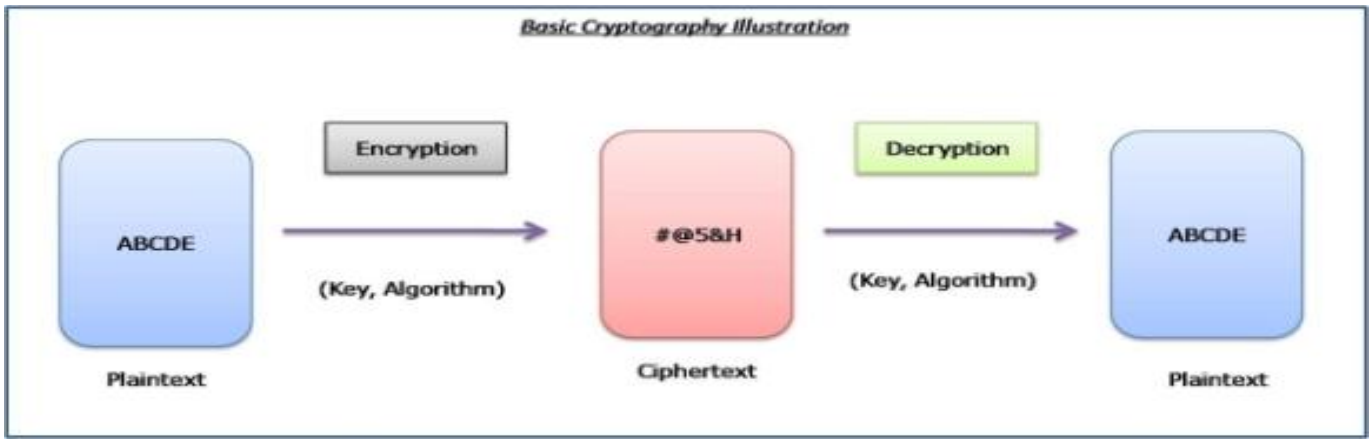
- Enkripsi Data

Di bidang kriptografi, enkripsi adalah proses mengamankan suatu informasi dengan membuat informasi tersebut tidak dapat dibaca tanpa bantuan pengetahuan khusus. Dikarenakan enkripsi telah digunakan untuk mengamankan komunikasi di berbagai negara, hanya organisasi-organisasi tertentu dan individu yang memiliki kepentingan yang sangat mendesak akan kerahasiaan yang menggunakan enkripsi. Di pertengahan tahun 1970-an, enkripsi kuat

dimanfaatkan untuk pengamanan oleh sekretariat agen pemerintah Amerika Serikat pada domain publik, dan saat ini enkripsi telah digunakan pada sistem secara luas, Sebuah cipher adalah sebuah algoritma

seperti Internet e-commerce, jaringan Telepon bergerak dan ATM pada bank.

dengan cipher. Berdasar pada diskusi secara



Gambar 4.2 Proses Enkripsi-Dekripsi

untuk menampilkan enkripsi dan kebalikannya dekripsi, serangkaian langkah yang terdefinisi yang diikuti sebagai prosedur. Alternatif lain ialah encipherment. Informasi yang asli disebut sebagai plaintext, dan bentuk yang sudah dienkripsi disebut sebagai chiphertext. Pesan chipertext berisi seluruh informasi dari pesan plaintext, tetapi tidak dalam format yang didapat dibaca manusia ataupun komputer tanpa menggunakan mekasnisme yang tepat untuk melakukan dekripsi. Cipher pada biasanya memiliki parameter dari sebagian dari informasi utama, disebut sebagai kunci. Prosedur enkripsi sangat bervariasi tergantung pada kunci yang akan mengubah rincian dari operasi algoritma. Tanpa menggunakan kunci, chiper tidak dapat digunakan untuk dienkirpsi ataupun didekripsi.

Pada penggunaan non teknis, sebuah secret code merupakan hal yang sama

teknis, bagaimanapun juga, code dan cipher dijelaskan dengan dua konsep. Code bekerja

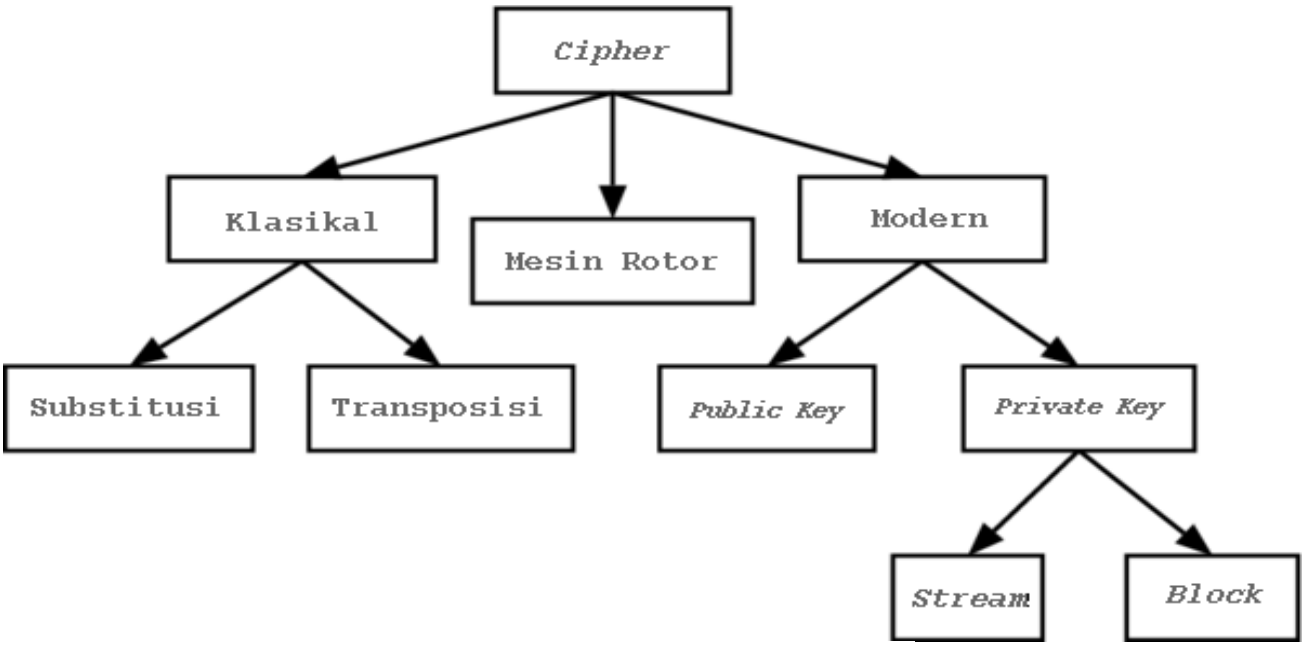
pada tingkat pemahaman, yaitu, kata atau frasa diubah menjadi sesuatu yang lain. Cipher, dilain pihak, bekerja pada tingkat yang lebih rendah, yaitu, pada tingkat masing-masing huruf, sekelompok huruf, pada skema yang modern, pada tiap-tiap bit. Beberapa sistem menggunakan baik code dan cipher dalam sistem yang sama, menggunakan superencipherment untuk meningkatkan keamanan.

Menurut sejarahnya, kriptografi dipisah menjadi dikotomi code dan cipher, dan penggunaan code memiliki terminologi sendiri, hal yang sama pun juga terjadi pada cipher: "encoding, codetext, decoding" dan lain sebagainya. Bagaimanapun juga, code

memiliki berbagai macam cara untuk dikembalikan, termasuk kerapuhan terhadap kriptoanalisis dan kesulitan untuk mengatur daftar kode yang susah. Oleh karena itu, code tidak lagi digunakan pada kriptografi modern, dan cipher menjadi teknik yang lebih dominan.

Ada banyak sekali variasi pada tipe enkripsi yang berbeda. Algoritma yang digunakan pada awal sejarah kriptografi sudah sangat berbeda dengan metode modern, dan cipher modern dan diklasifikasikan berdasar pada bagaimana cipher tersebut beroperasi dan cipher tersebut menggunakan sebuah atau dua buah kunci. Sejarah Cipher pena dan kertas pada waktu lampau sering disebut sebagai cipher klasik. Cipher klasik termasuk juga cipher pengganti dan cipher transposisi. Pada awal abad 20, mesin-mesin yang lebih mutakhir digunakan untuk kepentingan enkripsi, mesin rotor, merupkan skema awal yang lebih kompleks.

Metode enkripsi dibagi menjadi algoritma symmetric key dan algoritma asymmetric key. pada algoritma symmetric key (misalkan, DES dan AES), pengirim dan penerima harus memiliki kunci yang digunakan bersama dan dijaga kerahasiaanya. Pengirim menggunkan kunci ini untuk enkripsi dan penerima menggunakan kunci yang sama untuk dekripsi. Pada algoritma asymmetric key (misalkan, RSA), terdapat dua kunci terpisah, sebuah public key diterbitkan dan membolehkan siapapun pengirimnya untuk melakukan enkripsi, sedangkan sebuah private key dijaga kerahasiannya oleh penerima dan digunakan untuk melakukan dekripsi. Cipher symmetric key dapat dibedakan dalam dua tipe, tergantung pada bagaimana cipher tersebut bekerja pada blok simbol pada ukuran yang tetap (block ciphers), atau pada aliran simbol terus-menerus (stream ciphers).



Gambar 4.3 Macam-macam Cipher

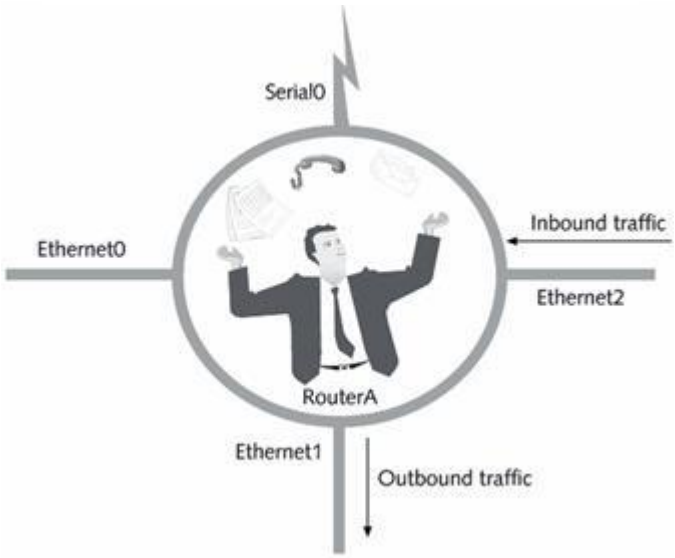
Peralatan Pengaman Pada ISP

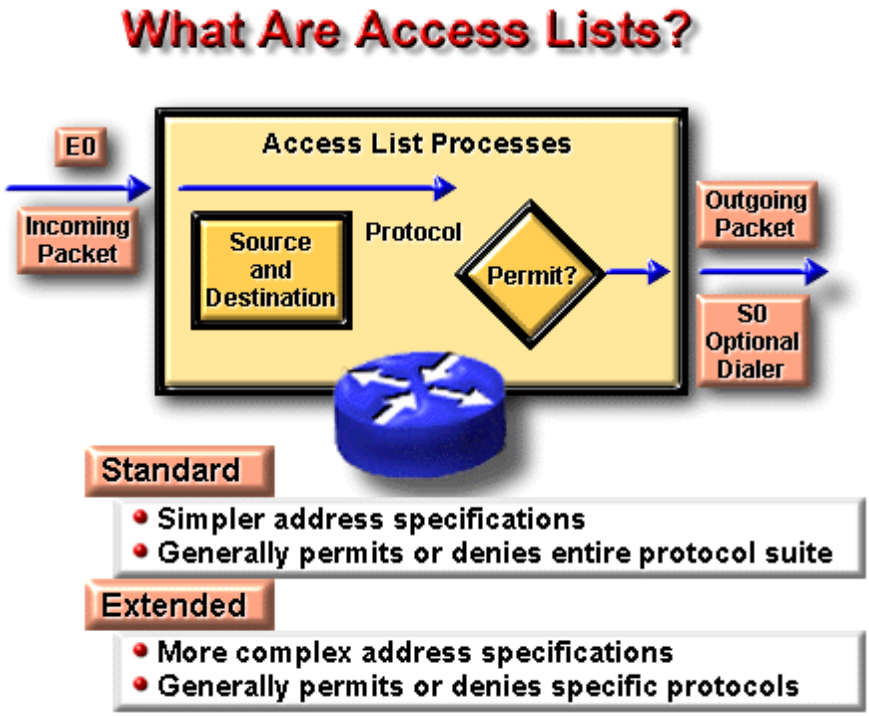
- ACL

Access Control List adalah pengelompokan paket berdasarkan kategori. Access Control list bisa sangat membantu ketika membutuhkan pengontrolan dalam lalu lintas network. Access Control list menjadi tools pilihan untuk pengambilan keputusan pada situasi ini. Penggunaan Access Control List yang paling muda dimengerti dan yang paling umum terdapat pada penyaringan paket yang tidak dikehendaki ketika menerapakan kebijakan keamanan.

Sebagai contoh kita dapat mengatur access list untuk membuat keputusan yang sangat spesifik tentang peraturan pola lalu lintas sehingga access list hanya memperbolehkan host tertentu mengakses sumber daya WWW sementara yang lainnya ditolak. Dengan kombinasi access list yang benar, network manajer mempunyai kekuasaan untuk memaksa hamper semua kebijakan keamananyang bisa mereka ciptakan. Access list juga bisa digunakan pada situasi lain yang tidak harus meliputi penolakan paket.

Gambar 4.4 Analogi Access Control List (ACL)





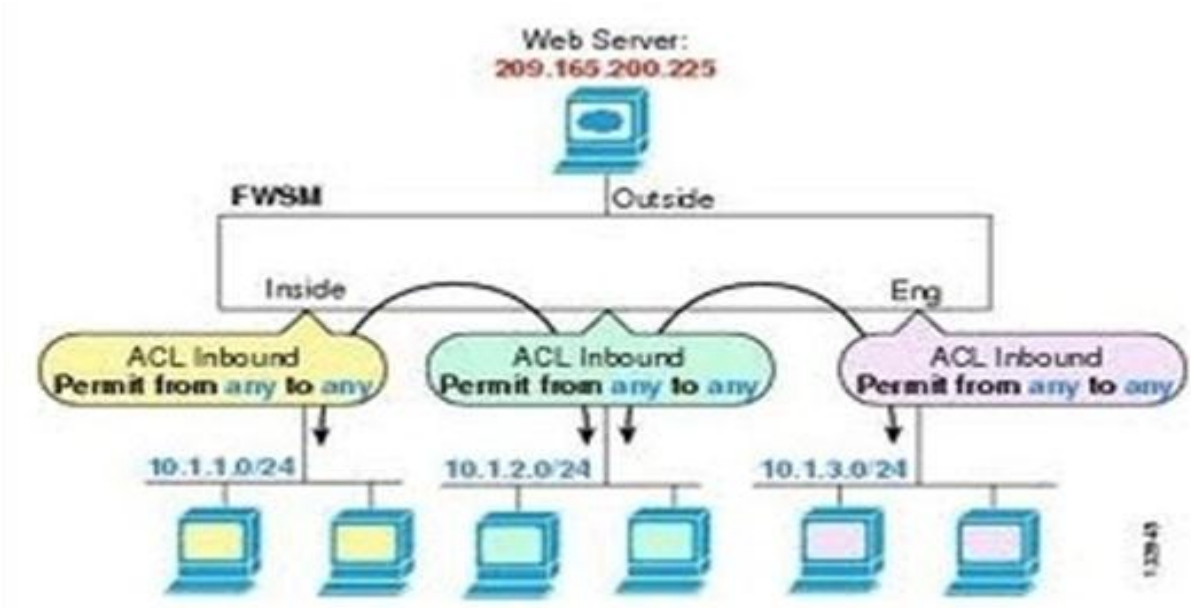
Gambar 4.5 Diagram Fungsi ACL

Membuat access list sangat mirip dengan statement pada programming if – then jika sebuah kondisi terpenuhi maka aksi yang diberikan akan dijalankantidak terpenuhi, tidak ada yang terjadi dan statemen berikutnya akan dievaluasi. Statement ACL pada dasarnaya dalah paket filter dimana paket dibandingkan, dimana paket dikategorikan dan dimana suatu tindakan terhadap paket dilakukan.

List(daftar) yang telah dibuat bisa diterpakan baik kepada lalulintas inbound maupun outbound pada interface mana saja. Menerapkan ACL menyebabkan router menganalisa setiap paket arah spesifik yang melalui interface tersebut dan mengmbil tindakan yang sesuai.

Ketika paket dibandingkan dengan ACL, terdapat beberapa peraturan (rule) penting yang diikuti:

– Paket selalu dibandingkan dengan setiap baris dari ACL secara berurutan, sebagai contoh paket dibandingkan dengan baris pertama dari ACL, kemudian baris kedua, ketiga, dan seterusnya.
– Paket hanya dibandingkan baris-baris ACL sampai terjadi kecocokan. Ketika paket cocok dengan kondisi pada baris ACL, paket akan ditindaklanjuti dan tidak ada lagi kelanjutan perbandingan.
– Terdapat statement “tolak” yang tersembunyi (impilicit deny) pada setiap akhir baris ACL, ini artinya bila suatu paket tidak cocok dengan semua baris kondisi pada ACL, paket tersebut akan ditolak.



Gambar 4.5 Access Control List (ACL)

Jenis ACL

- Standard ACL

Standard ACL hanya menggunakan alamat sumber IP di dalam paket IP sebagai kondisi yang ditest. Semua keputusan dibuat berdasarkan alamat IP sumber. Ini artinya, standard ACL pada dasarnya melewatkan atau menolak seluruh paket protocol. ACL ini tidak membedakan tipe dari lalu lintas IP seperti WWW, telnet, UDP, DSP.

Standard IP ACL memfilter lalu lintas network dengan menguji alamat sumber IP didalam paket. Kita membuat standard IP ACL dengan menggunakan nomor ACL 1-99 atau 1300-1999(expanded range).Tipe ACL pada ummnya dibedakan berdasarkan nomor yang digunakan ketika ACL dibuat, router akan mengetahui tipe syntax yang diharapkan untuk memesukkan daftar. Dengan menggunakan nomor 1-99 atau 1300-1999, kita memberitahukan kepada router bahwa kita ingin membuat IPACL, jadi router akan mengharapkan syntax yang hana menspesifikasikan alamat sumber IP pada baris pengujian. Banyak range nomor ACL pada contoh dibawah ini yang bisa kita gunakan untuk memfilter lalu lintas pada jaringan kita (protocol yang bisa kita terapkan ACL bisa tergantung pada versi IOS kita) :

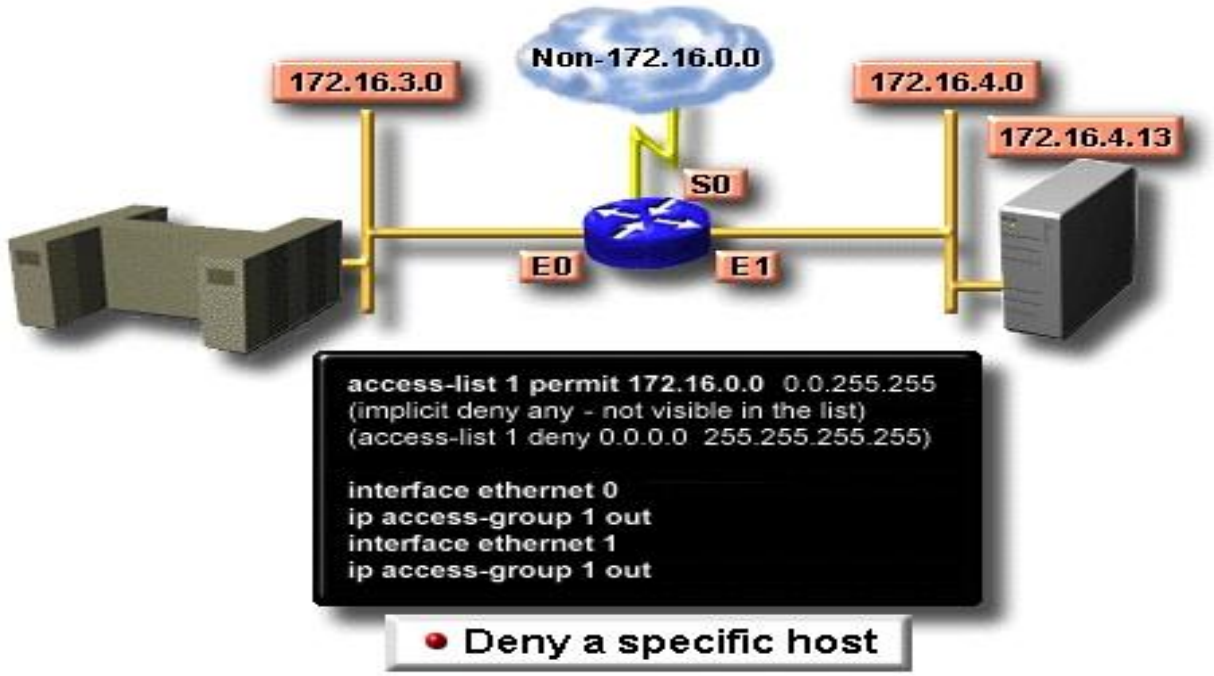
Tabel 4.1 Daftar Jangkauan Nomor ACL Sesuai Protokol

Protocol	Range
IP	1-99, 1300-1999
Extended IP	100-199, 2000-2699
Ethernet type code	200-299
Ethernet address	700-799
Transparent bridging (protocol type)	200-299
Transparent bridging (vendor code)	700-799
Extended transparent bridging	1100-1199
DECnet and extended DECnet	300-399
XNS	400-499
Extended XNS	500-599
AppleTalk	600-699
Source-route bridging (protocol type)	200-299
Source-route bridging (vendor code)	700-799
IPX	800-899
Extended IPX	900-999
IPX SAP	1000-1099
Standard VINES	1-100
Extended VINES	101-200
Simple VINES	201-300

Software Cisco IOS dapat memprovide pesan logging tentang paket – paket. Yang diijinkan atau ditolak oleh standard IP access list. Itulah sebabnya beberapa paket dapat cocok dengan access list.yang disebabkan oleh informasi pesan logging.tentang paket yang telah dikirimkan ke console. Level dari pesan logging ke console yang dikendalikan oleh perintah logging console.Kemampuan ini hanya terdapet pada extended IP access lists.

Triggers paket pertama access list menyebabkan logging message yang benar, dan paket – paket berikutnya yang dikunpulkan lebih dari interval 5-menit sebelum ditampilkan. Pesan logging meliputi nomor access list, apakah paket tersebut diterima atau ditolak, alamat IP sumber dari paket dan nomor asal paket yang diterima sumber atau ditolak dalam interval 5 menit.

Keuntungannya adalah dapat memantau berapa banyak paket yang diijinkan atau ditolak oleh access list khusus termasuk alamat tujuan setiap paket.

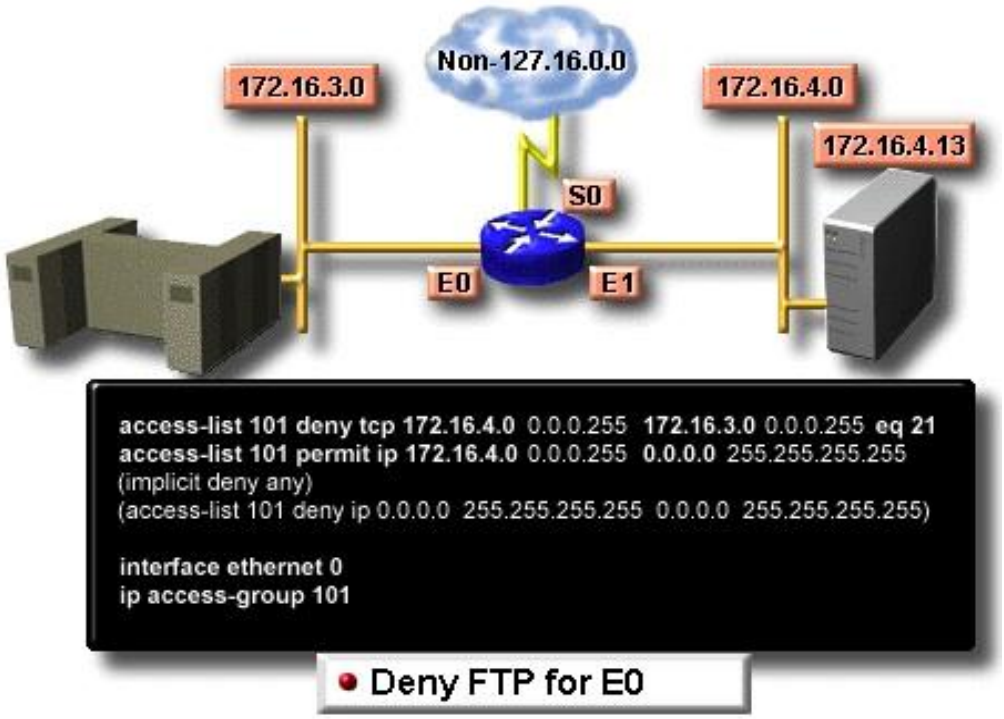


Gambar 4.6 Contoh Standar ACL

- Extended ACL

Extended ACL bisa mengevaluasi banyak field lain pada header layer 3 dan layer 4 pada paket IP. ACL ini bisa mengevaluasi IP sumber dan tujuan, field protocol dalam network header Network Layer dan nomor port pada Transport Layer. Ini memberikan extended ACL kemampuan untuk membuat keputusan – keputusan lebih spesifik ketika mengontrol lalu lintas. Pada contoh Standard ACL, perhatikan bagaimana kita harus memblok semua akses dari LAN Sales ke Department Finance. Bagaimana jika untuk urusan keamanan, kita membutuhkan Sales mendapatkan akses ke server tertentu pada LAN Finance tapi tidak ke layanan network lainnya ? Dengan standard IP ACl, kita tidak memperbolehkan user mendapat satu layanan sementara tidak untuk yang lainnya. Dengan kata lain, ketika kita membutuhkan membuat keputusan berdasarkan alamat sumber dan tujuan, standard ACL tidak memperbolehkan kita melakukannya karena ACL ini hanya mambuta kaputusan berdasrkan alamat sumber. Tetapi extended ACl akan membantu kita karena extended ACL memperbolehkan kita menentukan alamat sumber dan tujuan serta protocol dan nomor port yang mengidentfikasikan protocol upper layer atau aplikasi. Dengan menggunakan extended ACL kita bisa secara efisien memperbolehkan user mengakses ke fisik LAN dan menghentikan host tertentu atau bahkan layanan tertentu pada host tertentu. Hukum dalam pembuatan Access List, yaitu :

– Daftar aplikasi router secara berurutan menunjukan apa yang ditulis ke daalm router.
– Daftar aplikasi router untuk paket yang berurutan.
– Packet akan diproses jika cocok dan berdasarkan criteria access list termasuk pernyataan access list.
– Semua paket yang tidak memenuhi syarat dari acces list akan di blok oleh perintah permit any yang digunakan pada akhir list.
– Hanya satu list, per protocol, per perintah yang dapat diaplikasikan pada interface.
– Kita tidak dapat memindahkan satu baris dari access list.
– Access list akan efektif segera setelah diaplikasikan.



Gambar 4.7 Contoh Extended ACL

Jenis Lalu Lintas ACL

- Inbound ACL

Ketika sebauah ACL diterapkan pada paket inbound di sebuah interface, paket tersebut diproses melalui ACL sebelum di-route ke outbound interface. Setiap paket yang ditolak tidak bisa di-route karena paket ini diabaikan sebelum proses routing diabaikan.

- Outbond ACL

  Ketika sebuah ACL diterapkan pada paket outbound pada sebuah interface, paket tersebut di-route ke outbound interface dan diproses

Terdapat beberapa panduan umum ACL yang seharusnya diikuti ketika membuat dan mengimplementasikan ACL pada router :

- Hanya bisa menerapkan satu ACL untuk setiap interface, setiap protocol dan setiap arah. Artinya bahwa ketika membuat ACL IP, hanya bisa membuat sebuah inbound ACL dan satu Outbound ACL untuk setiap interface.
- Organisasikan ACL sehingga test yang lebih spesifik diletakkan pada bagian atas ACL
- Setiap kali terjadi penambahan entry baru pada ACL, entry tersebut akan diletakkan pada bagian bawah ACL. Sangat disarankan menggunakan text editor dalam menggunakan ACL
- Tidak bisa membuang satu baris dari ACL. Jika kita mencoba demikian, kita akan membuang seluruh ACL. Sangat baik untuk mengcopy ACL ke text editor sebelum mencoba mengubah list tersebut.

- Packet Filtering

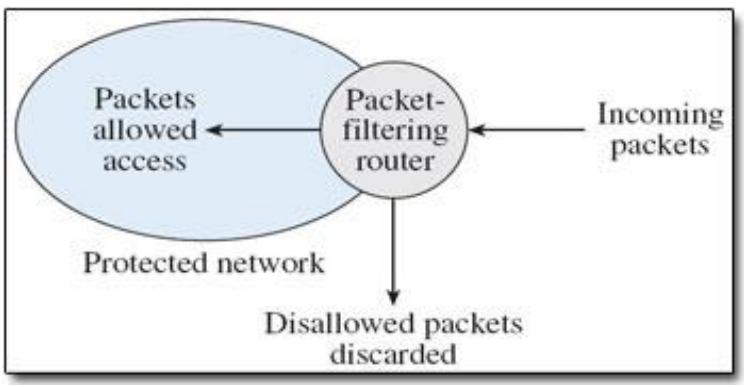
Sistem pada paket filtering merupakan sistem yang digunakan untuk mengontrol keluar, masuknya paket dari antara host yang didalam dan host yang yang diluar tetapi sistem ini melakukannya secara selektif. Sistem ini dapat memberikan jalan atau menghalangi paket yang dikirimkan, sistem ini sangat mengkitalkan arsitektur yang disebut dengan ‘Screened Router’. Router ini menjadi filter dengan menganalisa bagian kepala dari setiap paket yang dikirimkan. Karena bagian kepala dari paket ini berisikan informasi penting yaitu :

- IP source address.
- IP destination address.
- Protocol (dengan melihat apakah paket tersebut berbentuk TCP, UDP atau ICMP).
- Port sumber dari TCP atau UDP.
- Port tujuan dari TCP atau UDP.
- Tipe pesan dari ICMP.
- Ukuran dari paket

Cara Kerja Sistem Packet Filtering ini adalah mengawasi secara individual dengan melihat melalui router, sedangkan router yang telah dimaksud adalah sebuah perangkat keras yang dapat berfungsi sebagai sebuah server karena alat ini harus membuat keputusan untuk me-rout seluruh paket yang diterima. Alat ini juga harus menentukan seperti apakah pengiriman paket yang telah didapat itu kepada tujuan yang sebenarnya. Protokol yang dimaksudkan adalah Routing Information Protocol (RIP) atau Open Shortest Path First (OSPF) yang menghasilkan sebuah table routing. Tabel routing itu menunjukkan kemana tujuan dari paket yang diterima. Router yang menjadi filter pada packet filtering dapat menyediakan sebuah choke point (sebuah channel yang sempit yang sering digunakan untuk dipakai oleh penyerang sistem dan tentu saja dapat dipantau juga dikontrol oleh kita) untuk semua pengguna yang memasuki dan meninggalkan network. Karena sistem ini beroperasi ditingkat Network Layer dan Transport Layer dari tingkatan protokol pada tingkatan pada Transmission Control Protocol (TCP/IP). Bagian kepala dari

network dan transport mengawasi informasi-informasi berikut:

- Protokol (IP header, pada network layer); didalamnya byte 9 mengidentifikasikan protokol dari paket.
- Source address (IP header, pada network layer); alamat sumber merupakan alamat IP 32 bit dari host yang menciptakan oleh paket.
- Destination address (IP header, pada network layer); alamat tujuan yang berukuran 32 bit dari host yang menjadi tujuan dari paket.
- Source port (TCP atau UDP header, pada transport layer); pada setiap akhir dari koneksi TCP atau UDP tersambung dengan sebuah port, Walaupun port-port TCP terpisah dan cukup jauh dari port-port user datagram protocol (UDP). Port-port yang mempunyai nomor dibawah 1024 diterbalikan karena nomor-nomor ini telah didefinisikan secar khusus, sedangkan untuk port-port yang bernomor diatas 1024 (inklusif) lebih dikenal dengan port ephermal. Konfigurasi dari nomor pengalamatan ini diberikan sesuai dengan pilihan dari vendor.
- Destination port (TCP atau UDP header, transp ort layer); nomor port dari tujuan mengindikasikan port yang dikirimi paket. Servis yang akan diberikan pada sebuah host dengan mendengarkan port. Adapun port yang difilter adalah 20/TCP dan 21/TCP untuk koneksi ftp atau data, 23/TCP untuk telnet, 80/TCP untuk http dan 53/TCP untuk zona transfer DNS.
- Connection status (TCP atau UDP header, transport layer); status dari koneksi memberitahukan apakah paket yang dikirim merupakan paket pertama dari sesi di network. Jika paket merupakan paket pertama maka pada TCP header diberlakukan ‘false’ atau 0 dan untuk mencegah sebuah host untuk mengadakan ko neksi dengan menolak atau membuang paket yang mempunyai bit set ‘false’ atau 0.



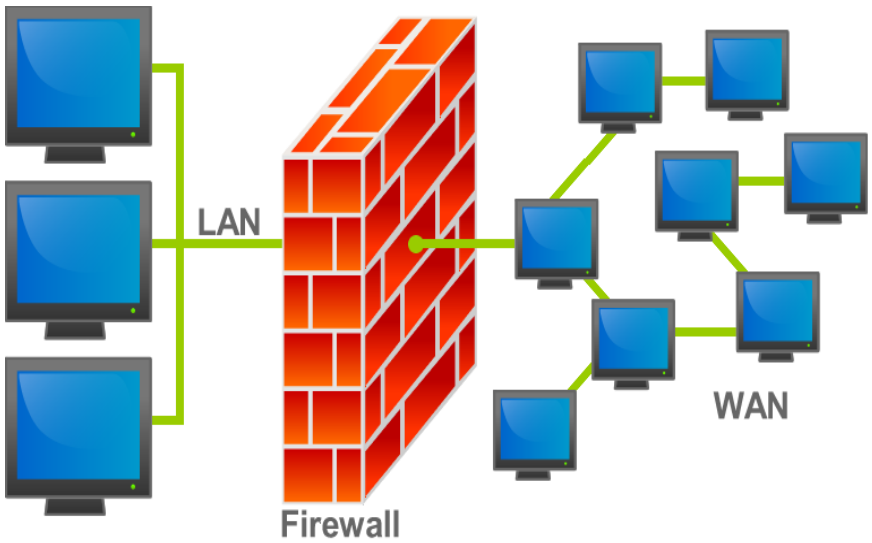
Gambar 4.8 Skema Kerja Packet Filtering

- Firewall

Tembok api atau dinding api adalah suatu sistem perangkat lunak yang mengizinkan lalu lintas jaringan yang dianggap aman untuk bisa melaluinya dan mencegah lalu lintas jaringan yang dianggap tidak aman. Umumnya, sebuah tembok-api diterapkan dalam sebuah mesin terdedikasi, yang berjalan pada pintu gerbang (gateway) antara jaringan lokal dengan jaringan Internet.

Tembok-api digunakan untuk jaringan pribadi dari pihak luar. Saat ini, istilah firewall menjadi istilah lazim yang merujuk pada sistem yang mengatur komunikasi antar dua macam jaringan yang berbeda. Mengingat saat ini banyak perusahaan yang memiliki akses ke Internet dan juga tentu saja jaringan berbadan hukum di dalamnya, maka perlindungan terhadap perangkat digital perusahaan tersebut dari serangan para peretas, pemata-mata, ataupun pencuri data lainnya, menjadi kenyataan.

Gambar 4.10 Ilustrasi Firewall Antara Jaringan Privat Dan Jaringan Publik



Gambar 4.9 Ilustrasi Firewall Antara Jaringan LAN Dan WAN

Secara mendasar, firewall dapat melakukan hal-hal berikut:

– Mengatur dan mengontrol lalu lintas jaringan

Fungsi pertama yang dapat dilakukan oleh firewall adalah firewall harus dapat mengatur dan mengontrol lalu lintas jaringan yang diizinkan untuk mengakses jaringan privat atau komputer yang dilindungi oleh firewall. Firewall melakukan hal yang demikian, dengan melakukan inspeksi terhadap paket-paket dan memantau koneksi yang sedang dibuat, lalu melakukan penapisan (filtering) terhadap koneksi berdasarkan hasil inspeksi paket dan koneksi tersebut.

Inspeksi paket ('packet inspection) merupakan proses yang dilakukan oleh firewall untuk 'menghadang' dan memproses data dalam sebuah paket untuk menentukan bahwa paket tersebut diizinkan atau ditolak, berdasarkan kebijakan akses (access policy) yang diterapkan oleh seorang administrator. Firewall, sebelum menentukan keputusan apakah hendak menolak atau menerima komunikasi dari luar, ia harus melakukan inspeksi terhadap setiap paket (baik yang masuk ataupun yang keluar) di setiap antarmuka dan membandingkannya dengan daftar kebijakan akses. Inspeksi paket dapat dilakukan dengan melihat elemen-elemen berikut, ketika menentukan apakah hendak menolak atau menerima komunikasi:

- Alamat IP dari komputer sumber
- Port sumber pada komputer sumber
- Alamat IP dari komputer tujuan
- Port tujuan data pada komputer tujuan
- Protokol IP
- Informasi header-header yang disimpan dalam paket

Agar dua host TCP/IP dapat saling berkomunikasi, mereka harus saling membuat koneksi antara satu dengan lainnya. Koneksi ini memiliki dua tujuan:

- Komputer dapat menggunakan koneksi tersebut untuk mengidentifikasikan dirinya kepada komputer lain, yang meyakinkan bahwa sistem lain yang tidak membuat koneksi tidak dapat mengirimkan data ke komputer tersebut. Firewall juga dapat menggunakan informasi koneksi untuk menentukan koneksi apa yang diizinkan oleh kebijakan akses dan menggunakannya untuk menentukan apakah paket data tersebut akan diterima atau ditolak.
- Koneksi digunakan untuk menentukan bagaimana cara dua host tersebut akan berkomunikasi antara satu dengan yang lainnya (apakah dengan menggunakan koneksi connection-oriented, atau connectionless).

Gambar 4.11 Komunikasi Antara 2 Host Melewati Firewall

Kedua tujuan tersebut dapat digunakan untuk menentukan keadaan koneksi antara dua host tersebut, seperti halnya cara manusia bercakap-cakap. Jika Amir bertanya kepada Aminah mengenai sesuatu, maka Aminah akan meresponsnya dengan jawaban yang sesuai dengan pertanyaan yang diajukan oleh Amir. Pada saat Amir melontarkan pertanyaannya kepada Aminah, keadaan percakapan tersebut adalah Amir menunggu respons dari Aminah. Komunikasi di jaringan juga mengikuti cara yang sama untuk memantau keadaan percakapan komunikasi yang terjadi.

Firewall dapat memantau informasi keadaan koneksi untuk menentukan apakah ia hendak mengizinkan lalu lintas jaringan. Umumnya hal ini dilakukan dengan memelihara sebuah tabel keadaan koneksi (dalam istilah firewall: state table) yang memantau keadaan semua komunikasi yang melewati firewall. Dengan memantau keadaan koneksi ini, firewall dapat menentukan apakah data yang melewati firewall sedang "ditunggu" oleh host yang dituju, dan jika ya, aka mengizinkannya. Jika data yang melewati firewall tidak cocok dengan keadaan koneksi yang didefinisikan oleh tabel keadaan koneksi, maka data tersebut akan ditolak. Hal ini umumnya disebut sebagai Stateful Inspection.

Ketika sebuah firewall menggabungkan stateful inspection dengan packet inspection, maka firewall tersebut dinamakan dengan Stateful Packet Inspection (SPI). SPI merupakan proses inspeksi paket yang tidak dilakukan dengan menggunakan struktur paket dan data yang terkandung dalam paket, tapi juga pada keadaan apa host-host yang saling berkomunikasi tersebut berada. SPI mengizinkan firewall untuk melakukan penapisan tidak hanya berdasarkan isi paket tersebut, tapi juga berdasarkan koneksi atau keadaan koneksi, sehingga dapat mengakibatkan firewall memiliki kemampuan yang lebih fleksibel, mudah diatur, dan memiliki skalabilitas dalam hal penapisan yang tinggi.

Salah satu keunggulan dari SPI dibandingkan dengan inspeksi paket biasa adalah bahwa ketika sebuah koneksi telah dikenali dan diizinkan (tentu saja setelah dilakukan inspeksi), umumnya sebuah kebijakan (policy) tidak dibutuhkan untuk mengizinkan komunikasi balasan karena firewall tahu respons apa yang diharapkan akan diterima. Hal ini memungkinkan inspeksi terhadap data dan perintah yang terkandung dalam sebuah paket data untuk menentukan apakah sebuah koneksi diizinkan atau tidak, lalu firewall akan secara otomatis memantau keadaan percakapan dan secara dinamis mengizinkan lalu lintas yang sesuai dengan keadaan. Ini merupakan peningkatan yang cukup signifikan jika dibandingkan dengan firewall dengan inspeksi paket biasa. Apalagi, proses ini diselesaikan tanpa adanya kebutuhan untuk mendefinisikan sebuah kebijakan untuk mengizinkan respons dan komunikasi selanjutnya. Kebanyakan firewall modern telah mendukung fungsi ini.

– Melakukan autentikasi terhadap akses

Protokol TCP/IP dibangun dengan premis bahwa protokol tersebut mendukung komunikasi yang terbuka. Jika dua host saling mengetahui alamat IP satu sama lainnya, maka mereka diizinkan untuk saling berkomunikasi. Pada awal-awal perkembangan Internet, hal ini boleh dianggap sebagai suatu berkah. Tapi saat ini, di saat semakin banyak yang terhubung ke Internet, mungkin kita tidak mau siapa saja yang dapat berkomunikasi dengan sistem yang kita miliki. Karenanya, firewall dilengkapi dengan fungsi autentikasi dengan menggunakan beberapa mekanisme autentikasi, sebagai berikut :

- Firewall dapat meminta input dari pengguna mengenai nama pengguna (user name) serta kata kunci (password). Metode ini sering disebut sebagai extended authentication atau xauth. Menggunakan xauth pengguna yang mencoba untuk membuat sebuah koneksi akan diminta input mengenai nama dan kata kuncinya sebelum akhirnya diizinkan oleh firewall. Umumnya, setelah koneksi diizinkan oleh kebijakan keamanan dalam firewall, firewall pun tidak perlu lagi mengisikan input password dan namanya, kecuali jika koneksi terputus dan pengguna mencoba menghubungkan dirinya kembali.
- Metode kedua adalah dengan menggunakan sertifikat digital dan kunci publik. Keunggulan metode ini dibandingkan dengan metode pertama adalah proses autentikasi dapat terjadi tanpa intervensi pengguna. Selain itu, metode ini lebih cepat dalam rangka melakukan proses autentikasi. Meskipun demikian, metode ini lebih rumit implementasinya karena membutuhkan banyak komponen seperti halnya implementasi infrastruktur kunci publik.

Metode selanjutnya adalah dengan menggunakan Pre-Shared Key (PSK) atau kunci yang telah diberitahu kepada pengguna. Jika dibandingkan

- dengan sertifikat digital, PSK lebih mudah diimplenentasikan karena lebih sederhana, tetapi PSK juga mengizinkan proses autentikasi terjadi tanpa intervensi pengguna. Dengan menggunakan PSK, setiap host akan diberikan sebuah kunci yang telah ditentukan sebelumnya yang kemudian digunakan untuk proses autentikasi. Kelemahan metode ini adalah kunci PSK jarang sekali diperbarui dan banyak organisasi sering sekali menggunakan kunci yang sama untuk melakukan koneksi terhadap host-host yang berada pada jarak jauh, sehingga hal ini sama saja meruntuhkan proses autentikasi. Agar tercapai sebuah derajat keamanan yang tinggi, umumnya beberapa organisasi juga menggunakan gabungan antara metode PSK dengan xauth atau PSK dengan sertifikat digital.
- Dengan mengimplementasikan proses autentikasi, firewall dapat menjamin bahwa koneksi dapat diizinkan atau tidak. Meskipun jika paket telah diizinkan dengan menggunakan inspeksi paket (PI) atau berdasarkan keadaan koneksi (SPI), jika host tersebut tidak lolos proses autentikasi, paket tersebut akan dibuang.

– Melindungi sumber daya dalam jaringan privat

Salah satu tugas firewall adalah melindungi sumber daya dari ancaman yang mungkin datang. Proteksi ini dapat diperoleh dengan menggunakan beberapa pengaturan peraturan akses (access control), penggunaan SPI, application proxy, atau kombinasi dari semuanya untuk mengamankan host yang dilindungi supaya tidak dapat diakses oleh host-host yang mencurigakan atau dari lalu lintas jaringan yang mencurigakan. Meskipun demikian, firewall bukan satu-satunya metode proteksi teraman terhadap sumber daya, dan mempercayakan proteksi firewall dari ancaman secara eksklusif adalah salah satu kesalahan fatal.

Jika sebuah host yang menjalankan sistem operasi tertentu yang memiliki lubang keamanan yang belum ditambal dikoneksikan ke Internet, firewall mungkin tidak dapat mencegah dieksploitasinya host tersebut oleh host-host lainnya, khususnya jika exploit tersebut menggunakan lalu lintas yang oleh firewall telah diizinkan (dalam konfigurasinya). Sebagai contoh, jika sebuah packet-inspection firewall mengizinkan lalu lintas HTTP ke sebuah web server yang menjalankan sebuah layanan web yang memiliki lubang keamanan yang belum ditambal, maka seorang pengguna yang "iseng" dapat saja membuat exploit untuk meruntuhkan web server tersebut karena memang web server yang bersangkutan memiliki lubang keamanan yang belum ditambal.

Dalam contoh ini, web server tersebut akhirnya mengakibatkan proteksi yang ditawarkan oleh firewall menjadi tidak

berguna. Hal ini disebabkan oleh firewall tidak dapat membedakan antara request HTTP

yang mencurigakan atau tidak. Apalagi, jika firewall yang digunakan bukan application proxy. Oleh karena itulah, sumber daya yang dilindungi haruslah dipelihara dengan melakukan penambalan terhadap lubang-lubang keamanan, selain tentunya dilindungi oleh firewall.

– Mencatat semua kejadian, dan melaporkan kepada administrator

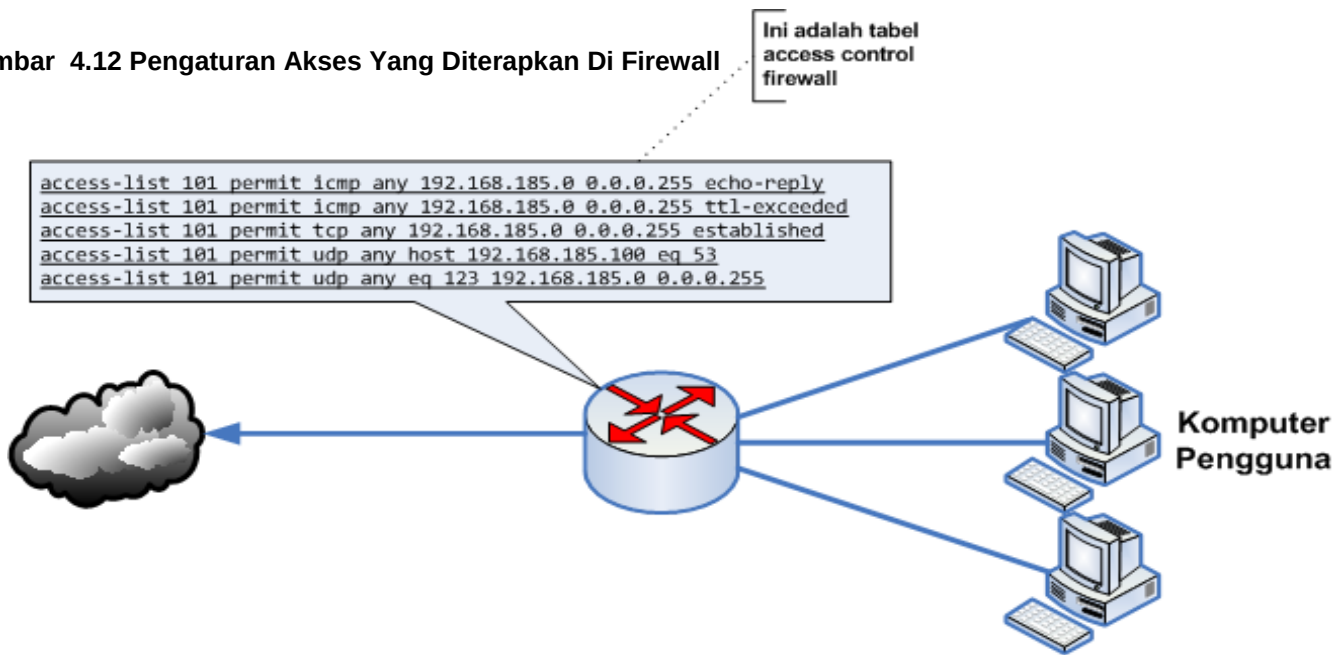
Jenis-jenis Firewall

- Packet-Filter Firewall

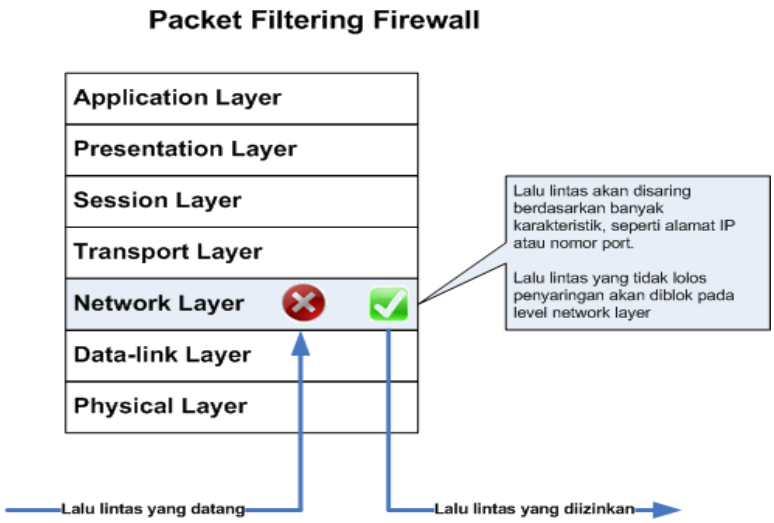
Pada bentuknya yang paling sederhana, sebuah firewall adalah sebuah router atau komputer yang dilengkapi dengan dua buah NIC (Network Interface Card, kartu antarmuka jaringan) yang mampu melakukan penapisan atau penyaringan terhadap paket-paket yang masuk. Perangkat jenis ini umumnya disebut dengan packet-filtering router.

Firewall jenis ini bekerja dengan cara membandingkan alamat sumber dari paket-paket tersebut dengan kebijakan pengontrolan akses yang terdaftar dalam Access Control List firewall, router tersebut akan mencoba memutuskan apakah hendak meneruskan paket yang masuk tersebut ke tujuannya atau menghentikannya. Pada bentuk yang lebih sederhana lagi, firewall hanya melakukan pengujian terhadap alamat IP atau nama domain yang menjadi sumber paket dan akan menentukan apakah hendak meneruskan atau menolak paket tersebut. Meskipun demikian, packet-filtering router tidak dapat digunakan untuk memberikan akses (atau menolaknya) dengan menggunakan basis hak-hak yang dimiliki oleh pengguna.

Gambar 4.12 Pengaturan Akses Yang Diterapkan Di Firewall



Packet-filtering router juga dapat dikonfigurasikan agar menghentikan beberapa jenis lalu lintas jaringan dan tentu saja mengizinkannya. Umumnya, hal ini dilakukan dengan mengaktifkan/menonaktifkan port TCP/IP dalam sistem firewall tersebut. Sebagai contoh, port 25 yang digunakan oleh Protokol SMTP (Simple Mail Transfer Protocol) umumnya dibiarkan terbuka oleh beberapa firewall untuk mengizinkan surat elektronik dari Internet masuk ke dalam jaringan privat, sementara port lainnya seperti port 23 yang digunakan oleh Protokol Telnet dapat dinonaktifkan untuk mencegah pengguna Internet untuk mengakses layanan yang terdapat dalam jaringan privat tersebut. Firewall juga dapat memberikan semacam pengecualian (exception) agar beberapa aplikasi dapat melewati firewall tersebut. Dengan menggunakan pendekatan ini, keamanan akan lebih kuat tapi memiliki kelemahan yang signifikan yakni kerumitan konfigurasi terhadap firewall: daftar Access Control List firewall akan membesar seiring dengan banyaknya alamat IP, nama domain, atau port yang dimasukkan ke dalamnya, selain tentunya juga exception yang diberlakukan.



Gambar 4.13 Cara Kerja Packet Filtering

Kelebihan dari tipe ini adalah mudah untuk di implementasikan, transparan untuk pemakai, lebih cepat Adapun kelemahannya adalah cukup rumitnya untuk menyetting paket yang akan difilter secara tepat, serta lemah dalam hal authentikasi. Adapun serangan yang dapat terjadi pada firewall dengan tipe ini adalah :

– IP address spoofing
  Intruder (penyusup) dari luar dapat melakukan ini dengan cara menyertakan/menggunakan IP address jaringan lokal yanbg telah diijinkan untuk melalui firewall.

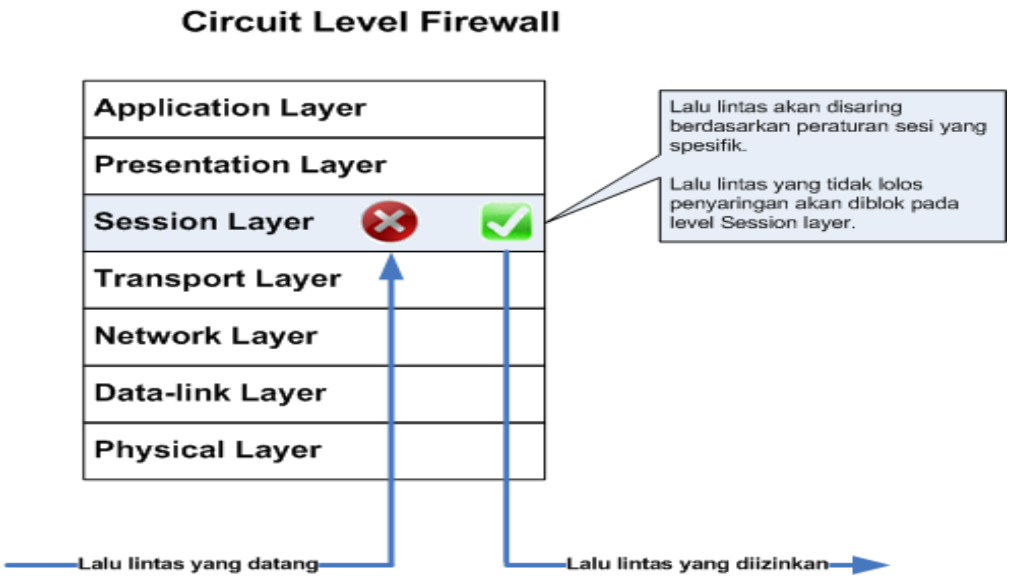
– Source routing attacks
  Tipe ini tidak menganalisa informasi routing sumber IP, sehingga memungkinkan untuk melewati firewall.

– Tiny Fragment attacks
  Intruder (penyusup) membagi IP kedalam bagian-bagian (fragment) yang lebih kecil dan memaksa terbaginya informasi mengenai TCP header. Serangan jenis ini di design untuk menipu aturan penyaringan yang bergantung kepada informasi dari TCP header. Penyerang berharap hanya bagian (fragment) pertama saja yang akan di periksa dan sisanya akan bisa lewat dengan bebas. Hal ini dapat di tanggulangi dengan cara menolak semua packet dengan protokol TCP dan memiliki Offset = 1 pada IP fragment (bagian IP)

- Circuit Level Gateway

Firewall jenis lainnya adalah Circuit-Level Gateway, yang umumnya berupa komponen dalam sebuah proxy server. Firewall jenis ini beroperasi pada level yang lebih tinggi dalam model referensi tujuh lapis OSI (bekerja pada lapisan sesi/session layer) daripada Packet Filter Firewall. Modifikasi ini membuat firewall jenis ini berguna dalam rangka menyembunyikan informasi mengenai jaringan terproteksi, meskipun firewall ini tidak melakukan penyaringan terhadap paket-paket individual yang mengalir dalam koneksi.

Dengan menggunakan firewall jenis ini, koneksi yang terjadi antara pengguna dan jaringan pun disembunyikan dari pengguna. Pengguna akan dihadapkan secara langsung dengan firewall pada saat proses pembuatan koneksi dan firewall pun akan membentuk koneksi dengan sumber daya jaringan yang hendak diakses oleh pengguna setelah mengubah alamat IP dari paket yang ditransmisikan oleh dua belah pihak. Hal ini mengakibatkan terjadinya sebuah sirkuit virtual (virtual circuit) antara pengguna dan sumber daya jaringan yang ia akses. Firewall ini dianggap lebih aman dibandingkan dengan Packet-Filtering Firewall, karena pengguna eksternal tidak dapat melihat alamat IP jaringan internal dalam paket-paket yang ia terima, melainkan alamat IP dari firewall.



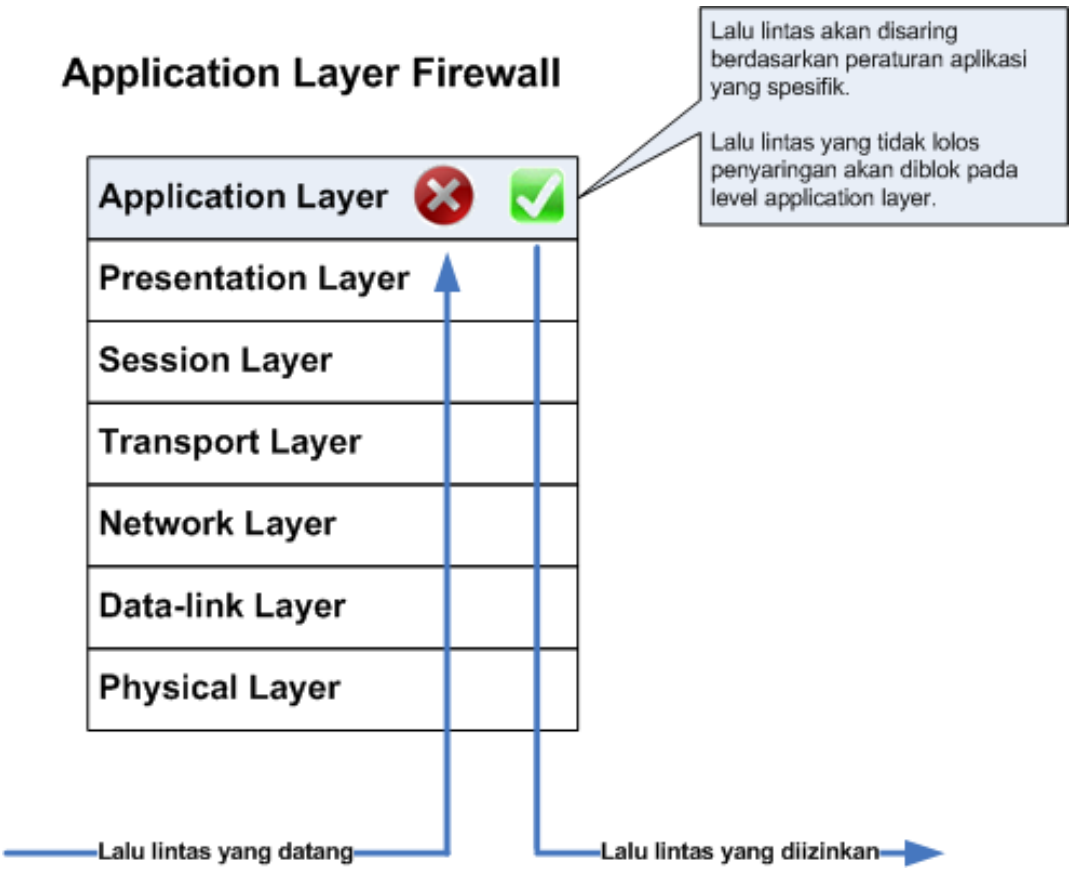
Gambar 4.14 Cara Kerja Circuit Level Firewall

- Application Level Firewall

Firewall jenis lainnya adalah Application Level Gateway (atau Application-Level Firewall atau sering juga disebut sebagai Proxy Firewall), yang umumnya juga merupakan komponen dari sebuah proxy server. Firewall ini tidak mengizinkan paket yang datang untuk melewati firewall secara langsung. Tetapi, aplikasi proxy yang berjalan dalam komputer yang menjalankan firewall akan meneruskan permintaan tersebut kepada layanan yang tersedia dalam jaringan privat dan kemudian meneruskan respons dari permintaan tersebut kepada komputer yang membuat permintaan pertama kali yang terletak dalam jaringan publik yang tidak aman.

Umumnya, firewall jenis ini akan melakukan autentikasi terlebih dahulu terhadap pengguna sebelum mengizinkan pengguna tersebut untuk mengakses jaringan. Selain itu, firewall ini juga mengimplementasikan mekanisme auditing dan pencatatan (logging) sebagai bagian dari kebijakan keamanan yang diterapkannya. Application Level Firewall juga umumnya mengharuskan beberapa konfigurasi yang diberlakukan pada pengguna untuk mengizinkan mesin klien agar dapat berfungsi. Sebagai contoh, jika sebuah proxy FTP dikonfigurasikan di atas sebuah application layer gateway, proxy tersebut dapat dikonfigurasikan untuk mengizinlan beberapa perintah FTP, dan menolak beberapa perintah lainnya. Jenis ini paling sering diimplementasikan pada proxy SMTP sehingga mereka dapat menerima surat elektronik dari luar (tanpa menampakkan

alamat e-mail internal), lalu meneruskan e-mail tersebut kepada e-mail server dalam jaringan. Tetapi, karena adanya pemrosesan yang lebih rumit, firewall jenis ini mengharuskan komputer yang dikonfigurasikan sebagai application gateway memiliki spesifikasi yang tinggi, dan tentu saja jauh lebih lambat dibandingkan dengan packet-filter firewall.



Gambar 4.15 Posisi Aplication Firewall Dalam Model OSI

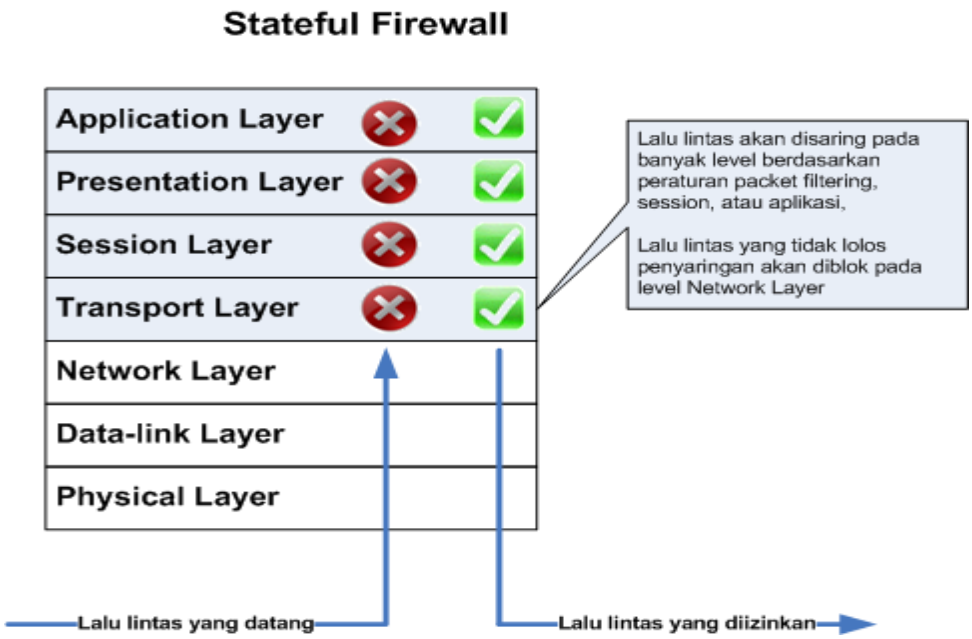
- NAT Firewall

NAT (Network Address Translation) Firewall secara otomatis menyediakan proteksi terhadap sistem yang berada di balik firewall karena NAT Firewall hanya mengizinkan koneksi yang datang dari komputer-komputer yang berada di balik firewall. Tujuan dari NAT adalah untuk melakukan multiplexing terhadap lalu lintas dari jaringan internal untuk kemudian menyampaikannya kepada jaringan yang lebih luas (MAN, WAN atau Internet) seolah-olah paket tersebut datang dari sebuah alamat IP atau beberapa alamat IP. NAT Firewall membuat tabel dalam memori yang mengandung informasi mengenai koneksi yang dilihat oleh firewall. Tabel ini akan memetakan alamat jaringan internal ke alamat eksternal. Kemampuan untuk menaruh keseluruhan jaringan di belakang

sebuah alamat IP didasarkan terhadap pemetaan terhadap port-port dalam NAT firewall.

- Stateful Firewall

Stateful Firewall merupakan sebuah firewall yang menggabungkan keunggulan yang ditawarkan oleh packet-filtering firewall, NAT Firewall, Circuit-Level Firewall dan Proxy Firewall dalam satu sistem. Stateful Firewall dapat melakukan filtering terhadap lalu lintas berdasarkan karakteristik paket, seperti halnya packet-filtering firewall, dan juga memiliki pengecekan terhadap sesi koneksi untuk meyakinkan bahwa sesi koneksi yang terbentuk tersebut diizinlan. Tidak seperti Proxy Firewall atau Circuit Level Firewall, Stateful Firewall umumnya didesain agar lebih transparan (seperti halnya packet-filtering firewall atau NAT firewall). Tetapi, stateful firewall juga mencakup beberapa aspek yang dimiliki oleh application level firewall, sebab ia juga melakukan inspeksi terhadap data yang datang dari lapisan aplikasi (application layer) dengan menggunakan layanan tertentu. Firewall ini hanya tersedia pada beberapa firewall kelas atas, semacam Cisco PIX. Karena menggabungkan keunggulan jenis-jenis firewall lainnya, stateful firewall menjadi lebih kompleks.



Gambar 4.16 Cara Kerja Stateful Firewall

- Transparent Firewall

Transparent Firewall (juga dikenal sebagai bridging firewall) bukanlah sebuah firewall yang murni, tetapi ia hanya berupa turunan dari stateful Firewall. Daripada firewall-firewall lainnya yang beroperasi pada lapisan IP ke atas, transparent firewall bekerja pada lapisan Data-Link Layer, dan kemudian ia memantau lapisan-lapisan yang ada di atasnya. Selain itu, transparent firewall juga dapat melakukan apa yang dapat dilakukan

oleh packet-filtering firewall, seperti halnya stateful firewall dan tidak terlihat oleh pengguna (karena itulah, ia disebut sebagai Transparent Firewall).

Intinya, transparent firewall bekerja sebagai sebuah bridge yang bertugas untuk menyaring lalu lintas jaringan antara dua segmen jaringan. Dengan menggunakan transparent firewall, keamanan sebuah segmen jaringan pun dapat diperkuat, tanpa harus mengaplikasikan NAT Filter. Transparent Firewall menawarkan tiga buah keuntungan, yakni sebagai berikut:

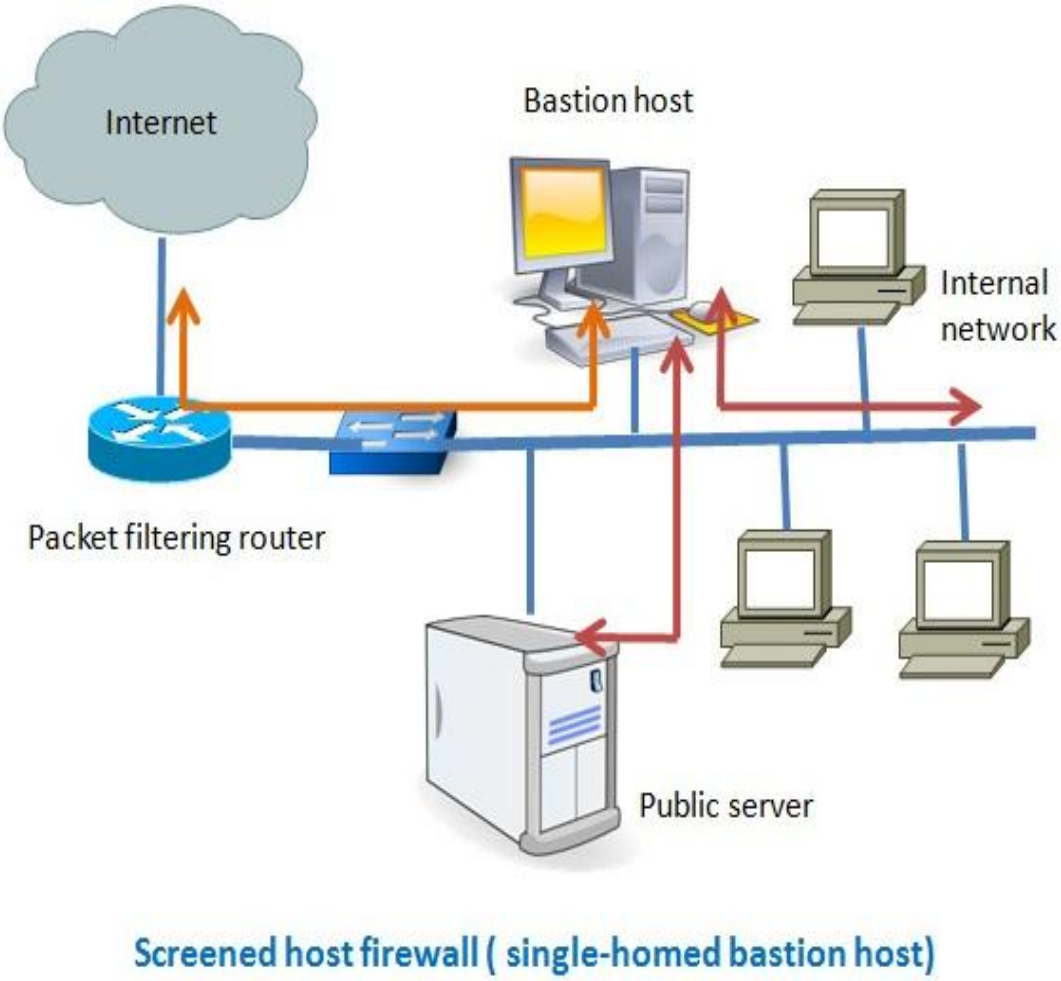
– Konfigurasi yang mudah (bahkan beberapa produk mengklaim sebagai "Zero Configuration"). Hal ini memang karena transparent firewall dihubungkan secara langsung dengan jaringan yang hendak diproteksinya, dengan memodifikasi sedikit atau tanpa memodifikasi konfigurasi firewall tersebut. Karena ia bekerja pada data-link layer, pengubahan alamat IP pun tidak dibutuhkan. Firewall juga dapat dikonfigurasikan untuk melakukan segmentasi terhadap sebuah subnet jaringan antara jaringan yang memiliki keamanan yang rendah dan keamanan yang tinggi atau dapat juga untuk melindungi sebuah host, jika memang diperlukan.
– Kinerja yang tinggi. Hal ini disebabkan oleh firewall yang berjalan dalam lapisan data-link lebih sederhana dibandingkan dengan firewall yang berjalan dalam lapisan yang lebih tinggi. Karena bekerja lebih sederhana, maka kebutuhan pemrosesan pun lebih kecil dibandingkan dengan firewall yang berjalan pada lapisan yang tinggi, dan akhirnya performa yang ditunjukannya pun lebih tinggi.
– Tidak terlihat oleh pengguna (stealth). Hal ini memang dikarenakan Transparent Firewall bekerja pada lapisan data-link, dan tidak membutuhkan alamat IP yang ditetapkan untuknya (kecuali untuk melakukan manajemen terhadapnya, jika memang jenisnya managed firewall). Karena itulah, transparent firewall tidak dapat terlihat oleh para penyerang. Karena tidak dapat diraih oleh penyerang (tidak memiliki alamat IP), penyerang pun tidak dapat menyerangnya.

Konfigurasi Firewall

- Screened Host FIrewall system (single-homed bastion)

Pada konfigurasi ini, fungsi firewall akan dilakukan oleh packet filtering router dan bastion host*.Router ini dikonfigurasikan sedemikian sehingga untuk semua arus data dari Internet, hanya paket IP yang menuju bastion host yang di ijinkan. Sedangkan untuk arus data (traffic) dari jaringan internal, hanya paket IP dari bastion host yang di ijinkan untuk keluar. Konfigurasi ini mendukung fleksibilitasdalam Akses internet secara langsung, sebagai contoh apabila terdapat web server pada jaringan ini maka dapat di konfigurasikan agar web server dapat diakses langsung dari internet. Bastion Host melakukan fungsi Authentikasi dan fungsi sebagai proxy. Konfigurasi ini memberikan tingkat keamanan yang lebih baik daripada

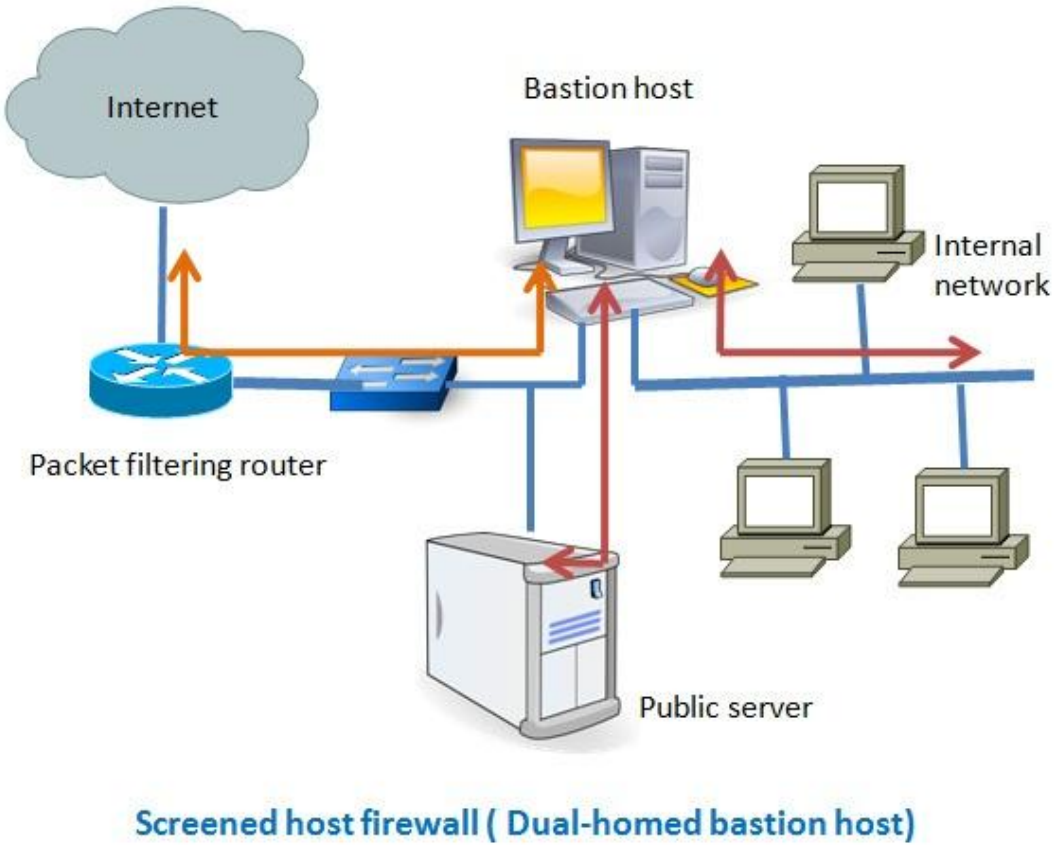
packet-filtering router atau application-level gateway secara terpisah.



Gambar 4.17 Diagram Kerja Sistem Firewall Screened Host (Single-Homed)

- Screened Host Firewall system (Dual-homed bastion)

Pada konfigurasi ini, secara fisik akan terdapat patahan/celah dalam jaringan. Kelebihannya adalah dengan adanya du ajalur yang meisahkan secara fisik maka akan lebih meningkatkan keamanan dibanding konfigurasi pertama,adapun untuk server-server yang memerlukan direct akses (akses langsung) maka dapat diletakkan ditempat/segmenrt yang langsung berhubungan dengan internet. Hal ini dapat dilakukan dengan cara menggunakan 2 buah NIC (Network Interface Card) pada Bastion Host.

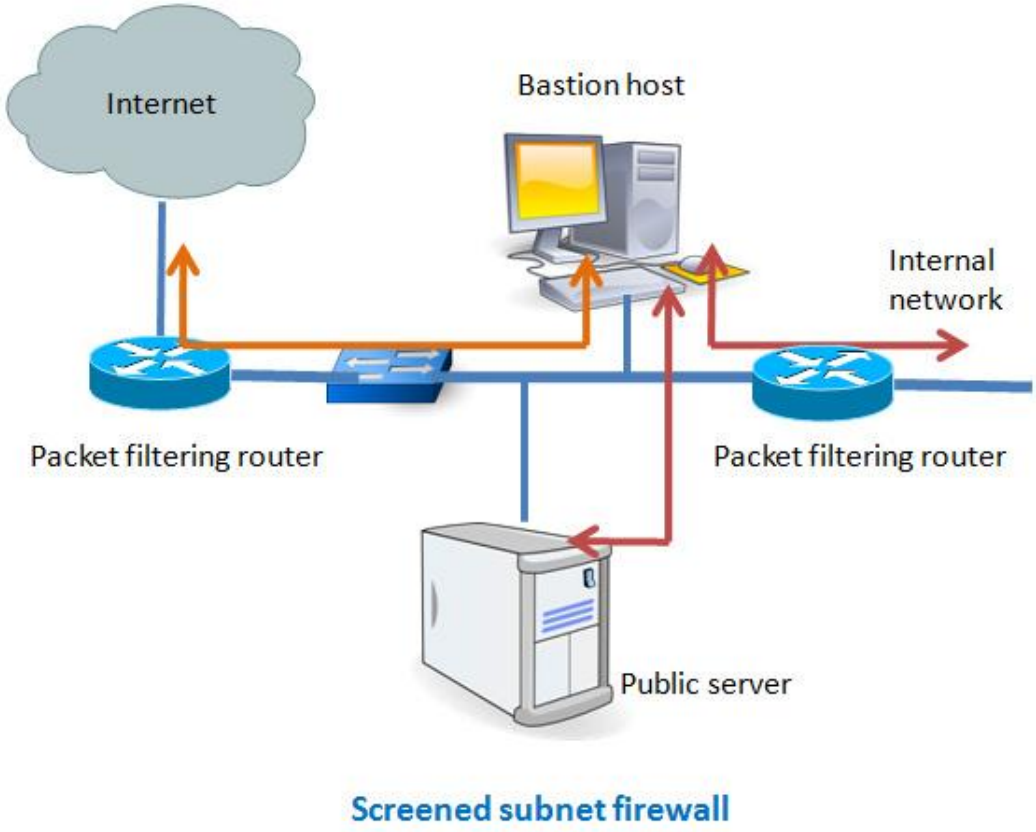


Gambar 4.18 Diagram Kerja Sistem Firewall Screened Host (Dual-Homed)

- Screened subnet firewall

Ini merupakan konfigurasi yang paling tinggi tingkat keamanannya. Karena pada konfigurasi ini di gunakan 2 buah packet filtering router, 1 diantara internet dan bastion host, sedangkan 1 lagi diantara bastian host dan jaringan local konfigurasi ini membentuk subnet yang terisolasi. Kelebihannya adalah :

– Terdapat 3 lapisan/tingkat pertahanan terhadap penyusup/intruder.
– Router luar hanya melayani hubungan antara internet dan bastion host sehingga jaringan lokal menjadi tak terlihat (invisible)
– Jaringan lokal tidak dapat mengkonstruksi routing langsung ke internet, atau dengan kata lain , Internet menjadi Invinsible (bukan berarti tidak bisa melakukan koneksi internet).



Gambar 4.19 Diagram Kerja Sistem Firewall Screened Subnet

IDS

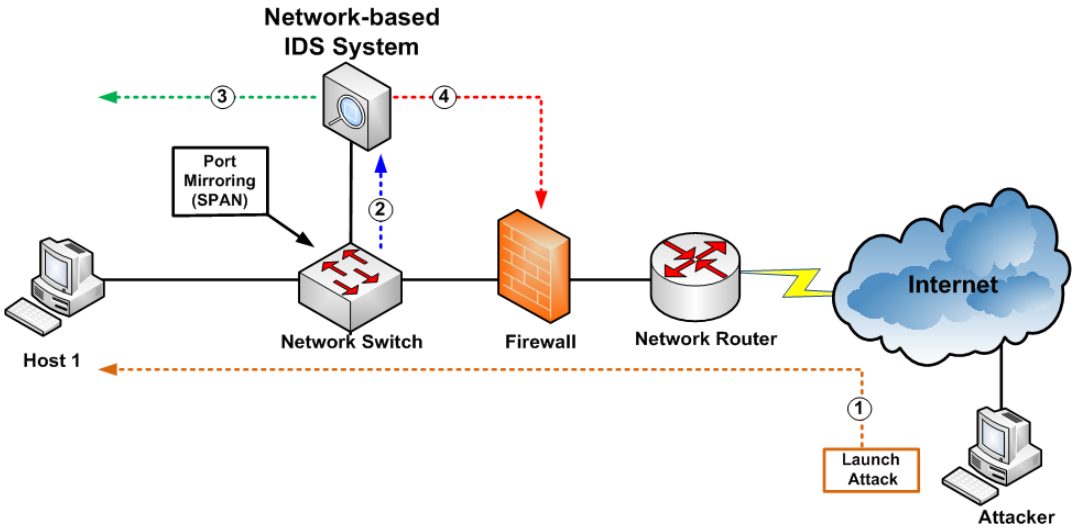
Intrusion Detection System (disingkat IDS) adalah sebuah aplikasi perangkat lunak atau perangkat keras yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan. IDS dapat melakukan inspeksi terhadap lalu lintas inbound dan outbound dalam sebuah sistem atau jaringan, melakukan analisis dan mencari bukti dari percobaan intrusi (penyusupan).

Jenis-jenis IDS

Ada dua jenis IDS, yakni:

- Network-based Intrusion Detection System (NIDS)

Semua lalu lintas yang mengalir ke sebuah jaringan akan dianalisis untuk mencari apakah ada percobaan serangan atau penyusupan ke dalam sistem jaringan. NIDS umumnya terletak di dalam segmen jaringan penting di mana server berada atau terdapat pada "pintu masuk" jaringan. Kelemahan NIDS adalah bahwa NIDS agak rumit diimplementasikan dalam sebuah jaringan yang menggunakan switch Ethernet, meskipun beberapa vendor switch Ethernet sekarang telah menerapkan fungsi IDS di dalam switch buatannya untuk memonitor port atau koneksi.

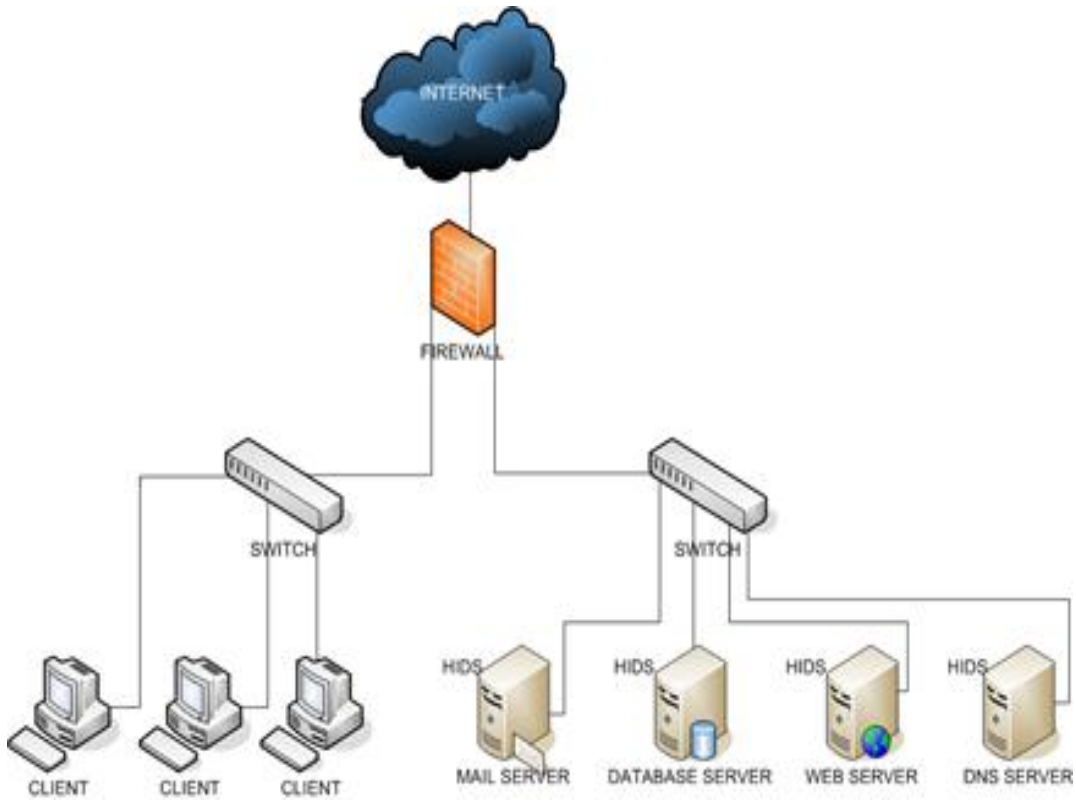


Gambar 4.20 Diagram IDS Berbasis Jaringan

- Host-based Intrusion Detection System (HIDS)

Aktivitas sebuah host jaringan individual akan dipantau apakah terjadi sebuah percobaan serangan atau penyusupan ke dalamnya atau tidak. HIDS seringnya diletakkan pada server-server kritis di jaringan, seperti halnya firewall, web server, atau server yang terkoneksi ke Internet.

Kebanyakan produk IDS merupakan sistem yang bersifat pasif, mengingat tugasnya



Gambar 4.21 Diagram IDS Berbasis Host

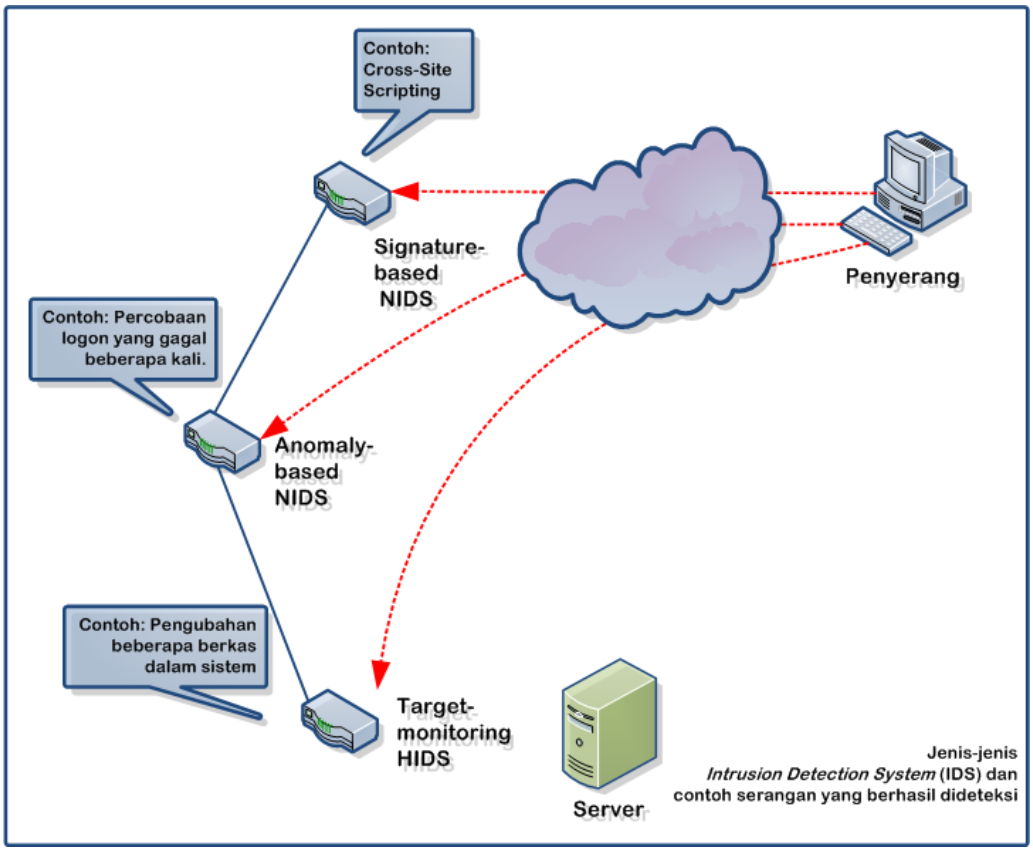
hanyalah mendeteksi intrusi yang terjadi dan memberikan peringatan kepada administrator jaringan bahwa mungkin ada serangan atau gangguan terhadap jaringan. Akhir-akhir ini, beberapa vendor juga mengembangkan IDS yang bersifat aktif yang dapat melakukan beberapa tugas untuk melindungi host atau jaringan dari serangan ketika terdeteksi, seperti halnya menutup beberapa port atau memblokir beberapa alamat IP. Produk seperti ini umumnya disebut sebagai Intrusion Prevention System (IPS). Beberapa produk IDS juga menggabungkan kemampuan yang dimiliki oleh HIDS dan NIDS, yang kemudian disebut sebagai sistem hibrid (Hybrid Intrusion Detection System).

Implementasi & Cara Kerja IDS

Ada beberapa cara bagaimana IDS bekerja. Cara yang paling populer adalah dengan menggunakan pendeteksian berbasis signature (seperti halnya yang dilakukan oleh beberapa antivirus), yang melibatkan pencocokan lalu lintas jaringan dengan basis data yang berisi cara-cara serangan dan penyusupan yang sering dilakukan oleh penyerang. Sama seperti halnya antivirus, jenis ini membutuhkan pembaruan terhadap basis data signature IDS yang bersangkutan.

Metode selanjutnya adalah dengan mendeteksi adanya anomali, yang disebut sebagai Anomaly-based IDS. Jenis ini melibatkan pola lalu lintas yang mungkin merupakan sebuah serangan yang sedang dilakukan oleh penyerang. Umumnya, dilakukan dengan menggunakan teknik statistik untuk membandingkan lalu lintas yang sedang dipantau dengan lalu lintas normal yang biasa terjadi. Metode ini menawarkan kelebihan dibandingkan signature-based IDS, yakni ia dapat mendeteksi bentuk serangan yang baru dan belum terdapat di dalam basis data signature IDS. Kelemahannya, adalah jenis ini sering mengeluarkan pesan false positive. Sehingga tugas administrator menjadi lebih rumit, dengan harus memilah-milah mana yang merupakan serangan yang sebenarnya dari banyaknya laporan false positive yang muncul.

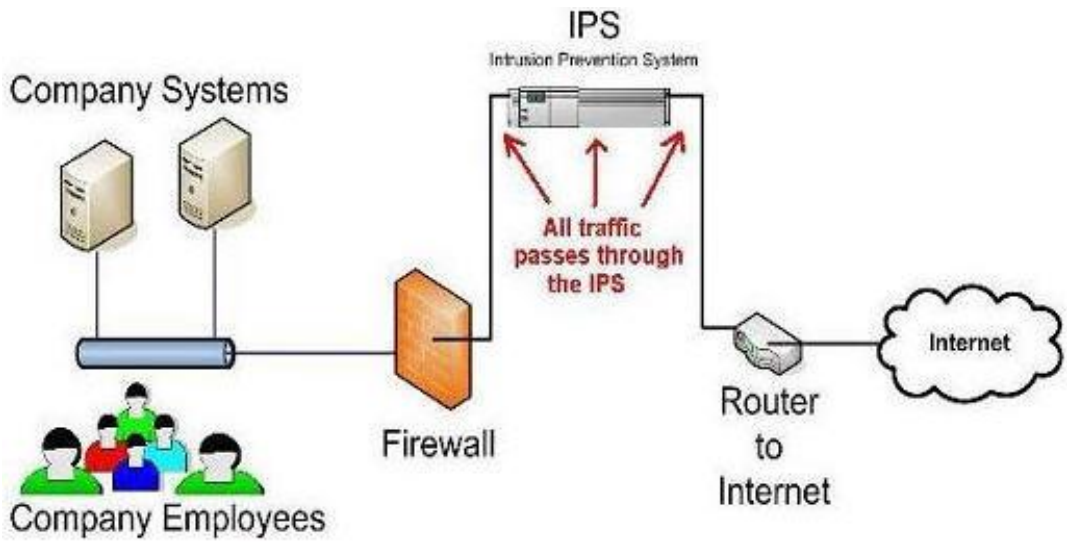
Teknik lainnya yang digunakan adalah dengan memantau berkas-berkas sistem operasi, yakni dengan cara melihat apakah ada percobaan untuk mengubah beberapa berkas sistem operasi, utamanya berkas log. Teknik ini seringnya diimplementasikan di dalam HIDS, selain tentunya melakukan pemindaian terhadap log sistem untuk memantau apakah terjadi kejadian yang tidak biasa.



Gambar 4.21 Cara Kerja Sistem IDS

IPS

Intrusion Prevention System merupakan kombinasi antara fasilitas blocking capabilities dari Firewall dan kedalaman inspeksi paket data dari Intrusion Detection System (IDS). IPS diciptakan pada awal tahun 1990-an untuk memecahkan masalah serangan yang selalu melanda jaringan komputer. IPS membuat akses kontrol dengan cara melihat konten aplikasi, dari pada melihat IP address atau ports, yang biasanya dilakukan oleh firewall. IPS komersil pertama dinamakan BlackIce diproduksi oleh perusahaan NetworkIce, hingga kemudian berubah namanya menjadi ISS(Internet Security System). Sistem setup IPS sama dengan sistem setup IDS. IPS mampu mencegah serangan yang datang dengan bantuan administrator secara minimal atau bahkan tidak sama sekali. Secara logic IPS akan menghalangi suatu serangan sebelum terjadi eksekusi dalam memori, selain itu IPS membandingkan file checksum yang tidak semestinya mendapatkan izin untuk dieksekusi dan juga bisa menginterupsi sistem call.



Gambar 4.22 Diagram Intrusion Prevention System (IPS)

Jenis-jenis IPS

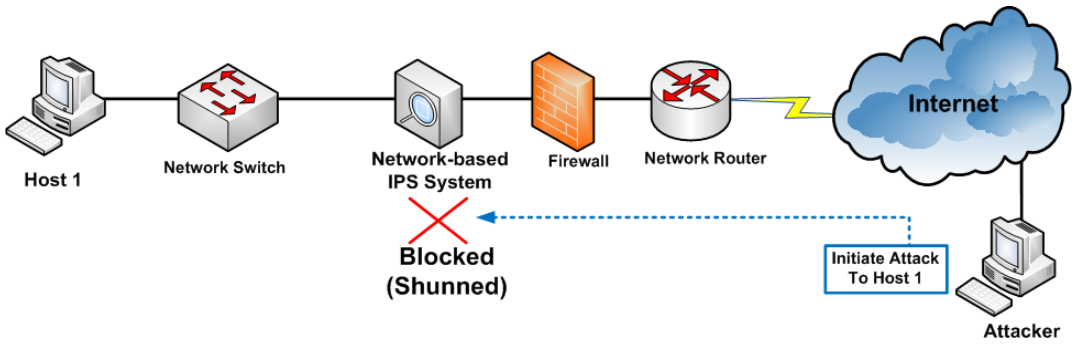
- Host-based Intrusion Prevention System

Host Based IPS (HIPS) bekerja dengan memaksa sekelompok perangkat lunak fundamental untuk berkovensi secara konstan. Hal ini disebut dengan Application Binary Interface (ABI). Hampir tidak mungkin untuk membajak sebuah aplikasi tanpa memodifikasi Application Binary Interface, karena konvensi ini bersifat universal di antara aplikasi-aplikasi yang dimodifikasi. HIPS merupakan sebuah system pecegahan yang terdiri dari banyak layer, menggunakan packet filtering, inspeksi status dan metode pencegahan intrusi yang bersifat real-time untuk menjaga host berada di bawah keadaan dari efisiensi performansi yang layak. Mekanisme kerjanya yaitu dengan mencegah kode-kode berbahaya yang memasuki host agar tidak dieksekusi tanpa perlu untuk mengecek threat signature.

- Network Intrusion Prevention System

Network Based IPS (NIPS), yang juga disebut sebagai “In-line proactive protection”, menahan semua trafik jaringan dan menginspeksi kelakuan dan kode yang mencurigakan. Karena menggunakan in-line model, performansi tinggi merupakan sebuah elemen krusial dari perangkat IPS untuk mencegah terjadinya bottleneck pada jaringan. Oleh karena itu, NIPS biasanya didesain menggunakan tiga komponen untuk mengakselerasi performansi bandwidth, yaitu :

  – Network Chips (Network processor)
  – FPGA Chips
  – ASIC Chips



Gambar 4.23 Contoh Sistem IPS Berbasis Jaringan

Network Based IPS (NIPS) biasanya dibangun dengan tujuan tertentu, sama halnya dengan switch dan router. Beberapa teknologi sudah diterapkan pada NIPS, seperti signature matching, analisa protocol dan kelainan pada protocol, identifikasi dari pola trafik, dan sebagainya. NIPS dibuat untuk menganalisa, mendeteksi, dan melaporkan seluruh arus data dan disetting dengan konfigurasi kebijakan keamanan NIPS, sehingga segala serangan yang datang dapat langsung terdeteksi. Kebijakan keamanan NIPS sendiri terdiri dari:

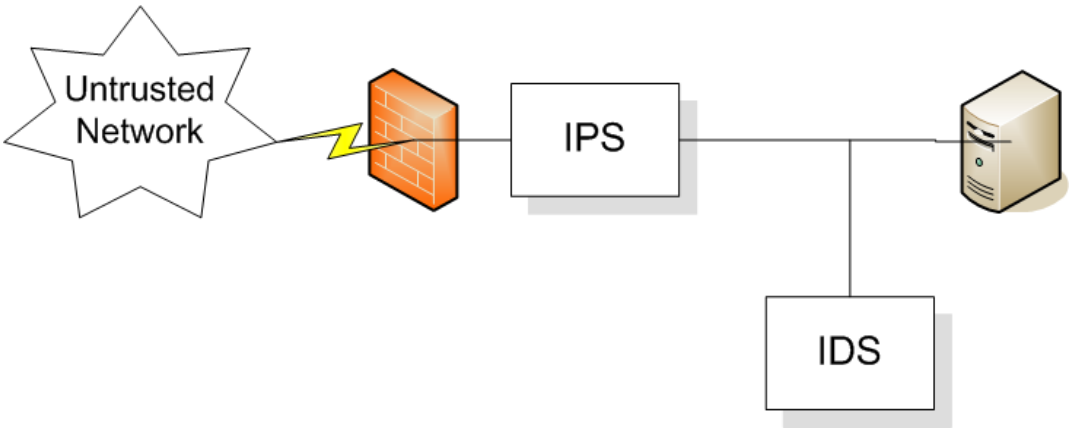
- Content based Intrusion Prevention System, yang bertugas mengawasi isi dari paket-paket yang berlalu lalang dan mencari urutan yang unik dari paket-paket tersebut, berisi virus worm, trojan horse,dll.
- Rate based Intrusion Prevention System, bertugas mencegah dengan cara memonitor melalui arus lalu lintas jaringan dan dibandingkan dengan data statistic yang tersimpan dalam database.

Baik host based maupun network IPS memiliki kelebihan dan kekurangannya masing-masing. HIPS dapat mengatasi semua jenis jaringan yang terenkripsi dan dapat menganalisa semua kode, sedangkat NIPS tidak menggunakan prosesor dan memori di client maupun host. NIPS tidak selalu bagus, kadang bisa gagal dalam mendeteksi serangan, kadang bisa langsung mendeteksi serangan. Keuntungan NIPS adalah administrasinya yang gampang.

Cara Kerja IPS

Firewall merupakan sebuah sistem yang menerapkan sebuah kebijakan kontrol akses yang memeriksa trafik data yang lalu lalang dan memblok paket data yang tidak sesuai dengan kebijakan keamanan. Sebuah Intrusion Detection System (IDS) memonitor performansi system atau jaringan, mencari pola tingkah laku yang tidak sesuai dengan kebijakan keamanan atau tanda-tanda serangan yang dapat dikenali, dan kemudian jika ditemukan maka IDS akan memicu alarm. Di sini, firewall akan menolak serangan yang sudah pasti/jelas, sementara trafik yang mencurigakan akan dibiarkan lewat. Di sisi lain, IDS memonitor semua data di dalam jaringan, memberitahukan administrator jaringan akan adanya serangan pada saat serangan mulai ‘hidup’ dan berada di dalam jaringan. Dengan kata lain, baik IDS maupun

firewall tidak mampu memblokir serangan ketika intrusi benar-benar telah terjadi.



Gambar 4.24 Penempatan IPS Dan IDS Dalam Satu Jaringan

Lebih jauh lagi, IPS sebenarnya lebih dari sekedar IDS + firewall. IPS didesain sebagai sebuah embedded system yang membuat banyak filter untuk mencegah bermacam-macam serangan seperti hacker, worm, virus, Denial of Service (DoS) dan trafik berbahaya lainnya, agar jaringan enterprise tidak menderita banyak kerugian bahkan ketika security patch terbaru belum diterapkan. Pembangunan IPS didasarkan pada sebuah modul “in-line”: data melewati perangkat IPS dari satu ujung dari kanal data tunggal, hanya data yang sudah dicek dan divalidasi oleh mesin IPS yang diperbolehkan untuk lewat menuju ujung lain dari kanal data. Pada scenario ini, paket yang mengandung tanda-tanda serangan pada paket asalnya akan dibersihkan dari jaringan.

Penggunaan multiple filter pada IPS membuatnya secara signifikan lebih efektif ketika menginspeksi, mengidentifikasi dan memblokir serangan berdasarkan urutan waktu. IPS membuat filter baru ketika sebuah metode serangan baru diidentifikasi. Mesin inspeksi paket data IPS normalnya terdiri dari integrated circuit yang didesain untuk inspeksi data mendalam. Setiap serangan yang mencoba mengeksploitasi kelemahan dari layer 2 sampai layer 7 OSI akan difilter oleh mesin IPS yang mana, secara tradisional, kemampuan firewall hanya terbatas sampai modul 3 atau 4 saja. Teknologi packet-filter dari firewall tradisional tidak menerapkan inspeksi untuk setiap byte dari segmen data yang bermakna tidak semua serangan dapat diidentifikasikan olehnya.

Tabel 4.2 Tabel Perbandingan IDS Dan IPS

	IDS	IPS
OSI Layer	Layer 3	Layer 2, 3 dan 7
Kegunaan	IDS didesign hanya untuk mengidentifikasi dan memeriksa semua paket yang lewat, jika ditemukan keganjilan maka akan memtrigger alarm	Mengkombinasikan Firewall, Policy, QoS dan IDS dengan baik. IPS memang dibuat untuk dapat mentrigger alarm dan melakukan Allow, Block, Log
Aktivitas	Mendeteksi serangan hanya disaat serangan tersebut telah masuk ke jaringan dan tidak akan melakukan sesuatu untuk menghentikannya	Early Detection, teknik yang proaktif, mencegah sedini mungkin attack masuk ke jaringan, dan akan menghentikannya jika teridentifikasi
Komponen	Tidak dapat mendeteksi semua aktivitas malicious dan malware setiap saat yang akan mengakibatkan false negative sangat banyak	Memungkinkan dapat mendeteksi new signature dan behavior attack, dan mengakibatkan rendahnya false negative
Integrated	Tidak dapat menggunakan ACL / script dari komponen system keamanan yang lain	Dapat diintegrasikan dengan ACL dan perimeter DMZ lainnya

Secara kontras, IPS mampu melakukan inspeksi tersebut dan semua paket data diklasifikasikan dan dikirim ke filter yang sesuai menurut informasi header yang ditemukan di segmen data, seperti alamat asal, alamat tujuan, port, data field dan sebagainya. Setiap filter bertanggung jawab untuk menganalisis paket-paket yang berkaitan, dan yang mengandung tanda-tanda membahayakan akan didrop dan jika dinyatakan tidak berbahaya akan dibiarkan lewat. Paket yang belum jelas akan diinspeksi lebih lanjut. Untuk setiap tipe serangan berbeda, IPS membutuhkan sebuah filter yang bersesuaian dengan aturan filtering yang sudah ditentukan sebelumnya. Aturan-aturan ini mempunyai definisi luas untuk tujuan akurasi, atau memastikan bahwa sebisa mungkin jangkauan aktifitas yang luas dapat terenkapsulasi di dalam sebuah definisi. Ketika mengklasifikasikan sebuah aliran data, mesin filter akan mengacu pada informasi segmen paket, menganalisa konteks dari field tertentu dengan tujuan untuk mengimprovisasi akurasi dari proses filtering.

Monitoring Dan Pengaturan ISP

- Service Level Agreement (SLA)

SLA adalah kepanjangan dari Service Level Agreement yang biasanya dinotasikan dalam level angka sembilan, yang artinya menunjukan seberapa besar downtime yang mereka toleransi terhadap layanan yang mereka berikan.

Semakin tinggi dan banyak level angka 9 yang ada dalam nilai SLA, makin bagus layanan yang diberikan. Hal itu menandakan mereka memiliki layanan yang toleransi downtimenya sangat kecil. Jadi SLA yang baik adalah yang mendekati 100. Tetapi pada umumnya, ideal untuk suatu kontrak SLA 99,999 adalah tertinggi karena itu berarti tidak akan diijinkan downtime lebih dari 5,26 menit dalam satu tahun.

Tabel 4.3 Tabel Perjanjian Level Layanan (SLA)

Availability %	Downtime per year	Downtime per month*	Downtime per week
90%	36.5 days	72 hours	16.8 hours
95%	18.25 days	36 hours	8.4 hours
98%	7.30 days	14.4 hours	3.36 hours
99%	3.65 days	7.20 hours	1.68 hours
99.5%	1.83 days	3.60 hours	50.4 minutes
99.8%	17.52 hours	86.23 minutes	20.16 minutes
99.9% ("three nines")	8.76 hours	43.2 minutes	10.1 minutes
99.95%	4.38 hours	21.56 minutes	5.04 minutes
99.99% ("four nines")	52.6 minutes	4.32 minutes	1.01 minutes
99.999% ("five nines")	5.26 minutes	25.9 seconds	6.05 seconds
99.9999% ("six nines")	31.5 seconds	2.59 seconds	0.605 seconds

- SNMP

Simple Network Management Protocol (SNMP) adalah standar manajemen jaringan pada TCP/IP. Gagasan di balik SNMP adalah bagaimana supaya informasi yang dibutuhkan untuk manajemen jaringan bisa dikirim menggunakan TCP/IP. Protokol tersebut memungkinkan administrator jaringan untuk menggunakan perangkat jaringan khusus yang berhubungan dengan perangkat jaringan yang lain untuk mengumpulkan informasi dari mereka, dan mengatur bagaimana mereka beroperasi.

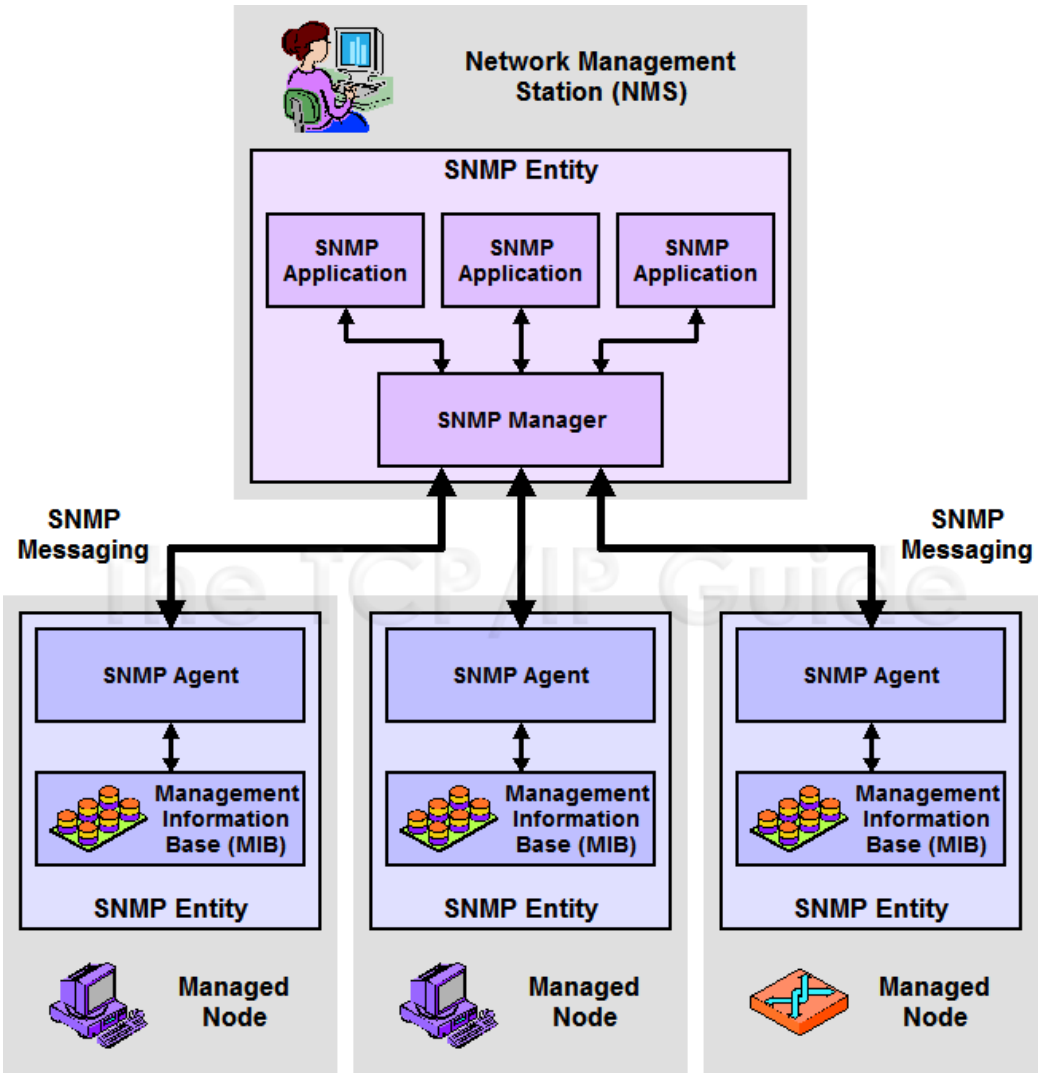
SNMP singkatan dari Simple Network Management Protocol. Protokol ini digunakan untuk memonitor device-device yang terhubung ke jaringan akan kondisi-kondisi systemnya yang penting. Sebagai contoh penggunaan CPU, penggunaan harddisk, penggunaan memory, traffic jaringan dan lain-lain. Untuk device-device yang dapat dipantau adalah device-device seperti PC, Server, atau router. Sedangkan Operating System bisa Linux, *Nix, Windows, atau yang lain.

Dengan Adanya SNMP tidak perlu memeriksa-memeriksa satu-satu server, tetapi anda cukup mengakses satu komputer untuk melihat kondisi seluruh server dan router. Hal ini disebabkan server dan router akan bertindak sebagai SNMP-server yang tugasnya yang menyediakan requset SNMP dari komputer lain. Satu PC akan bertindak sebagai SNMP Agent yaitu komputer yang mengumpulkan informasi-informasi dari SNMP-servers.

Selain digunakan untuk memonitoring sebetulnya SNMP dapat digunakan untuk melakukan perubahan dan memberikan konfigurasi baru ke server. Tetapi pengubahan konfigurasi system di server hanya dilakukan apabila ada perubahan infrastruktur di jaringan.

Nilai-nilai variabel yang diakses menggunakan SNMP diatur dalam bentuk

hirarki. Tipe hirarki dan metadata (seperti tipe dan deskripsi variabel) diatur oleh Management Information Bases (MIBs).



Gambar 4.25 Diagram Model Protokol Manajemen Jaringan Sederhana (SNMP)

Ada dua jenis perangkat SNMP. Pertama adalah Managed Nodes yang merupakan node biasa pada jaringan yang telah dilengkapi dengan software supaya mereka dapat diatur menggunakan SNMP. Mereka biasanya adalah perangkat TCP/IP biasa; mereka juga kadang-kadang disebut managed devices. Managed nodes bisa berupa perangkat jaringan apa saja yang dapat berkomunikasi menggunakan TCP/IP, sepanjang diprogram dengan software SNMP. SNMP didesain supaya host biasa dapat diatur, demikian juga dengan perangkat pintar seperti router, bridge, hubs, dan switch. Perangkat yang “tidak konvensional” juga bisa diatur sepanjang mereka terhubung ke jaringan TCP/IP: printer, scanner, dan lain-lain. Masing-masing perangkat dalam

manajemen jaringan yang menggunakan SNMP menjalankan suatu software yang umumnya disebut SNMP entity. SNMP entity bertanggung jawab untuk mengimplementasikan semua beragam fungsi SNMP. SNMP entity pada managed nodes terdiri atas SNMP Agent: yang merupakan program yang mengimplementasikan protokol SNMP dan memungkinkan managed nodes memberikan informasi kepada NMS dan menerima perintah darinya, dan SNMP Management Information Base (MIB): yang menentukan jenis informasi yang disimpan tentang node yang dapat dikumpulkan dan digunakan untuk mengontrol managed nodes. Informasi yang dikirim menggunakan SNMP merupakan objek dari MIB.

Kedua adalah Network Management Station (NMS) yang merupakan perangkat jaringan khusus yang menjalankan software tertentu supaya dapat mengatur managed nodes. Pada jaringan harus ada satu atau lebih NMS karena mereka adalah perangkat yang sebenarnya “menjalankan” SNMP. Pada jaringan yang lebih besar, NMS bisa saja terpisah dan merupakan komputer TCP/IP bertenaga besar yang didedikasikan untuk manajemen jaringan. Namun, adalah software yang sebenarnya membuat suatu perangkat menjadi NMS, sehingga suatu NMS bisa bukan hardware terpisah. Ia bisa berfungsi sebagai NMS dan juga melakukan fungsi lain. SNMP entity pada NMS terdiri dari SNMP Manager: yang merupakan program yang mengimplementasikan SNMP sehingga NMS dapat mengumpulkan informasi dari managed nodes dan mengirim perintah kepada mereka, dan SNMP Application: yang merupakan satu atau lebih aplikasi yang memungkinkan administrator jaringan untuk menggunakan SNMP dalam mengatur jaringan. Dengan demikian, secara keseluruhan SNMP terdiri dari sejumlah NMS yang berhubungan dengan perangkat TCP/IP biasa yang disebut managed nodes. SNMP manager pada NMS dan SNMP agent pada managed nodes mengimplementasikan SNMP dan memungkinkan informasi manajemen jaringan dikirim. SNMP application berjalan pada NMS dan menyediakan interface untuk administrator, dan memungkinkan informasi dikumpulkan dari MIB pada masing-masing SNMP agent.

Model umum yang digunakan SNMP adalah adanya network management station (NMS) yang mengirim request kepada SNMP agent. SNMP Agent juga bisa melakukan komunikasi dengan mengirim pesan trap untuk memberitahu management station ketika terjadi suatu event tertentu. Model ini bekerja dengan baik, yang mana inilah mengapa SNMP menjadi sangat populer. Namun, satu masalah mendasar dari protokol dan model yang digunakan adalah bahwa ia diorientasikan pada komunikasi dari SNMP agent yang biasanya perangkat TCP/IP seperti host dan router. Jumlah informasi yang dikumpulkan oleh perangkat ini biasanya terbatas, karena sudah pasti host dan router mempunyai “tugas sebenarnya yang harus dilakukan”—yaitu melakukan tugas sebagai host dan router. Mereka tidak bisa mendedikasikan diri mereka untuk melakukan tugas manajemen jaringan. Oleh karena itu, pada situasi di mana dibutuhkan

informasi jaringan yang lebih banyak dibanding yang dikumpulkan oleh perangkat biasa, administrator sering kali menggunakan hardware khusus bernama network analyzer, monitor,atau

probe. Mereka hanya mengumpulkan statistik dan memantau event yang diinginkan oleh administrator. Jelas akan sangat berguna jika perangkat tersebut dapat menggunakan SNMP supaya informasi yang mereka kumpulkan bisa diterima, dan membiarkan mereka mengeluarkan pesan trap ketika ada sesuatu yang penting.

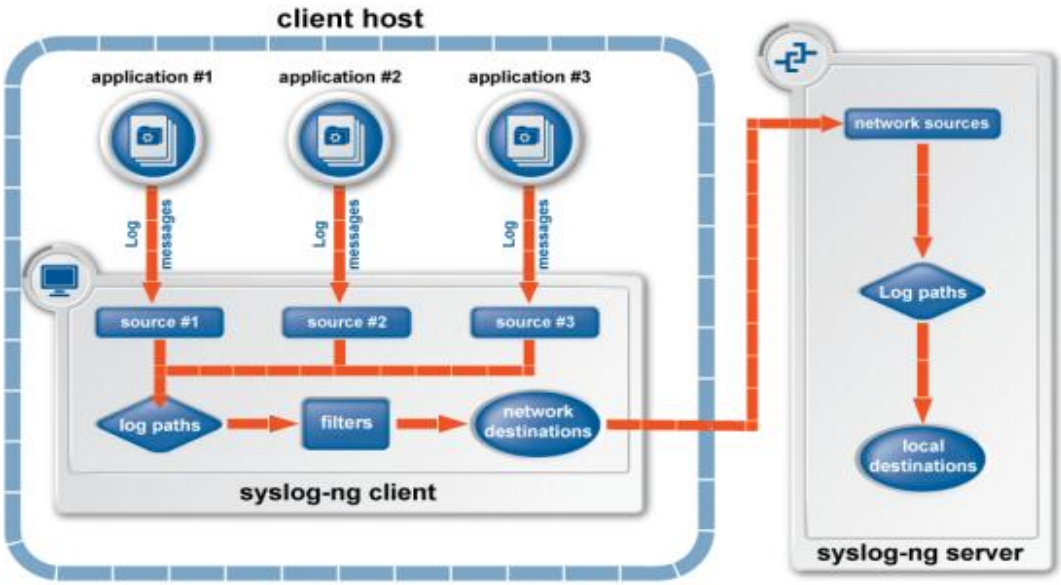
Untuk melakukan itu, dibuatlah Remote Network Monitoring (RMON). RMON sering kali disebut sebagai protokol, dan Anda kadang-kadang akan melihat SNMP dan RMON disebut sebagai “protokol manajemen jaringan TCP/IP”. Namun, RMON sama sekali bukan protocol yang terpisah—ia tidak melakukan operasional protokol. RMON sebenarnya adalah bagian dari SNMP, dan RMON hanya suatu modul management information base (MIB) yang menentukan objek MIB yang digunakan oleh probe. Secara arsitektur, RMON hanyalah salah satu modul MIB yang menjadi bagian dari SNMP.

- Syslog

Segala kegiatan di sistem UNIX (dan variannya seperti Linux, FreeBSD, Solaris, AIX, HP- UX dan sejenisnya) dapat dicatat. Pencatatan ini digunakan untuk kebutuhan audit, yaitu memeriksa sistem jika dibutuhkan. Misalnya, jika terjadi kesalahan (error) maka administrator dapat lebih mudah mencari sumber kesalahan karena informasinya tercatat dengan rapi. Demikian pula jika terjadi penyalahgunaan fasilitas, maka dapat diketahui siapa yang melakukannya dan apa saja yang dilakukannya. Pencatatan kegiatan dilakukan dengan menuliskan data-data ke dalam berkas catatan yang sering disebut dengan nama “logfile” atau berkas log. Proses pencatatan ini sendiri sering disebut dengan istilah logging.

Pada mulanya pencatatan ini dilakukan sekehendak dari sang pembuat program. Berkas log dapat disimpan dimana saja dengan format yang berbeda-beda. Bayangkan sebuah sistem UNIX yang memiliki banyak fungsi misalnya sebagai server database, server web, server email, dan seterusnya. Pencatatan yang berbeda-beda ini tentunya akan membingungkan administrator sehingga akhirnya muncul standar logging yang menggunakan fasilitas atau program “syslog”.

Program syslog pada mulanya dikembangan oleh Eric Allman (yang juga membuat program mail sendmail). Saat ini sudah ada beberapa variasi dari program syslog tersebut. Namun pada intinya fungsinya adalah sama. Program syslog ini mencatat kegiatan dalam sebuah format yang standar. Letak logfile dan apa saja yang dicatat dapat diatur oleh sebuah berkas konfigurasi (syslog.conf) yang biasanya berada di direktori /etc.



Gambar 4.26 Diagram Pencatatan Di Server Syslog

- Backup dan recovery

Pengertian backup data adalah memindahkan atau menyalin kumpulan informasi (data) yang tersimpan di dalam hardisk komputer yang biasanya dilakukan dari satu lokasi/perangkat ke lokasi/perangkat lain. Data atau kumpulan informasi tersebut bisa berupa file dokumen, gambar, video, audio, system windows, driver, atau software/program tertentu. Kegunaan atau manfaat back up data yaitu kita masih mempunyai cadangan data dari data yang hilang/rusak/terhapus, baik yang disebabkan oleh kesalahan kita sendiri atau faktor lain di luar kemampuan kita, seperti: terkena virus, file rusak (tidak bisa dibuka), perangkat komputer error/bermasalah, mati listrik, bencana, dan lain sebagainya.

Dengan begitu cadangan data yang sudah kita simpan tersebut dapat kita gunakan kembali sebagai pengganti data yang telah hilang/rusak/terhapus tadi. Fungsi back up data lebih mengacu pada faktor keamanan dan kenyamanan dalam menggunakan komputer.

Beberapa sebab kerusakan atau kegagalan operasi adalah:

- Aliran listrik terputus, yang dapat mengakibatkan hilangnya informasi yang ada dimemori utama dan register.
- Kesalahan operator (human error), dimana operator/manusia melakukan kesalahan operasi yang tidak disengaja.
- Kesalahan perangkat lunak, yang dapat mengakibatkan hasil pengolahan (akhir/antara) tidak benar, informasi yang disajikqan ke user salah, dan basis data menjadi tidak konsisten.
- Disk rusak,yang dapat mengakibatkan hilangnya informasi atau rusaknya basis data yang ada dalam disk.

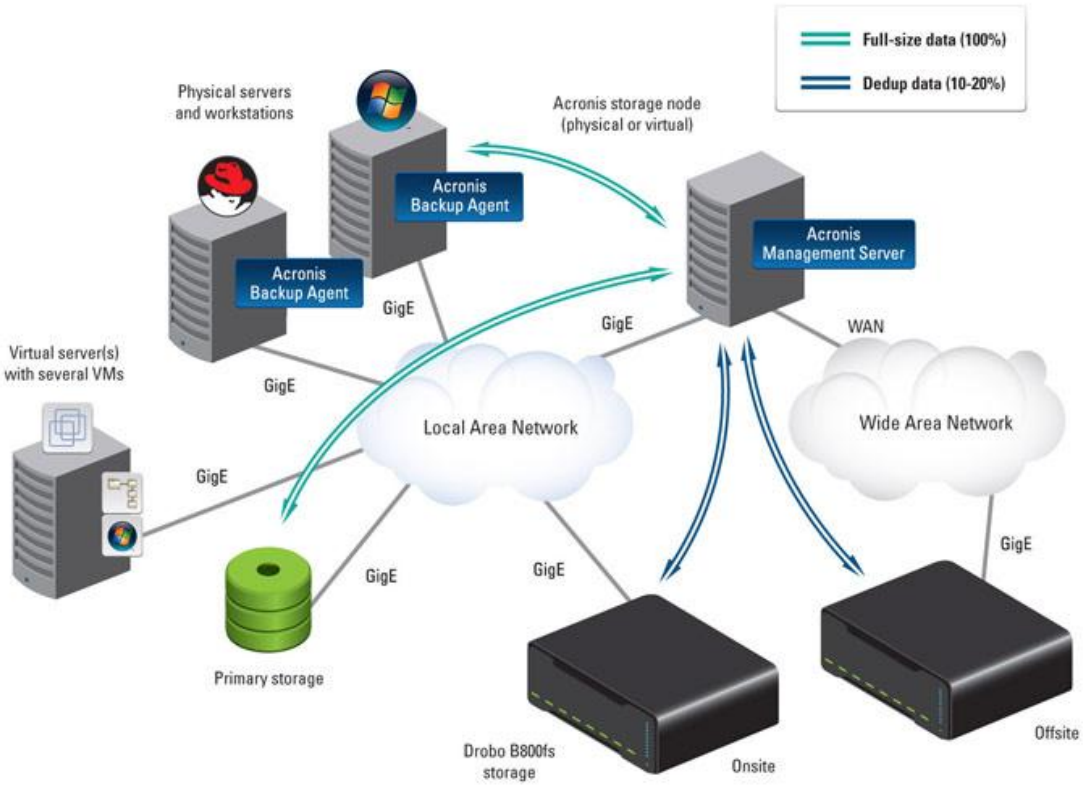
- Jenis Kerusakan Dan Jenis Media Penyimpanan

Beberapa jenis kerusakan yang dapat terjadi diantaranya adalah:

– Kegagalan transaksi (transaksi failure)

Ada beberapa jenis kesalahan yang dapat menyebabkan sebuah transaksi menjadi gagal:

- Kesalahan logika (logical error), dimana program tidak dapat melanjutkan eksekusi normalnya karena adanya kondisi internal tertentu seperti masukan yang salah/rusak, data yang tidak tersedia, nilai data di luar batas domain yang diperbolehkan (overflow), logika program yang tidak tepat.
- Kesalahan sistem (system error), dimana program/ sistem telah memasuki kondisi yang tidak diharapkan (seperti deadlock), sebagai hasil dari tidak tereksekusinya program/sistem secara normal.
- Kerusakan sistem (system crash), hardware macet (hang), menyebabkan isi media penyimpanan sementara hilang.
- Kegagalan/ kerusakan disk (disk failure), adanya/ terjadinya bad sector atau disk macet pada saat berlangsungnya operasi I/O ke disk.



Gambar 4.27 Diagram Backup Dengan Menggunakan Aplikasi Acronis

4.1.2.4 Mengasosiasi

Setelah mengikuti kegiatan belajar 4 ini siswa diharapkan dapat menyimpulkan pelbagai hasil percobaan dan pengamatan terkait dengan pertimbangan layanan keamanan ISP (enkripsi data), peralatan pengaman pada ISP (acl, port filtering, firewall, IDS, IPS), monitoring dan pengaturan ISP (Service Level Agreement, SNMP, Syslog) dan backup dan recovery (media, file).

4.1.3 Rangkuman

Layanan yang diberikan oleh sebuah ISP tidak hanya terbatas pada layanan untuk memenuhi kebutuhan pengguna, namun juga layanan yang aman dan nyaman. Hal tersebut terkait dengan faktor keamanan yang dapat disediakan oleh sebuah ISP. Faktor keamanan ini akan menjadi pertimbangan banyak pengguna saat memutuskan untuk menggunakan layanan-layanan sebuah ISP. Mereka harus yakin bahwa data-data yang bersifat rahasia aman untuk melewati jaringan yang disediakan. Selain itu faktor ketersediaan (SLA) sebuah ISP membawa pengaruh besar bagi kelangsungan hidup suatu bisnis. Dengan demikian maka sebuah ISP yang memberikan layanan 1x24jam selama 365 hari dalam setahun dengan waktu downtime yang paling sedikit akan menjadi pilihan bagi perusahaan-perusahaan yang mengantungkan layanan-layanan mereka di jaringan internet maupun jaringan lokal atau antar cabang.

Selain faktor keamanan, kenyamanan dan ketersediaan, sebuah ISP juga harus mampu melakukan perawatan dan pemantauan jaringan yang dikelolanya. Hal ini agar supaya ISP dapat melacak atau dapat melaporkan jika ada suatu pelanggaran yang terjadi dengan menggunakan jaringan mereka. Dan yang terakhir dan tak kalah penting adalah fasilitas backup dan recovery yang dapat digunakan untuk berjaga-jaga jika suatu keadaan yang tidak diharapkan terjadi.

4.1.4 Tugas

Buatlah kelompok terdiri atas 2-3 orang. Masing-masing kelompok membuat ringkasan tentang tugas dan tanggung jawab ISP, kemudian secara bergantian masing-masing kelompok mempresentasikan hasilnya didepan kelas.

1. Bacalah uraian materi diatas dengan teliti dan cermat.
2. Buatlah ringkasan materi menggunakan aplikasi pengolah presentasi.
3. Presentasikan hasil ringkasan di depan kelas.

4.1.5 Penilaian Diri

Setelah mengikuti kegiatan belajar 4 ini siswa diharapkan memiliki wawasan pengetahuan dan dapat menjawab pelbagai hal terkait dengan pertimbangan layanan keamanan ISP (enkripsi data), peralatan pengaman pada ISP (acl, port filtering, firewall, IDS, IPS), monitoring dan pengaturan ISP (Service Level Agreement, SNMP, Syslog) dan backup dan recovery (media, file).

BAB V

5.1 Kegiatan Belajar 5 : Jaringan Di Perusahaan

5.1.1 Tujuan Pembelajaran

Setelah mengikuti kegiatan belajar 5 ini siswa diharapkan dapat memahami tentang jaringan di perusahaan.

5.1.2 Aktifitas Belajar Siswa

5.1.2.1 Mengamati

Melalui kegiatan belajar 5 ini siswa diharapkan dapat melakukan pengamatan mengenai :

- Trafik yang mengalir pada jaringan perusahaan
- LAN dan WAN perusahaan
- Intranet dan ekstranet
- Iaplikasi-aplikasi perusahaan dan pola trafik yang mengalir
- Aplikasi-aplikasi dan trafik pada jaringan perusahaan
- Prioritas trafik jaringan
- Asas teleworking dan VPN

5.1.2.2 Menanya

Melalui kegiatan belajar 5 ini siswa diharapkan dapat melakukan :

- Mendiskusikan trafik yang mengalir pada jaringan perusahaan
- Mendiskusikan LAN dan WAN perusahaan
- Mendiskusikan intranet dan ekstranet
- Mendiskusikan aplikasi-aplikasi perusahaan dan pola trafik yang mengalir
- Mendiskusikan aplikasi-aplikasi dan trafik pada jaringan perusahaan
- Mendiskusikan prioritas trafik jaringan
- Mendiskusikan asas teleworking dan VPN

5.1.2.3 Mengumpulkan Informasi

Jaringan Perusahaan

Ada prinsip-prinsip yang harus diperhatikan dalam membangun jarkom kantor atau perusahaan yang semuanya tidak lepas dari prinsip keamanan jaringan. Ada tiga pilar yang harus diperhatikan yang merupakan objective dari prinsip keamanan jaringan yaitu:

- High Availability (HA)

Bahwa sistem infrastruktur jaringan komputer perusahaan anda harus bisa memberikan layanan dengan tingkat ketersediaan yang tinggi (high availability) terhadap semua user yang mendapatkan authorisasi terhadap informasi perusahaan tersebut termasuk system yang mendukungnya bisa mengaksesnya dengan mudah dan tanpa kendala.

Tingkat ketersediaan layanan ini tergantung pada seberapa kritis perusahaan anda bergantung pada system infrastructure jarkom ini. Adakalanya perusahaan kecil menengah mengabaikan prinsip availability ini karena tingkat ketergantungan terhadap system kecil atau buruknya lagi adalah bahwa mereka kurang sadar bahwa ketergantungan mereka terhadap system sangat tinggi akan tetapi mereka tidak sadar bahwa system mereka tidak dibangun secara redundansi. Sehingga akibatnya begitu system down, semua user tidak bisa akses data perusahaan dan akibatnya perusahaan kehilangan produktifitas karyawan. Dan jika

system ini sudah terintegrasi dengan system produksi bisa dibayangkan berapa kerugian jika terjadi system down selama beberapa jam atau mungkin saja system jaringan komputer down selama satu atau dua minggu karena suatu disaster katakan kebakaran ruang server. Jadi jika jaringan komputer perusahaan mengabaikan prinsip availability menjadi tidak ada bedanya dengan jaringan yang ada dirumah sendiri.

- Integrity

Pilar kedua manajemen informasi technology dalam jaringan komputer perusahaan anda adalah integrity. System anda harus bisa menjaga keakuratan dan kelengkapan dari informasi dan metoda-metoda proses yang berkaitan. Dalam pertukaran informasi antar dua party integritas data informasi kritis perusahaan harus tetap terjaga. Data kritis perusahaan hanya boleh dan bisa diubah atau di update oleh user yang memang authorize untuk itu. Tidak boleh ada pihak ketiga bisa mengubah integritas data tersebut termasuk oleh infeksi virus atau dibajak dalam perjalanannya dari satu titik awal ke titik destinasi. Untuk itulah, jika data melewati jaringan public maka enkripsi data harus dilakukan. Koneksi lewat internet harus menggunakan certificate yang terpercaya agar integritas data tetap terjaga. Koneksi clients ke jaringan komputer perusahaan harus melalui protocol enkripsi SSL.

- Confidentiality

Pilar ketiga adalah confidentiality yang merupakan jaminan bahwa system jaringan komputer perusahaan anda hanyalah diperuntukkan bagi mereka yang berhak saja. System keamanan data kritis perusahaan anda harus sangat secure dari segala unauthorized access. Jaringan komputer bisnis anda haruslah aman dari segala bentuk compromi baik dari dalam terlebih dari external melalui intrusi end-point jaringan yang menghadap langsung kepada internet. System firewall dan router harus sangat kuat dengan rule base policy yang didefinisikan secara exclusive agar segala inbound traffic hanyalah yang permitted saja. Secara default semua inbound traffic harus access denied kecuali yang didefinisikan secara exclusive.

Jadi ada prinsip-prinsip manejemen informasi yang harus diterapkan sesuai kebutuhan bisnis anda. Akan tetapi tidak semua jaringan komputer perusahaan dirancang dengan benar sesuai prinsip tiga pilar tersebut diatas.

LAN Dan WAN

- *LAN*

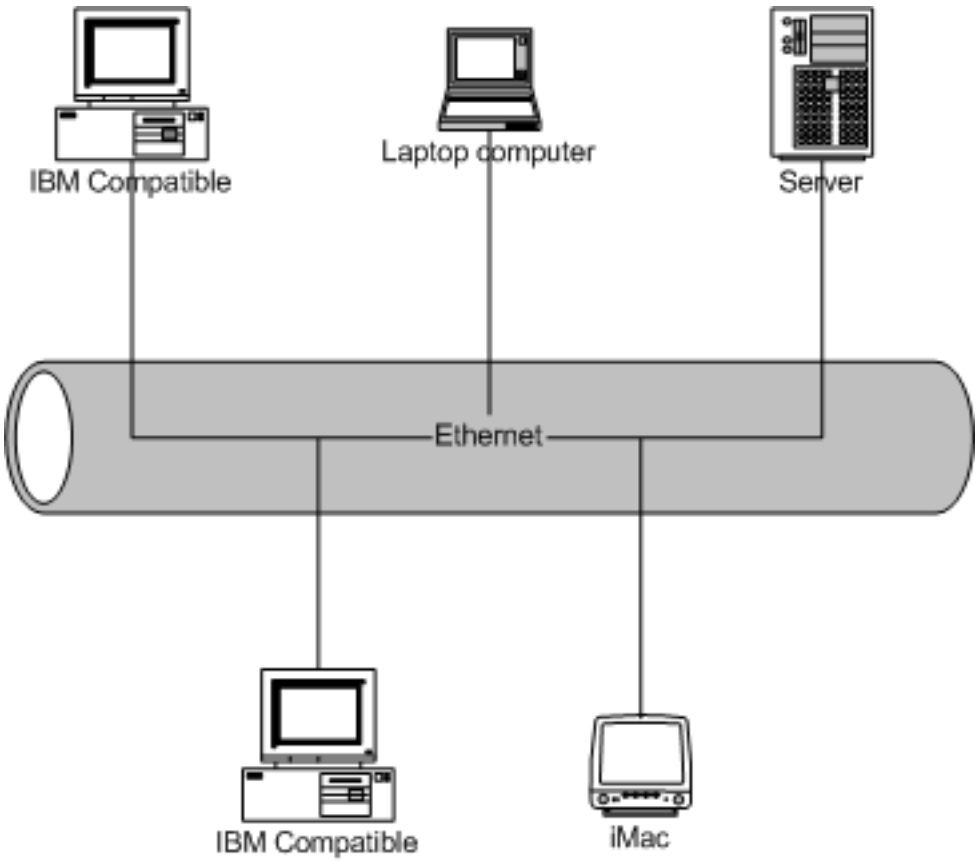
Jaringan wilayah lokal (bahasa Inggris: *local area network* biasa disingkat LAN) adalah jaringan komputer yang jaringannya hanya mencakup wilayah kecil; seperti jaringan komputer kampus, gedung, kantor, dalam rumah, sekolah atau yang lebih kecil. Saat ini, kebanyakan LAN berbasis pada teknologi IEEE 802.3 Ethernet menggunakan perangkat switch, yang mempunyai kecepatan transfer data 10, 100, atau 1000 Mbit/s. Selain teknologi Ethernet, saat ini teknologi 802.11b (atau biasa disebut

Wi-fi) juga sering digunakan untuk membentuk LAN. Tempat-tempat yang menyediakan koneksi LAN dengan teknologi *Wi-fi* biasa disebut *hotspot*.

Pada sebuah LAN, setiap node atau komputer mempunyai daya komputasi sendiri, berbeda dengan konsep *dump terminal*. Setiap komputer juga dapat mengakses sumber daya yang ada di LAN sesuai dengan hak akses yang telah diatur. Sumber daya tersebut dapat berupa data atau perangkat seperti printer. Pada LAN, seorang pengguna juga dapat berkomunikasi dengan pengguna yang lain dengan menggunakan aplikasi yang sesuai.

Berbeda dengan Jaringan Area Luas atau Wide Area Network (WAN), maka LAN mempunyai karakteristik sebagai berikut :

- Mempunyai pesat data yang lebih tinggi
- Meliputi wilayah geografi yang lebih sempit
- Tidak membutuhkan jalur telekomunikasi yang disewa dari operator telekomunikasi
- Biasanya salah satu komputer di antara jaringan komputer itu akan digunakan menjadi server yang mengatur semua sistem di dalam jaringan tersebut.



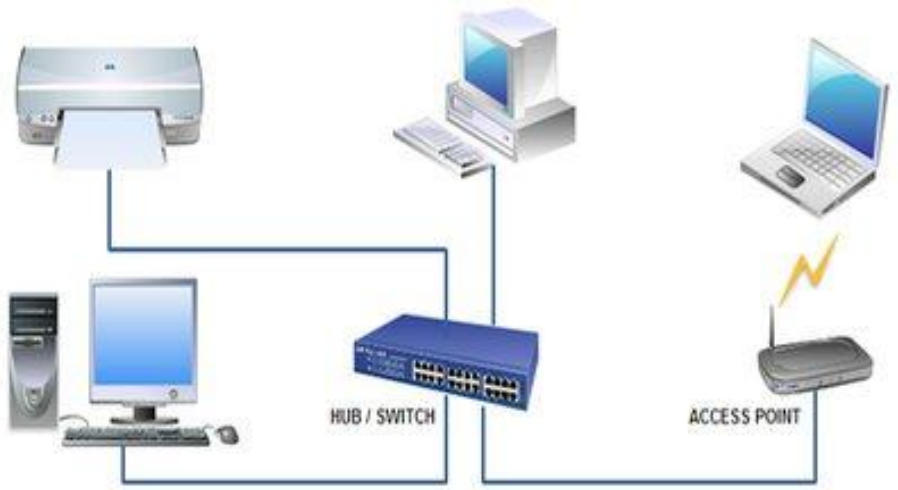
Gambar 5.1 Diagram Jaringan LAN Berbasis Ethernet

Sejarah LAN

Peningkatan permintaan dan penggunaan komputer di universitas dan laboratorium riset pada akhir tahun 1960an membutuhkan tersedianya interkoneksi kecepatan tinggi antar sistem komputer. Sebuah laporan dari Lawrence Radiation Laboratory pada tahun 1970 menjelaskan pertumbuhan jaringan *Octopus* mereka memberikan indikasi situasi yang bagus. Cambridge Ring dibangun di Universitas Cambridge pada tahun 1974 namun tidak sukses sampai ke tahap produk komersial.

Ethernet dibangun di Xerox PARC tahun 1973 - 1975 dan dipatenkan di Amerika (U.S. Patent 4.063.220). Pada tahun berikutnya setelah sistem selesai dibangun di PARC, Metcalfe dan Boggs mengumumkan makalah "Ethernet: Distributed Packet-Switching For Local Computer Networks."

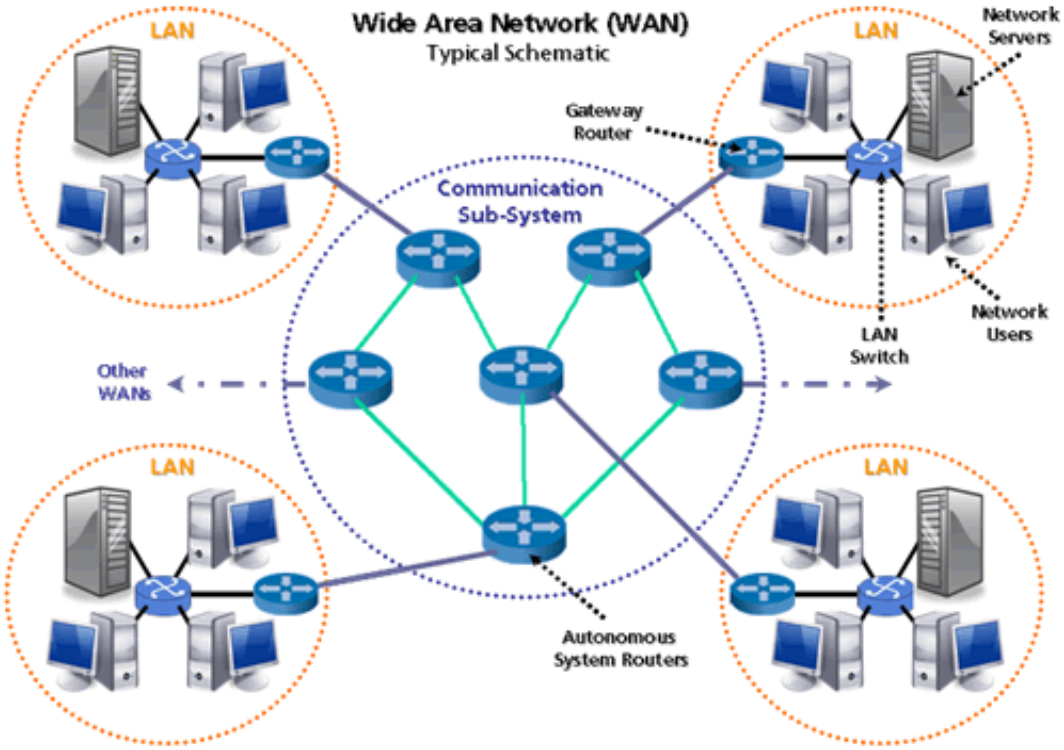
ARCNET dibangun oleh perusahaan Datapoint pada tahun 1976 dan diumumkan tahun 1977. Itu adalah instalasi komersial pertama dibuka pada bulan Desember 1977 di Chase Manhattan Bank New York.



Gambar 5.2 Diagram LAN Menggunakan Hub/Switch

WAN

WAN adalah singkatan dari Wide Area Network adalah suatu jaringan yang digunakan sebagai jaringan yang menghubungkan antar jaringan lokal. Jaringan komputer lokal secara fisik tidak hanya yang berdekatan satu sama lain, namun menggunakan satu grup alamat IP yang sama. Jaringan lokal bisa satu ruangan, satu kantor atau bahkan satu kota. Sedangkan WAN sendiri adalah jaringan yang menghubungankan antar jaringan lokal ini dalam satu kota, provinsi atau bahkan antar negara. Perbedaan antara jaringan WAN dan LAN ada pada jenis media yang digunakan. Umumnya jaringan lokal atau LAN menggunakan media jaringan yang sejenis. Sedangkan WAN terhubung dengan perangkat dengan media transmisi dan protokol yang berbeda-beda. Area cakupan WAN juga sangat luas, namun menyatukan jaringan tersebut seolah-olah seperti berada dalam satu ruangan. Jaringan WAN memiliki kecepatan transfer data yang lebih rendah daripada jaringan lokal atau LAN.Teknologi jaringan WAN bergantung pada perusahaan yang menyediakan jasa layanan telekomunikasi jarak jauh. Jaringan WAN menggunakan banyak macam teknologi jaringan dengan perpaduan sinyal analog dan digital untuk transmisi data. Tentu saja ini berbeda dengan jaringan lokal atau LAN yang mana menggunakan koneksi antar komputer yang terkoneksi secara fisik satu sama lainnya dengan protokol dan media transmisi yang sama.

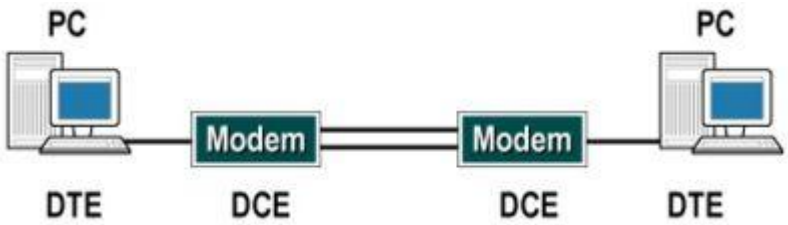


Gambar 5.3 Diagram Jaringan WAN

Komponen WAN

- Data Terminal Equipment (DTE)

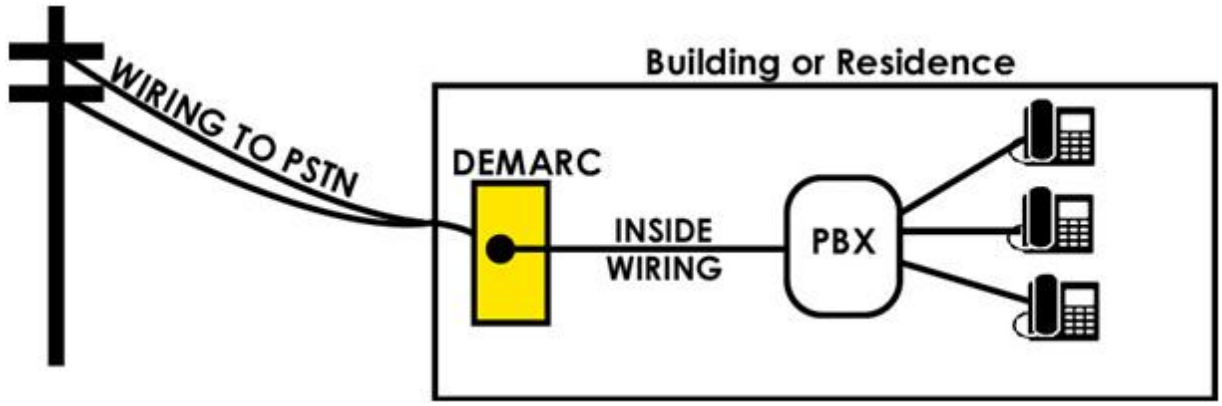
DTE adalah suatu komponen yang menyusun jaringan WAN yang posisinya berada di pihak pelanggan, seperti misalnya gedung atau rumah. Komponen jaringan ini berfungsi untuk mengirim dan menerima data. Komponen DTE umumnya berupa router atau kadang juga komputer. DTE ini merupakan tanda batas antara jaringan lokal dan WAN. DTE inilah yang akan berkomunikasi dengan DTE di ujung yang lain.



Gambar 5.4 Komponen DTE Dalam Jaringan WAN

- Demarc

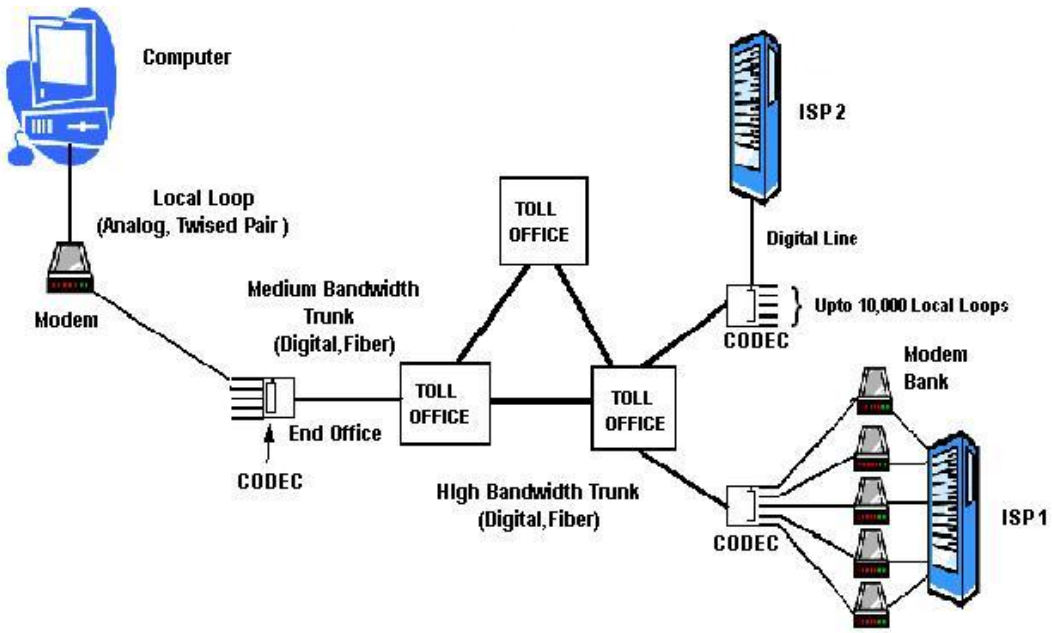
Demarc merupakan salah satu komponen jaringan WAN yang disebut juga demarkasi yang merupakan tampilan antarmuka atau interface yang menghubungkan antara rumah dan sambungan dari perusahaan telekomunikasi, yang bisa menggunakan fiber optik atau kabel tembaga.



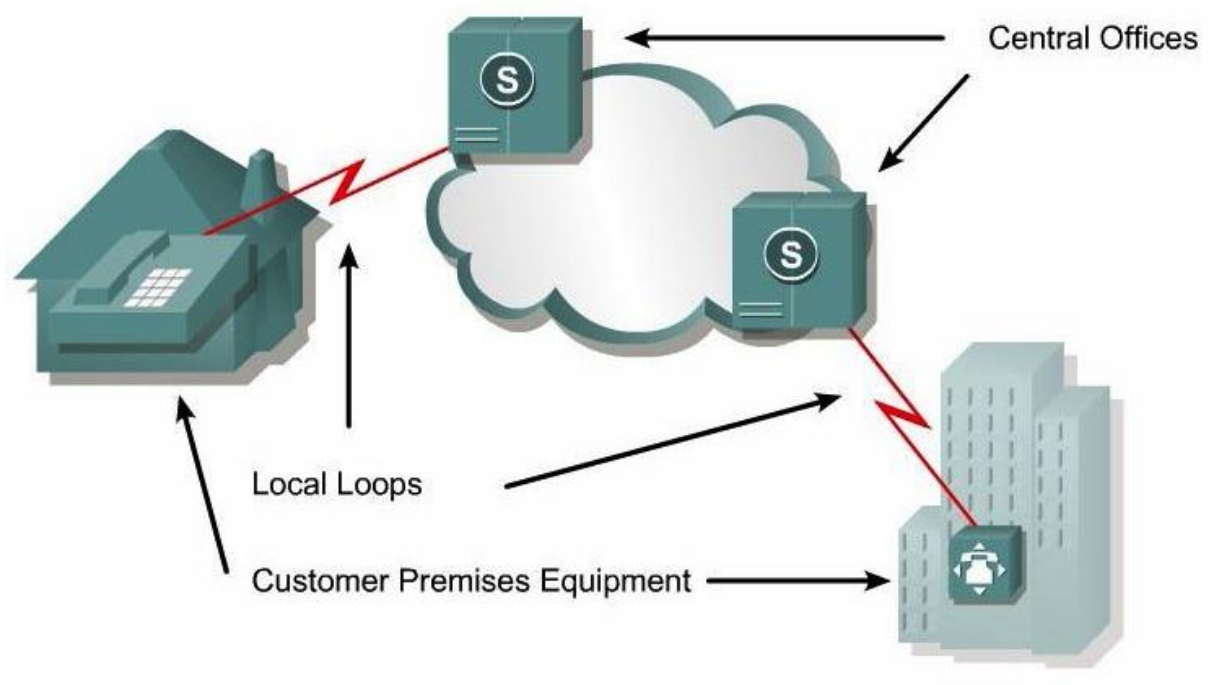
Gambar 5.5 Posisi Komponen Demarc Dalam Suatu Jaringan

- Local Loops

Local loops adalah komponen penyusun WAN yang merupakan perpanjangan jaringan telepon dari komponen Demarc menuju kantor pusat dari penyedia layanan telekomunikasi. Perawatan komponen Local Loops ini adalah tanggung jawab dari penyedia layanan telekomunikasi. Umumnya komponen ini berupa kabel UTP, fiber optik, tembaga biasa atau gabungan dari ketiganya.



Gambar 5.6 Komponen Local Loops Dalam Suatu Jaringan



Gambar 5.7 Contoh Local Loops Pada Jaringan

- Data Communication Equipment

DCE adalah komponen penyusun jaringan yang berkomunikasi dengan DTE dan WAN secara keseluruhan. Perangkat ini ada di sisi penyedia jasa atau ISP. Umumnya, komponen ini berupa router yang berada di sisi ISP yang menyambungkan sinyal-sinyal pada DTE. Dengan kata lain, sebuah modem dapat dikatakan DCE dan DTE yang pirantinya sama namun memiliki fungsi yang sedikit berbeda karena terletak di tempat yang berbeda.

Gambar 5.8 Komponen DCE Pada Jaringan WAN

Intranet Dan Ekstranet

- *Intranet*

Sebuah intranet adalah sebuah jaringan privat (*private network*) yang menggunakan protokol-protokol Internet (TCP/IP), untuk membagi informasi rahasia perusahaan atau operasi dalam perusahaan tersebut kepada karyawannya. Kadang-kadang, istilah intranet hanya merujuk kepada layanan yang terlihat, yakni situs web internal perusahaan. Untuk membangun sebuah intranet, maka sebuah jaringan haruslah memiliki beberapa komponen yang membangun Internet, yakni protokol Internet

(Protokol TCP/IP, alamat IP, dan protokol lainnya), klien dan juga server. Protokol HTTP dan beberapa protokol Internet lainnya (FTP, POP3, atau SMTP) umumnya merupakan komponen protokol yang sering digunakan. Umumnya, sebuah intranet dapat dipahami sebagai sebuah "versi pribadi dari jaringan Internet", atau sebagai sebuah versi dari Internet yang dimiliki oleh sebuah organisasi.

Intranet mulai diperkenalkan pada tahun 1995 oleh beberapa penjual produk jaringan yang mengacu kepada kebutuhan informasi dalam bentuk web di dalam perusahaan. Intranet merupakan jaringan komputer dalam perusahaan yang menggunakan komunikasi data standar seperti dalam internet. Artinya, semua fasilitas intranet dapat digunakan untuk kebutuhan dalam suatu organisasi atau komunitas. Saat ini perangkat elektronik pintar sudah merambah di seluruh aspek kehidupan contohnya di kantor, sekolah, rumah. Beberapa sekolah sudah menerapkan teknologi intranet. Seluruh komputer terhubung dengan satu jaringan lokal. Intranet sebagai pendatang baru mengandalkan biaya yang murah, fleksibilitas, open standard, dan banyaknya vendor yang bergabung dalam menigkatkan kemampuan intranet serta jaminan perkembangan teknologi yang makin meningkat kemampuannya.

Intranet digunakan untuk membantu alat dan aplikasi, misalnya kolaborasi dalam kerja sama (untuk memfasilitasi bekerja dalam kelompok dan telekonferensi) atau direktori perusahaan yang sudah canggih, penjualan dan alat manajemen hubungan dengan pelanggan, manajemen proyek dll, untuk memajukan produktivitas. Intranet juga digunakan sebagai budaya perusahaan perubahan platform. Sebagai contoh, sejumlah besar karyawan membahas isu-isu kunci dalam aplikasi forum intranet dapat menyebabkan ide-ide baru dalam manajemen, produktivitas, kualitas, dan isu-isu perusahaan lainnya. Dalam intranet yang besar, lalu lintas situs web seringkali sama dengan lalu lintas situs Web publik dan dapat dipahami dengan lebih baik dengan menggunakan software web metrik untuk melacak aktivitas secara keseluruhan. Survei pengguna juga meningkatkan efektivitas situs intranet. Bisnis yang lebih besar memungkinkan pengguna dalam intranet mereka untuk mengakses internet publik melalui server firewall. Mereka memiliki kemampuan menangani pesan yang datang dan pergi serta menjaga keamanan yang utuh.

Ketika bagian dari intranet diakses oleh pelanggan dan lainnya di luar bisnis, menjadi bagian dari sebuah extranet. Bisnis dapat mengirim pesan pribadi melalui jaringan publik, menggunakan enkripsi khusus / dekripsi dan perlindungan keamanan lainnya untuk menghubungkan satu bagian dari intranet mereka yang lain.

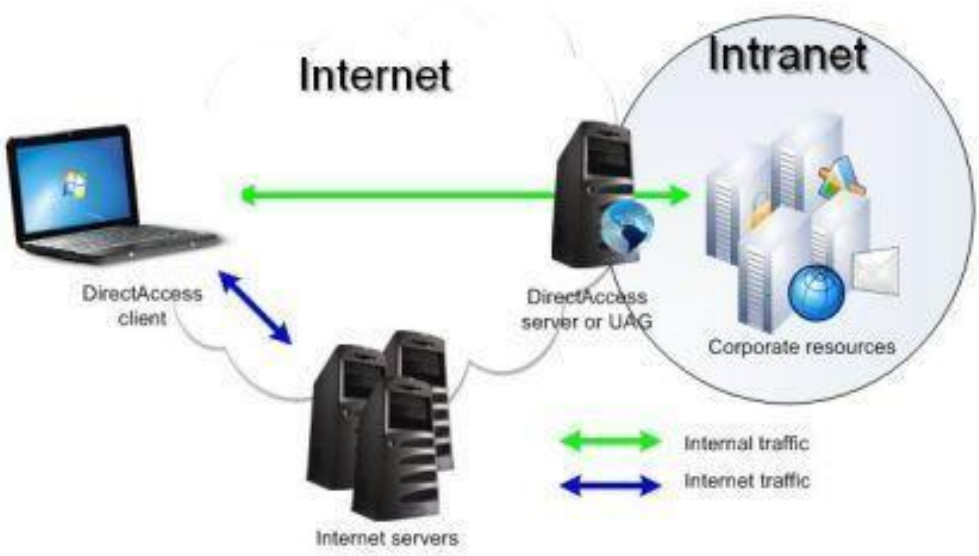
Pengguna intranet yang berpengalaman, editorial, dan tim teknologi bekerja sama untuk menghasilkan website. Paling umum, intranet dikelola oleh departemen komunikasi,

HR atau CIO organisasi besar, atau kombinasinya.

Kebutuhan intranet didorong oleh beberapa tekanan teknologi yaitu :

– Intranet menjadi alat bantu untuk meningkatkan perkembangan dan pertumbuhan produk industri
– Intranet lebih meningkatkan tanggapan terhadap keluhan dan kebutuhan pelanggannya.
– Intranet mampu menurunkan biaya atas kebutuhan informasi kolaborasi, workflow, dan enterprise connectivity.

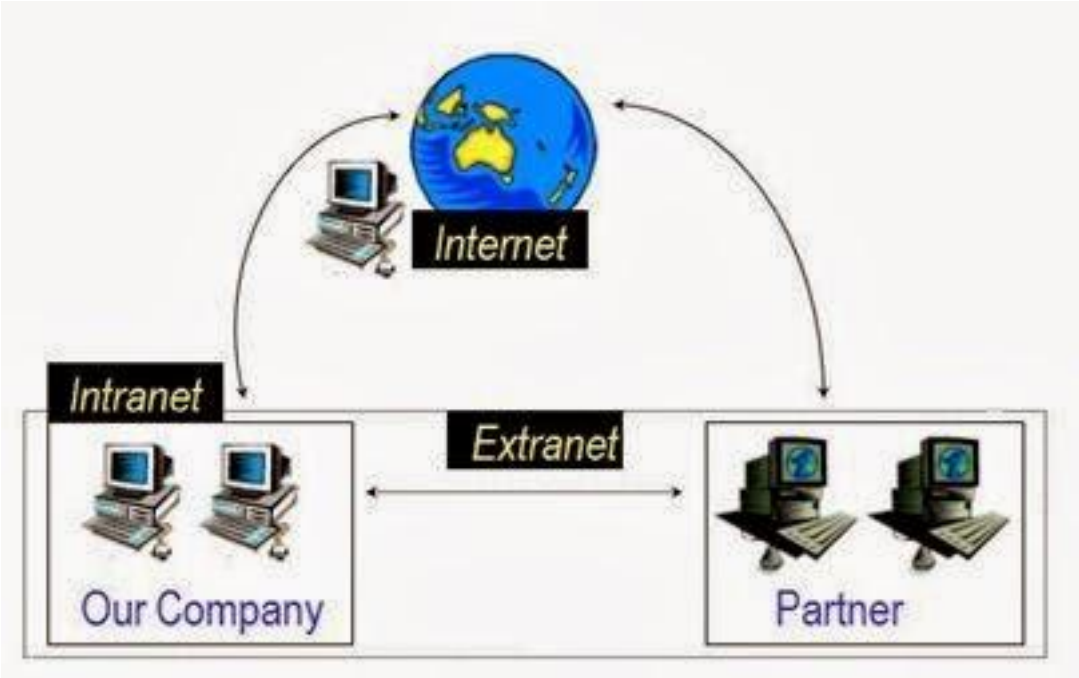
Intranet mendapat banyak keuntungan karena adanya suksesnya dukungan world wide web yang memungkinkan penggunaan yang luas karena digunakan masyarakat luas yang menggunakan internet. Caranya adalah dengan membuat website. Intranet menjadi tren saat ini karena kefleksibelan webnya yang mudah digunakan.



Gambar 5.9 Contoh Suatu Jaringan Intranet

Ekstranet

Extranet atau Ekstranet adalah jaringan pribadi yang menggunakan protokol internet dan sistem telekomunikasi publik untuk membagi sebagian informasi bisnis atau operasi secara aman kepada penyalur (*supplier*), penjual (*vendor*), mitra (*partner*), pelanggan dan lain-lain. Extranet dapat juga diartikan sebagai intranet sebuah perusahaan yang dilebarkan bagi pengguna di luar perusahaan. Perusahaan yang membangun extranet dapat bertukar data bervolume besar dengan EDI (*Electronic Data Interchange*), berkolaborasi dengan perusahaan lain dalam suatu jaringan kerjasama dan lain-lain. Contoh aplikasi yang dapat digunakan untuk extranet adalah Lotus Notes.



Gambar 5.10 Contoh Jaringan Ekstranet

Asas Teleworking Dan VPN

- *Teleworking*

Telework adalah model atau perjanjian kerja di mana karyawan memperoleh fleksibilitas bekerja dalam hal tempat dan waktu kerja dengan bantuan teknologi telekomunikasi. Dengan kata lain, kegiatan bepergian ke kantor atau tempat kerja digantikan dengan hubungan telekomunikasi. Dengan sistem ini, banyak karyawan yang pada akhirnya bekerja di rumah, sementara lainnya, yang lazim disebut pekerja nomaden (nomad workers) atau web commuters menggunakan teknologi komunikasi untuk bekerja dari kafe atau tempat lain yang nyaman bagi mereka. Telework, di sisi lain, merupakan istilah yang bermakna lebih luas lagi. Telework merujuk pada penggantian segala bentuk teknologi telekomunikasi yang terkait dengan pekerjaan-yang-perlu-bepergian, yang pada akhirnya mengurangi hambatan jarak dengan telecommuting. Seseorang yang ber-telecommuting biasa disebut dengan “telecommuter”. Motto yang sering didengungkan oleh para telecommuter adalah “pekerjaan adalah sesuatu yang kita lakukan, bukan dan bukan tujuan bepergian.

Agar telecommuting dapat berjalan dengan baik, diperlukan gaya manajemen yang baik, yang didasarkan dan ditujukan pada hasil, bukan pengamatan yang mendetil dari masing-masing karyawan secara individual. Hal ini menunjuk pada manajemen berbasis tujuan (management by objectives) yang bertolakbelakang dengan manajemen berbasis observasi (management by observation). Istilah telecommuting dan telework sendiri mulai berkembang pada tahun 1973. Penggagasnya bernama Jack Nilles.

Gambar 5.11 Diagram Konsep Teleworking

- VPN

VPN merupakan singkatan dari Virtual Private Network, yaitu sebuah koneksi private melalui jaringan publik (dalam hal ini internet). Dengan VPN ini kita seolah-olah membuat jaringan didalam jaringan atau biasa disebut tunnel (terowongan). **Tunneling** adalah suatu cara membuat jalur privat dengan menggunakan infrastruktur pihak ketiga. VPN menggunakan salah satu dari tiga teknologi tunneling yang ada yaitu: PPTP, L2TP dan standar terbaru, Internet Protocol Security (biasa disingkat menjadi IPSec). VPN merupakan perpaduan antara teknologi tunneling dan enkripsi. VPN merupakan paket solusi komunikasi data (baik berupa data suara, video, atau file digital lainnya) yang memberikan layanan berbasis IP ke end user. Layanan VPN dapat mengirimkan data antar-dua komputer yang melewati jaringan publik, misal nya Internet, sehingga seolah-olah terhubung secara point-to-point.

Perusahaan dengan banyak kantor cabang yang tersebar di berbagai kota. Anda pasti membutuhkan jalur komunikasi private yang terjangkau dan aman, untuk mengontrol dan mengintegrasikan semua proses bisnis di masing-masing kantor. VPN adalah solusi yang tepat untuk menjawab kebutuhan tersebut. Virtual Private Network (VPN), dari namanya saja Anda pasti sudah dapat membayangkan benda apa ini: sebuah jaringan (network) yang tidak private (public), yang dibuat seolaholah private. VPN sangat dibutuhkan sebagai jembatan komunikasi antar beberapa kantor cabang, menggantikan modus komunikasi tradisional menggunakan sambu ngan telepon private (leased line).

Penggunaan banyak sambungan telepon tentu akan membengkakkan fi xed cost. Solusi untuk permasalahan di atas adalah penggunaan VPN yang

memanfaatkan jaringan publik, Internet, sebagai media intranet, sehingga daerah jangkauannya menjadi luas tanpa investasi yang besar. Setiap dibuka kantor baru, Anda cukup menyediakan akses ke Internet, maka tersambunglah kantor tersebut dengan kantor pusat dan kantor-kantor cabang lainnya. Anda sama sekali tidak perlu memasang jaringan sendiri yang merepotkan pengelolaan, serta membutuhkan biaya yang tidak sedikit.

Data dienkapsulasi (dibungkus atau dikenal dengan istilah tunneling) dengan header yang berisi informasi routing untuk mendapatkan koneksi point-to-point, sehingga dapat melewati jaringan Internet dan dapat mencapai tujuan. Sedangkan untuk mendapatkan koneksi yang bersifat private, data yang dikirimkan harus dienkripsi terlebih dahulu untuk menjaga kerahasiaanya, sehingga paket yang tertangkap ketika mele wati jaringan publik tidak terbaca, karena harus melewati proses deskripsi. Dengan demikian, komunikasi antara beberapa kantor cabang yang semula dilakukan secara interlokal melalui sambungan telepon, kini bi sa dilakukan sebagai hubungan lokal.

Penggunaan VPN tidak hanya menekan biaya komunikasi yang harus dikeluarkan perusahaan, tetapi juga menjamin keamanan data yang ditransmisikan melalui jaringan publik dari penyadapan, penyalinan, atau pengubahan yang dilakukan pihak ketiga.

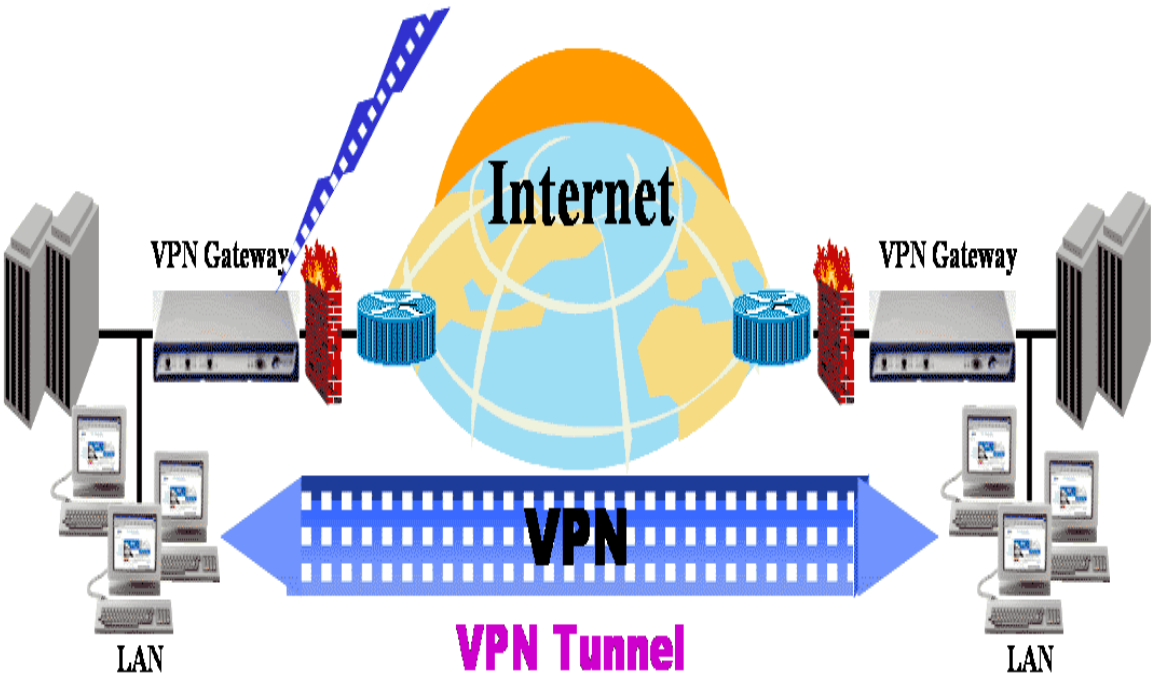
Manfaat & Kegunaan VPN :

– Kemampuan membentuk jaringan LAN yang tidak di batasi tempat dan waktu, karena koneksitasnya dilakukan via internet. Koneksi internet apapun dapat digunakan seperti Dial-Up, ADSL, Cable Modem, WIFI, 3G, CDMA Net, GPRS. Sistem VPN ini paling tepat digunakan untuk penggunaan suatu database terpusat untuk mengkomunikasikan antara server dan client via internet seperti Aplikasi Perdagangan, Purchase, P.O.S, Accounting, Cashir, Billing system, General Ledger, dan lain-lain.
– Tidak ada ketergantungan terhadap keharusan memiliki IP Publik yang berharga mahal. Cukup menggunakan IP dynamic saja dengan kata lain asal PC anda bisa berinternet .
– Bisa print dari rumah ke kantor via internet
– Bisa melakukan transfer data atau remote view untuk mengendalikan komputer dirumah/kantor dimana saja
– Tidak membutuhkan peralatan/hardware tambahan yang berfungsi sebagai IP forwarder/ Port Forwader yang menambah investasi.
– Dimanapun berada seperti sedang berada di warnet ataupun saat traveling di luar negeri, dapat melakukan koneksitas dengan PC dikantor misalnya dengan memanfaatkan software yang bekerja dijaringan LAN seperti Citrix, Windows Terminal Server 2003, VNC, Radmin, VOIP, DLL
– Dengan menggunakan software yang

bekerja dijaringan LAN dapat melakukan pertukaran data secara langsung, printing , remote view, mengatur administrasi PC anda, yang semua itu dapat dilakukan dimanapun berada selama bisa terhubung ke internet

- Dapat mengakses akses yang diblok
- Berselancar dengan aman ketika di akses internet publik / hotspot
- Jika perusahaan ingin mengoptimalkan biaya untuk membangun jaringan mereka yang luas. Oleh karena itu VPN dapat digunakan sebagai teknologi alternatif untuk menghubungkan jaringan lokal yang luas dengan biaya yang relatif kecil, karena transmisi data teknologi VPN menggunakan media jaringan public yang sudah ada.
- Jangkauan jaringan lokal yang dimiliki suatu perusahaan akan menjadi luas, sehingga perusahaan dapat mengembangkan bisnisnya di daerah lain. Waktu yang dibutuhkan untuk menghubungkan jaringan lokal ke tempat lain juga semakin cepat, karena proses instalasi infrastruktur jaringan dilakukan dari perusahaan / kantor cabang yang baru dengan ISP terdekat di daerahnya. penggunaan VPN secara tidak langsung akan meningkatkan efektivitas dan efisiensi kerja.
- Penggunaaan VPN dapat mengurangi biaya operasional bila dibandingkan dengan penggunaan leased line sebagai cara tradisional untuk mengimplementasikan WAN.
- VPN dapat mengurangi biaya pembuatan jaringan karena tidak membutuhkan kabel (leased line) yang panjang. Penggunaan kabel yang panjang akan membutuhkan biaya produksi yang sangat besar. Semakin jauh jarak yang diinginkan, semakin meningkat pula biaya produksinya.
- VPN menggunakan internet sebagai media komunikasinya. Perusahaan hanya membutuhkan biaya dalam jumlah yang relatif kecil untuk menghubungkan perusahaan tersebut dengan pihak ISP (internet service provider) terdekat.
- Penggunaan VPN akan meningkatkan skalabilitas.

VPN memberi kemudahan untuk diakses dari mana saja, karena VPN terhubung ke internet. Sehingga pegawai yang mobile dapat mengakses jaringan khusus perusahaan di manapun dia berada. Selama dia bisa mendapatkan akses ke internet ke ISP terdekat, pegawai tersebut tetap dapat melakukan koneksi dengan jaringan khusus perusahaan



Gambar 5.12 Diagram Konsep Cara Kerja Jaringan VPN

5.1.2.4 Mengasosiasi

Setelah mengikuti kegiatan belajar 5 ini siswa diharapkan dapat menyimpulkan pelbagai hasil percobaan dan pengamatan terkait dengan trafik yang mengalir pada jaringan perusahaan, LAN dan WAN perusahaan, intranet dan ekstranet, aplikasi-aplikasi perusahaan dan pola trafik yang mengalir, aplikasi-aplikasi dan trafik pada jaringan perusahaan, prioritas trafik jaringan, dan asas teleworking dan VPN.

5.1.3 Rangkuman

Jaringan suatu perusahaan terdiri dari berbagai perangkat keras dan perangkat lunak yang secara bersama-sama membentuk suatu sistem jaringan perusahaan yang menyokong kelangsungan bisnis perusahaan tersebut. Oleh karena itu maka dalam pembuatan jaringan perusahaan harus diperhatikan hal-hal yang menjadi pilar dari jaringan itu sendiri. Hal ini penting untuk dilakukan karena suatu jaringan yang dibangun dengan perencanaan yang baik akan menghasilkan suatu jaringan yang handal, termasuk aspek keamanannya.

Jenis jaringan yang dapat digunakan oleh suatu perusahaan dapat berupa jaringan LAN yang hanya melingkupi daerah dalam perusahaan, sampai dengan jaringan WAN yang dapat melingkupi daerah yang lebih jauh dari kantor pusat perusahaan itu sendiri, misalkan kantor-kantor cabang. Dengan ketersediaan jaringan perusahaan yang handal bahkan bisa mencakup daerah yang luas, maka pemanfaatan kerja jarak jauh (teleworking) dengan menggunakan jaringan VPN perusahaan dapat dimaksimalkan untuk memberikan hasil yang lebih baik.

5.1.4 Tugas

Buatlah kelompok terdiri atas 2-3 orang. Masing-masing kelompok membuat ringkasan tentang jaringan di enterprise, kemudian secara bergantian masing-masing kelompok mempresentasikan hasilnya didepan kelas.

1. Bacalah uraian materi diatas dengan teliti dan cermat.
2. Buatlah ringkasan materi menggunakan aplikasi pengolah presentasi.
3. Presentasikan hasil ringkasan di depan kelas.

5.1.5 Penilaian Diri

Setelah mengikuti kegiatan belajar 5 ini siswa diharapkan memiliki wawasan pengetahuan dan dapat menjawab pelbagai hal terkait dengan trafik yang mengalir pada jaringan perusahaan, LAN dan WAN perusahaan, intranet dan ekstranet, aplikasi-aplikasi perusahaan dan pola trafik yang mengalir, aplikasi-aplikasi dan trafik pada jaringan perusahaan, prioritas trafik jaringan, asas teleworking dan VPN.

BAB VI

6.1 Kegiatan Belajar 6 : Eksplorasi Infrastruktur Jaringan Perusahaan

6.1.1 Tujuan Pembelajaran

Setelah mengikuti kegiatan belajar 6 ini siswa diharapkan dapat memahami tentang eksplorasi infrastruktur jaringan perusahaan.

6.1.2 Aktifitas Belajar Siswa

6.1.2.1 Mengamati

Melalui kegiatan belajar 6 ini siswa diharapkan dapat melakukan pengamatan mengenai :

- Pusat operasi jaringan
- Pertimbangan desain ruang telekomunikasi
- Pemberian pelayanan pada PoP (Point of Presence)
- Pertimbangan keamanan pada kerja perusahaan
- Koneksi jaringan perusahaan ke layanan eksternal
- Routing dan switching
- Perangkat keras router dan switch
- Perintah dasar dan konfigurasi CLI router

6.1.2.2 Menanya

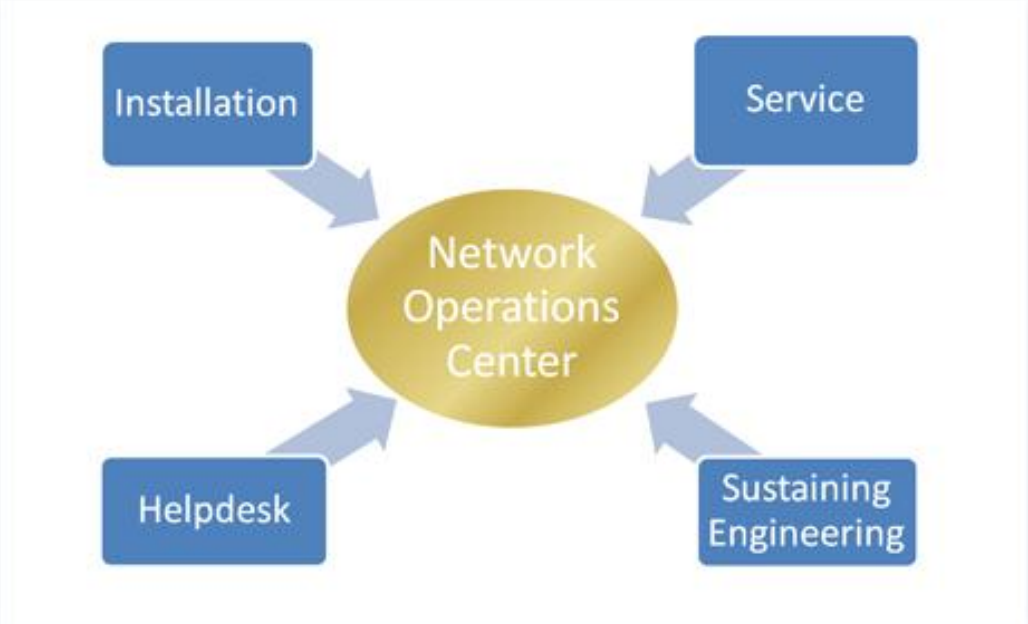
Melalui kegiatan belajar 6 ini siswa diharapkan dapat :

- Mendiskusikan pusat operasi jaringan
- Mendiskusikan pertimbangan desain ruang telekomunikasi
- Mendiskusikan pemberian pelayanan pada PoP (Point of Presence)
- Mendiskusikan pertimbangan keamanan pada kerja perusahaan
- Mendiskusikan koneksi jaringan perusahaan ke layanan eksternal
- Mendiskusikan routing dan switching
- Mendiskusikan perangkat keras router dan switch
- Mendiskusikan perintah dasar dan konfigurasi CLI router

6.1.2.3 Mengumpulkan Informasi

Pusat Operasi Jaringan

Network Operation Center (NOC) Adalah tempat administrator yang mengawasi, memantau dan mengamankan jaringan komunikasi. Berupa sebuah ruangan yang berisi visualisasi dari jaringan atau jaringan yang sedang dipantau, workstation di mana status rinci jaringan dapat dilihat, dan perangkat lunak yang diperlukan untuk mengelola jaringan.



Gambar 6.1 Diagram Layanan Pusat Operasi Jaringan

NOC merupakan perangkat infrastruktur yang melakukan fungsi-fungsi pengaturan, pengendalian, dan pengawasan jaringan (network) sedemikian rupa sehingga dapat berfungsi sesuai dengan standar pelayanan yang diberikan. Tugas NOC adalah menangani konfigurasi dan perubahan manajemen jaringan, network security, performance dan policy monitoring, pelaporan, jaminan kualitas, scheduling dan dokumentasi dengan memanfaatkan kemampuan management network, monitoring dan analysis tools.

Gambar 6.2 Contoh Ilustrasi Pusat Operasi Jaringan

NOC memberikan kemudahan kepada user dalam melakukan aktivitas koordinasi operasi dengan semua pendukung dan vendor terkait dengan fungsi network. Kegiatan pada NOC adalah memberikan support selama 24 jam dengan aktivitas sebagai berikut :

- Memonitor operais semua hubungan backbone dan pendukung jaringan lainnya.
- Menjamin bahwa server dan pelayanan bekerja secara terus menerus selama 24 jam.
- Memberi jaminan untuk mendukung kualitas layanan jaringan kepada pengguna.
- Perbaikan semua masalah jaringan dan sistem terkait.
- Membuka pelacakan dan resolusi dokumentasi permasalahan pada sistem jaringan.

Agar NOC dapat berfungsi seusai dengan standar layanan yang telah ditetapkan maka perlu suatu disain khusus yaitu : memperhatikan penempatan peralatan dan pengaturan suhu udara sehingga sesuai dengan kebutuhan; menempatkan peralatan pemadam kebakaran; pembatasan akses; pengunaan raised floor sebagai sirkulasi suhu udara dan jalur kabel.

Ruang ini dipergunakan oleh staff IT yang hanya mempunyai otoritas untuk mengontrol Server atau peralatan lainnya yang ada di dalam ruang server dan ruangan MDF/Telecomm. Setiap staff IT tersebut harus memiliki keahlian khusus dalam menangani setiap system dan hardware yang

ada.

Ruangan NOC adalah ruangan yang berisi peralatan-peralatan yang sangat vital bagi keberlangsungan sustem jaringan di lingkungan penyedia layanan internet sehingga perlu tingkat pengamanan yang ekstra ketat. Oleh karena itu dibuat akses masuk yang terbatas bagi staff IT tertentu yang memiliki wewenang.

Gambar 6.3 Contoh Pusat Operasi Jaringan

Pemberian Pelayanan Di PoP (Point of Presence)

Di Internet, POP (Point of Presence) adalah lokasi/tempat titik akses dari keseluruhan internet. (POP juga disebut Post Office Protocol atau POP). Sebuah POP mempunyai alamat IP yang unik. Internet Provider yang anda gunakan, seperti AOL, mempunyai lebih dari satu POP. Jumlah POP dalam ISP atau OSP merupakan sebuah ukuran tingkat pertumbuhan. POP sebenarnya bisa berada dalam ruang sewaan yang dimiliki oleh operator telekomunikasi dengan ISP yang saling terhubung. POP biasanya termasuk router, agregator panggilan digital / analog, server, dan relay frame atau switch ATM.

Internet Service Provider (ISP) yang menyediakan layanan internet kepada pelanggan menggunakan berbagai macam sarana dalam menjalankan layanannya. Salah satu caranya adalah dengan Wireless LAN, dimana ISP mmeberikan layanan kepada pelanggan melalui jaringan wireless atau tanpa kabel, biasanya menggunakan teknologi WiFi. Dengan cara ini, ISP dapat memberikan layanan internet dengan kecepatan cukup tinggi tanpa terbatas kabel. Namun teknologi ini memiliki keterbatasan, salah satunya dalam hal jarak jangkauan. Semakin jauh letak pelanggan dengan

access point titik akses ISP, pelanggan tersebut akan semakin terpengaruh oleh masalah ini. Sampai pada jarak tertentu dari ISP, calon pelanggan tidak dapat dilayani oleh ISP tersebut. Dengan adanya POP, jangkauan suatu ISP akan bertambah, sehingga dapat melayani lebih banyak klien. selain itu, POP juga meningkatkan ketersediaan jaringan secara keseluruhan, artinya: jika salah satu titik akses mati, masih ada titik akses lainnya yang dapat menggantikan, paling tidak tidak keduanya mati.

Pertimbangan Keamanan Pada Kerja Perusahaan

Pada Jaringan nirkabel keamanan menjadi sesuatu yang melekat erat pada pengaturan atau setting jaringan tersebut, hal ini salah satunya dikarenakan metode yang digunakan untuk dapat berkomunikasi satu peralatan dengan peralatan yang lainnya menggunakan metode broadcast. Sehingga menjadi suatu hal yang sangat penting buat Anda yang menggunakan model jaringan nirkabel ini terutama dengan teknologi WiFi untuk mengetahui beberapa model pengamanan yang biasanya disediakan oleh perangkat Access Point (AP) untuk mengamankan jaringan WiFi Anda.

Keamanan jaringan mencakup berbagai jaringan komputer, baik negeri maupun swasta, yang digunakan dalam pekerjaan sehari-hari melakukan transaksi dan komunikasi di kalangan bisnis, instansi pemerintah dan individu. Jika diamati mengenai keamanan maka keamanan jaringan komputer dapat ditinjau dari segi bentuknya yaitu seperti berikut:

- Keamanan hardware

Keamanan *Hardware* berkaitan dengan perangkat keras yang digunakan dalam jaringan komputer. Keamanan hardware sering dilupakan padahal merupakan hal utama untuk menjaga jaringan dari agar tetap stabil. Dalam keamanan hardware, server dan tempat penyimpanan data harus menjadi perhatian utama. Akses secara fisik terhadap server dan data-data penting harus dibatasi semaksimal mungkin.

Akan lebih mudah bagi pencuri data untuk mengambil harddisk atau tape backup dari server dan tempat penyimpanannya daripada harus menyadap data secara software dari jaringan. Sampah juga harus diperhatikan karena banyak sekali hacker yang mendatangi tempat sampah perusahaan untuk mencari informasi mengenai jaringan komputernya. Salah satu cara mengamankan hardware adalah menempatkan di ruangan yang memiliki keamanan yang baik. Lubang saluran udara perlu diberi perhatian karena dapat saja orang masuk ke ruangan server melaui saluran tersebut. Kabel-kabel jaringan harus dilindungi agar tidak mudah bagi hacker memotong kabel lalu menyambungkan ke komputernya.

Akses terhadap komputer juga dapat dibatasi dengan mengeset keamanan di level BIOS yang dapat mencegah akses terhadap komputer, memformat harddisk, dan mengubah isi Main Boot Record (tempat informasi partisi) harddisk. Penggunaan hardware autentifikasi seperti smart card dan

finger print detector juga layak dipertimbangkan untuk meningkatkan keamanan.

- Keamanan software.

Sesuai dengan namanya, maka yang harus diamankan adalah perangkat lunak. Perangkat lunak yang kita maksud disini bisa berupa sistem operasi, sistem aplikasi, data dan informasi yang tersimpan dalam komputer jaringan terutama pada server. Contohnya, jika server hanya bertugas menjadi router, tidak perlu software *web server* dan FTP server diinstal. Membatasi software yang dipasang akan mengurangi konflik antar software dan membatasi akses, contohnya jika router dipasangi juga dengan FTP server, maka orang dari luar dengan login anonymous mungkin akan dapat mengakses router tersebut.

Software yang akan diinstal sebaiknya juga memiliki pengaturan keamanan yang baik. Kemampuan enkripsi (mengacak data) adalah spesifikasi yang harus dimilki oleh software yang akan digunakan, khususnya enkripsi 128 bit karena enkripsi dengan sistem 56 bit sudah dapat dipecahkan dengan mudah saat ini. Beberapa software yang memiliki lubang keamanan adalah mail server sendmail dan aplikasi telnet. Sendmail memiliki kekurangan yaitu dapat ditelnet tanpa login di port (25) dan pengakses dapat membuat email dengan alamat palsu. Aplikasi telnet memiliki kekurangan mengirimkan data tanpa mengenkripsinya (mengacak data) sehingga bila dapat disadap akan sangat mudah untuk mendapatkan data.

Hal kedua yang perlu diperhatikan adalah *password.* Sebaiknya diset panjang password minimum unutk mempersulit hacker memcahkan password. Password juga akan semakin baik jika tidak terdiri huruf atau angak saja, huruf kecil atau kapital semua, namun sebaiknya dikombinasi. Enkripsi dapat menambah keamanan jaringan dengan cara mengacak password dan username, baik dalam record di host maupun pada saat password dan username itu dilewatkan jaringan saat melakukan login ke komputer lain.

Routing tidak terlepas pula dari gangguan keamanan. Gangguan yang sering muncul adalah pemberian informasi palsu mengenai jalur routing (source routing pada header IP). Pemberian informasi palsu ini biasanya dimaksudkan agar datagram-datagram dapat disadap. Untuk mencegah hal seperti itu, router harus diset agar tidak mengijinkan source routing dan dalam protokol routing disertakan autentifikasi atau semacam password agar informasi routing hanya didapat dari router yang terpercaya.

Routing Dan Switching

Routing adalah proses untuk memilih jalur (path) yang harus dilalui oleh paket. Jalur yang baik tergantung pada beban jaringan, panjang datagram, type of service requested dan pola trafik. Pada umumnya skema routing hanya mempertimbangkan jalur terpendek (the shortest path).

Terdapat 2 bentuk routing, yaitu:

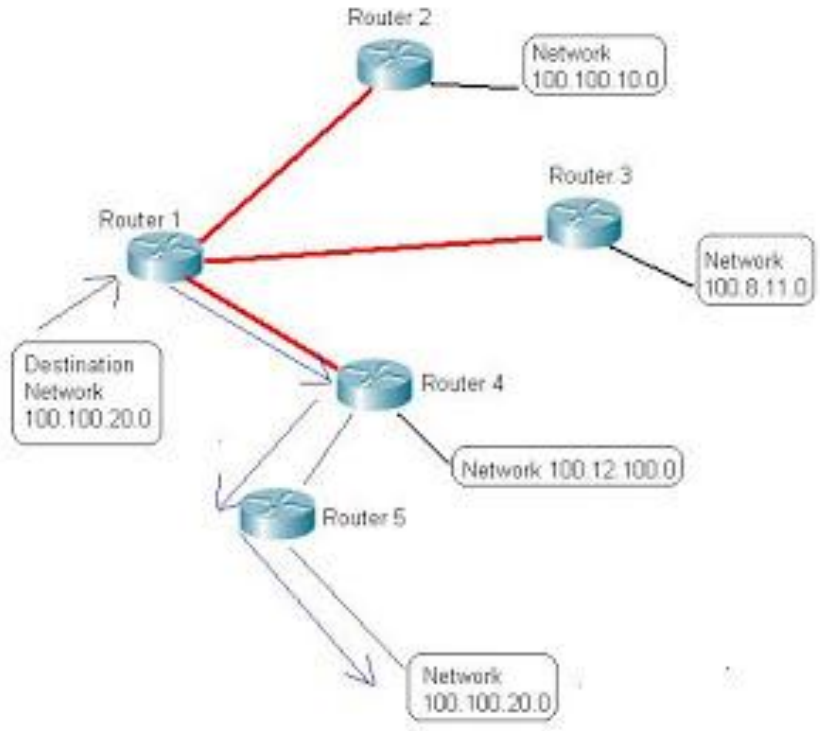
- Direct Routing *(direct delivery)*; paket dikirimkan dari satu mesin ke mesin lain

secara langsung (host berada pada jaringan fisik yang sama) sehingga tidak perlu melalui mesin lain atau gateway.

- Indirect Routing *(indirect delivery)*; paket dikirimkan dari suatu mesin ke mesin yang lain yang tidak terhubung langsung (berbeda jaringan) sehingga paket akan melewati satu atau lebih gateway atau network yang lain sebelum sampai ke mesin yang dituju.

Untuk dapat me"routing" segala sesuatu, Router, atau segala sesuatu yang dapat melakukan fungsi routing, membutuhkan informasi sebagai berikut :

– Alamat Tujuan/Destination Address, yaitu tujuan atau alamat item yang akan dirouting
– Mengenal sumber informasi, yaitu dari mana sumber (router lain) yang dapat dipelajari oleh router dan memberikan jalur sampai ke tujuan.
– Menemukan rute, yaitu rute atau jalur mana yang mungkin diambil sampai ke tujuan.
– Pemilihan rute, yaitu rute yang terbaik yang diambil untuk sampai ke tujuan.
– Menjaga informasi routing, yaitu suatu cara untuk menjaga jalur sampai ke tujuan yang sudah diketahui dan paling sering terjadi.



Gambar 6.4 Contoh Skema Routing

- Switching

Switching merupakan proses *bridging transparan* yang terjadi di lapisan data link dimana dua atau lebih segmentasi jaringan dihubungkan dengan cara forwarding . Device Network yang melakukan proses switching adalah Switch dan Bridge. Switch dan Bridge bekerja based on destination

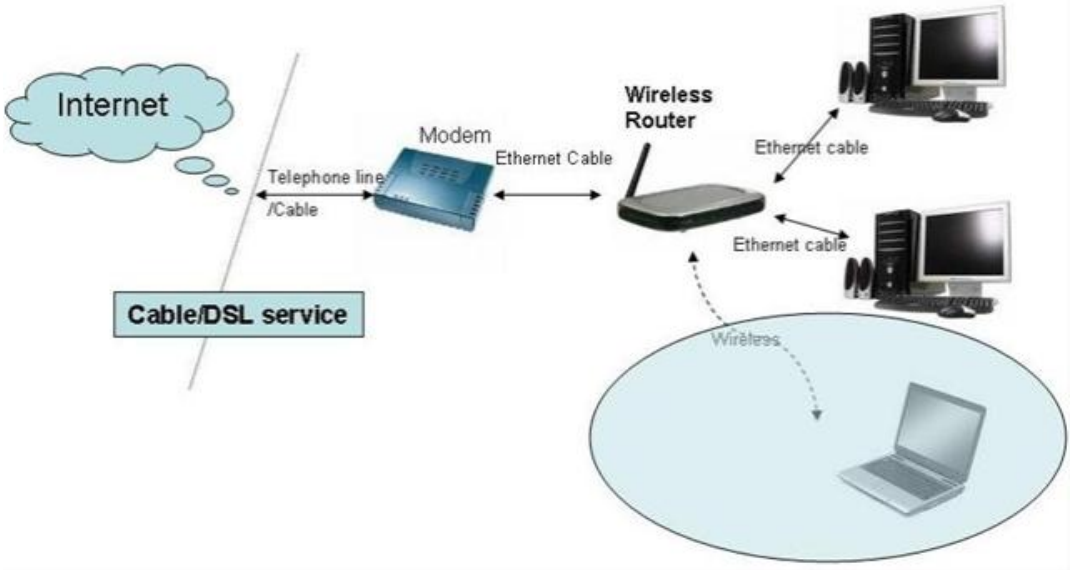
MAC Address, memiliki CAM (Content Addressable Memory) untuk menyimpan MAC dan portnya. Switch adalah multiport Bridge yang mempunyai fungsi dan cara kerja yang sama atau lebih. Device Network yang melakukan proses switching adalah Switch dan Bridge. Switch dan Bridge bekerja based on destination MAC Address, memiliki CAM (Content Addressable Memory) untuk menyimpan MAC dan portnya. Switch adalah multiport Bridge yang mempunyai fungsi dan cara kerja yang sama atau lebih.

Perangkat Keras Router Dan Switch

- *Router*

Router merupakan salah satu perangkat dalam dunia jaringan komputer. Pengertian Router adalah perangkat jaringan yang berfungsi untuk menghubungkan beberapa jaringan atau network, baik jaringan yang menggunakan teknologi sama atau yang berbeda, misalnya menghubungkan jaringan topologi Bus, topologi Star atau topologi Ring. Karena router ini menghubungkan beberapa jaringan tentunya router berbeda dengan Switch. Switch hanya perangkat yang digunakan untuk menghubungkan beberapa komputer sehingga membentuk LAN atau local area network. Sedangkan router adalah perangkat yang menghubungkan satu LAN dengan banyak LAN lainnya.

Router dapat digunakan untuk menghubungkan banyak jaringan kecil ke sebuah jaringan yang lebih besar, yang disebut dengan internetwork, atau untuk membagi sebuah jaringan besar ke dalam beberapa subnetwork untuk meningkatkan kinerja dan juga mempermudah manajemennya. Router juga kadang digunakan untuk mengoneksikan dua buah jaringan yang menggunakan media yang berbeda atau berbeda arsitektur jaringan, seperti halnya dari Ethernet ke Token Ring. Router umumnya dipakai untuk jaringan berbasis teknologi protokol TCP/IP, router jenis ini dinamakan IP Router. Internet merupakan contoh utama dari jaringan yang memiliki IP Router.



Gambar 6.5 Diagram Penempatan Wireless Router Dalam Jaringan

Umumnya router ada dua jenis, yaitu router statis dan router dinamis. Router statis atau static router merupakan router yang memiliki tabel routing statis yang disetting dengan cara manual oleh para administrator jaringan. Sedangkan router dinamis atau rynamic router merupakan router yang memiliki dan membuat tabel routing dinamis dengan membaca lalu lintas jaringan dan juga dengan saling berhubungan dengan router lainnya.

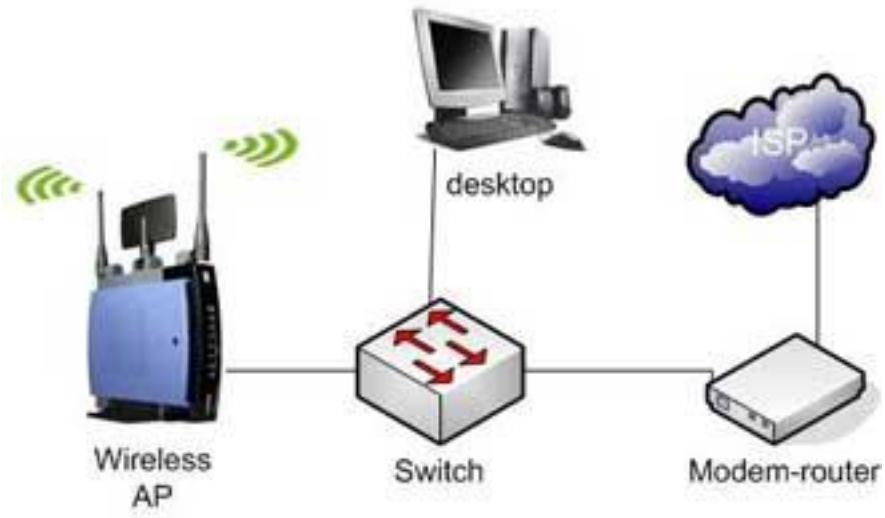
Gambar 6.6 Contoh Router Dari Mikrotik

Gambar 6.7 Contoh Router Dari Cisco

- *Switch*

Switch ialah sebuah perangkat keras yang memungkinkan terjadinya distribusi packet data antar komputer dalam jaringan dan mampu untuk mengenali topologi jaringan di banyak layer sehingga packet data dapat langsung sampai ke tujuan. Switch dan Hub sebenarnya memiliki fungsi yang sama, karena dengan menggunakan salah satu diantaranya kita tetap bisa membuat Jaringan Komputer, tapi penggunaan Switch akan lebih cepat daripada Hub apalagi bila jaringan yang kita punya sangat besar. Ketika data masuk atau datang ke Hub, Hub akan mengambil data tersebut dan akan mentransmisikannya ke setiap komputer yang terhubung ke Jaringan.

Tetapi lain halnya dengan Switch, ia akan menerima data tersebut dan hanya akan mengirimkannya ke komputer yang berkepentingan menerima data tersebut. Penggunaan Switch akan memotong penggunaan bandwith jaringan anda secara signifikan, terutama bila kita memiliki jaringan dengan banyak komputer dan semuanya sibuk untuk mengirim dan menerima data disaat bersamaan. Keunggulan switch yang lain ialah data akan lebih aman dari aksi pencurian data dengan cara sniffer.



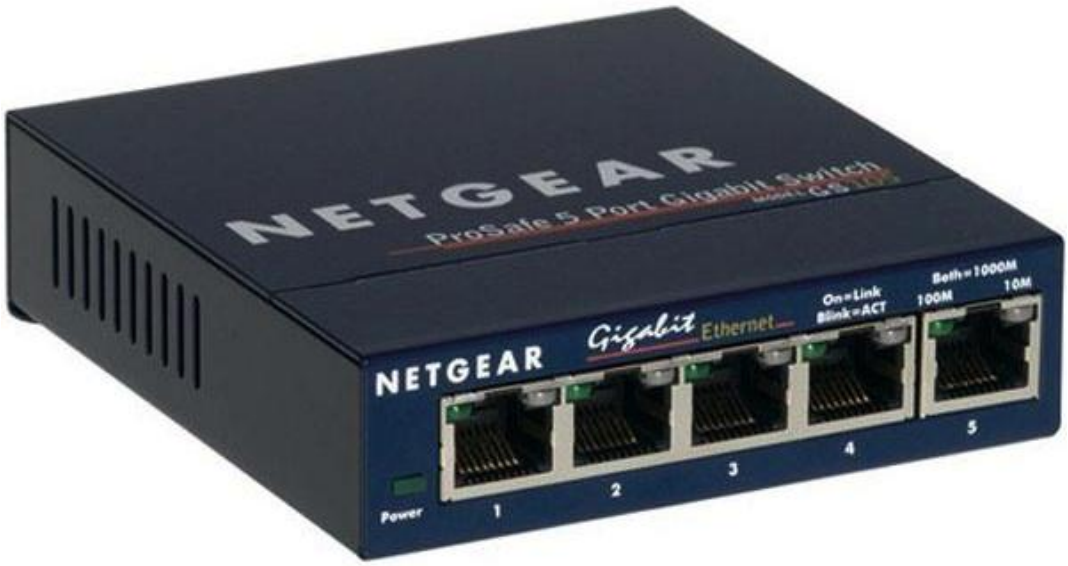
Gambar 6.8 Diagram Penempatan Switch Dalam Suatu Jaringan

Saat membeli switch kita akan diberi beberapa pilihan tipe, ada tipe yang managed, unmanaged, dan smart managed. Selain itu ada juga beberapa switch yang memiliki fitur khusus. Bila kita memiliki jaringan dengan komputer yang relatif sedikit seperti rumah atau kantor kecil, kita dapat menggunakan Switch dengan fitur Unmanaged. Tipe ini cukup praktis karena kita tidak perlu melakukan konfigurasi untuk penggunaannya dan harganya lebih murah. Cukup hubungkan / colok kabel LAN

ke switch, maka komputer akan langsung terhubung ke jaringan.

Lain halnya bila kita memiliki jaringan yang cukup besar, kita bisa menggunakan Switch dengan fitur managed. Managed Switch memiliki pilihan setting Admin dimana kita bisa membuat Virtual Lan (VLAN), menyetting kecepatan port, host dan pilihan lainnya. Biasanya penggunaannya akan membutuhkan Web Browser atau command line dengan interface seperti telnet atau Shell untuk pengaksesan pengaturan Switch. Sedangkan untuk Switch dengan fitur smart managed, adalah percampuran fitur antara managed dan unmanaged. Fungsinya hampir sama seperti managed tetapi menawarkan penggunaan yang lebih mudah, meskipun fitur ini tidak memiliki fitur sebanyak managed Switch.

Gambar 6.9 Contoh Switch Dari D-Link



Gambar 6.10 Contoh Switch Dari Netgear

Perintah Dasar Dan Konfigurasi CLI Router

Salah satu cara konfigurasi pada router cisco adalah menggunakan CLI *(Command Line Interface).* Perintah-peritah harus diketikan pada terminal. Software yang menangani input/output dan pemerosesan perintah-perintah adalah *Cisco IOS (Internetwork Operating System).*

Cisco IOS adalah sistem operasi berbasis teks yang digunakan pada perangkat switch dan router buatan Cisco. Perintah-perintah Cisco IOS dikelompokan menjadi beberapa mode yang disebut Exec mode. Secara umum ada dua mode utama, User Exec mode dan Privileged Exec mode. Pada Privileged Exec mode ini kita bisa masuk pada Global Configuration yang biasa digunakan untuk mengkonfigurasi IP pada tiap interface, Routing, Vlan dsb.

Selajutnya untuk melakukan konfigurasi Cisco Catalyst, yang harus kita persiapkan adalah sebuah (PC) komputer, atau laptop dengan port COM (atau converter serial to USB untuk komputer yg tidak memiliki port com serial), kabel Console, dan sebuah program Hyper Terminal. Langkah selanjutnya adalah menghubungkan kabel Console ke port COM komputer dan port Console Cisco Catalyst. Tentunya komputer dan Catalyst harus udah terhubung ke power supply. Selanjutnya buka hyper terminal. Pilih nama port yang digunakan ke Catalyst. Bikin speed rate nya jadi 9600.

Berikut ini daftar perintah dasar yang sering digunakan dalam mode CLI (*Command Line*), yaitu :

- **Setting Password** router>enable router#configure terminal router(config)#enable password forumsains (set password untuk masuk ke mode privilege) router(config)#enable secret secret (set enkripsi untuk password yang disimpan)
- **Setting Host Name** router>enable router#configure terminal router(config)#hostname nama-host
- **Setting VLAN** router>enable router#configure terminal router(config)#vlan nomor-vlan router(config-vlan)#name nama-vlan
- **Setting IP Address pada VLAN** router>enable router#configure terminal router(config)#interface vlan 1 router(config-if)#ip address address mask (misal: ip address 172.10.46.1 255.255.255.0) router(config-if)#no shutdown
- **Setting Identitas pada Port Cisco Catalyst** router>enable router#configure terminal router(config)#interface nama-port router(config-if)**#**description “Port Setting Identitas” router(config-if)#end
- **Setting IP Gateway** router>enable router#configure terminal router(config)#ip default-gateway address
- **Setting Port-Speed dan Link-**

Mode router#configure terminal router(config)#interface nama-port (misal : interface fast ethernet 0/1) router(config-if)#speed 100 router(config-if)#duplex full router#configure terminal router(config)#interface nama-port router(config-if)#switchport mode access router(config-if)#switchport access vlan nama-vlan router#configure terminal router(config)#interface nama-port router(config-if)#switchport mode trunk router(config-if)#switchport trunk allowed vlan nama-vlan

- **Setting Line VTY** router#configure terminal router(config)#line vty 0 4 router(config-line)#login router(config-line)#password password
- **Setting Line Con 0** router#configure terminal router(config)#line con 0 router(config-line)#login router(config-line)#password password
- **Melihat Semua Konfigurasi** router#show running-config
- ***Menghapus Semua Konfigurasi*** router#erase startup-config router#dir router#delete flash:vlan.dat router#dir router#reload

6.1.2.4 Mengasosiasi

Setelah mengikuti kegiatan belajar 6 ini siswa diharapkan dapat menyimpulkan pelbagai hasil percobaan dan pengamatan terkait dengan pusat operasi jaringan, pertimbangan desain ruang telekomunikasi, pemberian pelayanan pada PoP (Point of Presence), pertimbangan keamanan pada kerja perusahaan, koneksi jaringan perusahaan ke layanan eksternal, routing dan switching, perangkat keras router dan switch, dan perintah dasar dan konfigurasi CLI router.

6.1.3 Rangkuman

Jaringan komputer suatu perusahaan memiliki banyak potensi untuk dimanfaatkan demi kepentingan dan keberlangsungan bisnis perusahaan tersebut. Tugas-tugas tersebut biasanya dilaksanakan oleh administrator jaringan dari pusat operasi jaringan (NOC). Dari pusat operasi ini mereka dapat mengatur, melakukan instalasi, melakukan audit, memonitor bahkan memperbaiki perangkat-perangkat yang tersambung ke dalam jaringan perusahaan.

6.1.4 Tugas

Buatlah kelompok terdiri atas 2-3 orang. Masing-masing kelompok membuat ringkasan tentang eksplorasi infrastruktur jaringan perusahaan, kemudian secara bergantian masing-masing kelompok mempresentasikan hasilnya didepan kelas.

1. Bacalah uraian materi diatas dengan teliti dan cermat.
2. Buatlah ringkasan materi

menggunakan aplikasi pengolah presentasi.

3. Presentasikan hasil ringkasan di depan kelas.

6.1.5 Penilaian Diri

Setelah mengikuti kegiatan belajar 6 ini siswa diharapkan memiliki wawasan pengetahuan dan dapat menjawab pelbagai hal terkait dengan pusat operasi jaringan, pertimbangan desain ruang telekomunikasi, pemberian pelayanan pada PoP (Point of Presence), pertimbangan keamanan pada kerja perusahaan, koneksi jaringan perusahaan ke layanan eksternal, routing dan switching, perangkat keras router dan switch, dan perintah dasar dan konfigurasi CLI router.

BAB VII

7.1 Kegiatan Belajar 7 : Switching Pada Jaringan Perusahaan

7.1.1 Tujuan Pembelajaran

Setelah mengikuti kegiatan belajar 7 ini siswa diharapkan dapat memahami tentang switching pada jaringan perusahaan.

7.1.2 Aktifitas Belajar Siswa

7.1.2.1 Mengamati

Melalui kegiatan belajar 7 ini siswa diharapkan dapat melakukan pengamatan mengenai :

- Prinsip kerja switching dan segmentasi jaringan
- Prinsip kerja switching multilayer
- Identifikasi macam-macam switching
- Keamanan switch
- Perlindungan jaringan terhadap switching loop
- Redundansi pada sebuah jaringan dengan switch
- Protokol Spanning Tree (STP)
- Prinsip root bridges
- Identifikasi spanning tree pada jaringan hirarkikal
- Protokol Spanning Tree Cepat (RSTP)
- Identifikasi dan konfigurasi VLAN
- Rute inter VLAN dan trunking
- Yang dimaksud dengan port trunk
- Memperluas VLAN melalui switch
- Routing antara VLAN-VLAN
- Perawatan VLAN dalam suatu jaringan perusahaan
- Program trunking VLAN (VTP)
- Konfigurasi VTP
- Konfigurasi VLAN untuk IP telephony dan nirkabel

7.1.2.2 Menanya

Melalui kegiatan belajar 7 ini siswa diharapkan dapat :

- Mendiskusikan prinsip kerja switching dan segmentasi jaringan
- Mendiskusikan prinsip kerja switching multilayer
- Mendiskusikan identifikasi macam-macam switching
- Mendiskusikan keamanan switch
- Mendiskusikan perlindungan jaringan terhadap switching loop
- Mendiskusikan redundansi pada sebuah jaringan dengan switch
- Mendiskusikan Protokol Spanning Tree (STP)
- Mendiskusikan prinsip root bridges
- Mendiskusikan identifikasi spanning tree pada jaringan hirarkikal
- Mendiskusikan Protokol Spanning Tree Cepat (RSTP)
- Mendiskusikan identifikasi dan konfigurasi VLAN
- Mendiskusikan rute inter VLAN dan trunking
- Mendiskusikan yang dimaksud dengan port trunk
- Mendiskusikan memperluas VLAN melalui switch
- Mendiskusikan routing antara VLAN-VLAN
- Mendiskusikan perawatan VLAN dalam suatu jaringan perusahaan
- Mendiskusikan program trunking VLAN (VTP)

- Mendiskusikan konfigurasi VTP
- Mendiskusikan konfigurasi VLAN untuk IP telephony dan nirkabel

7.1.2.3 Mengumpulkan Informasi

Prinsip Kerja Switching Dan Segmentasi Jaringan

Komunikasi voice ataupun data tidak terlepas dari teknik switching. Berikut adalah uraian beberapa teknik switching yang diterapkan. Secara umum arti switching dalam teknik jaringan komunikasi adalah melakukan proses hubungan antara dua pelanggan telepon sehingga keduanya dapat berbicara satu sama lain. Jaringan telepon terdiri dari banyak titik penyambungan sehingga tiap telepon dalam jaringan dapat saling dihubungkan melalui junction atau trunk. Hubungan antara operator disebut Junction. Penyambungan merupakan masalah kompleks dalam pendefinisian fungsi, features, kemajuan teknologi dan operasinya.

Teknik Switching dibagi menjadi 2, yaitu :

- Circuit Switching

Jaringan circuit switching digunakan untuk menghubungkan pasangan terminal dengan cara menyediakan sirkuit atau kanal yang tersendiri dan terus menerus selama hubungan berlangsung. Jaringan circuit switching, kinerjanya tergantung pada loss bukan pada delay (tetapi pada digital switching juga menimbulkan delay). Tiga fase yang terdapat dalam circuit switching, yaitu;

  – Pembentukan hubungan
  – Transfer data
  – Pembubaran (terminasi) hubungan

Jaringan circuit switching digunakan untuk hubungan yang bersifat :

  – Real time-spech (contoh : telepon)
  – Real time-data very high bit transmitted

Contoh :

  – Jaringan Telepon
  – ISDN (Integrated Services Digital Networks)

Dalam sistem ini pengirim yaitu rangkaian masukan disambungkan ke penerima atau rangkaian keluaran selama pengalihan informasi. Untuk tiap hubungan diperlukan satu rangkaian. Bilamana pihak yang dituju sibuk ataupun tidak berada dalam keadaan siap menerima informasi hubungan tidak dapat dilaksanakan atau gagal. Informasi yang hendak dikirmkan dapat hilang. Jaringan telepon menggunakan cara ini. Untuk transmisi data, komunikasi biasanya dilakukan dengan cara melalui transmisi data dari sumber ke tujuan melalui simpul-simpul jaringan switching perantara. Simpul switching bertujuan menyediakan fasilitas switching yang akan memindah data dari simpul ke simpul sampai mencapai tujuan.

Ujung perangkat yang ingin melakukan komunikasi disebut station. Station bisa berupa komputer, terminal, telepon, atau perangkat komunikasi lainnya. Sedangkan perangkat yang tujuannya menyediakan komunikasi disebut simpul. Simpul-simpul saling dihubungkan melalui jalur transmisi. Masing-masing station terhubung ke sebuah simpul, dan kumpulan

simpul-simpul itulah yang disebut sebagai jaringan komunikasi.

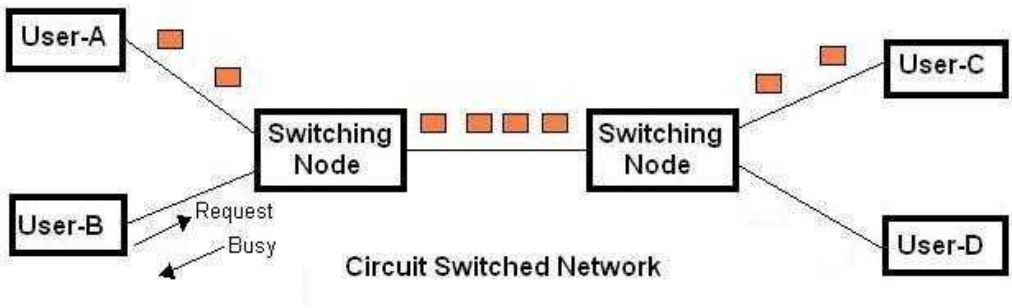
Simpul yang hanya terhubung dengan simpul lain, tugasnya hanya untuk switching data secara internal (ke jaringan). Sedangkan yang terhubung ke satu station atau lebih, fungsinya selain menerima data juga sekaligus mengirimkannya ke station yang terhubung. Jalur simpul-simpul biasanya dimultiplexingkan, baik dengan menggunakan Frequency Division Multiplexing (FDM) maupun Time Division Multiplexing (TDM). Tidak ada saluran langsung diantara sepasang simpul. Sehingga diharapkan selalu memiliki lebih dari 1 jalur disepanjang jaringan untuk tiap pasangan station untuk mempertahankan reliabilitas jaringan.

Keuntungan Teknik Switching

- Jaringan transparan (seolah hanya koneksi langsung antar stations)
- Fixed data rate tanpa adanya delay
- Sangat baik untuk komunikasi real time

Kelemahan Teknik Switching

- Selama koneksi berlangsung, time slot akan selalu diduduki walaupun tidak ada data yang dikirim
- Delay sebelum terbentuknya hubungan (call set up delay)



Gambar 7.1 Skema Circuit Switching

- Packet Switching

Sebuah metode yang digunakan untuk memindahkan data dalam jaringan internet. Dalam packet switching, seluruh paket data yang dikirim dari sebuah node akan dipecah menjadi beberapa bagian. Setiap bagian memiliki keterangan mengenai asal dan tujuan dari paket data tersebut. Hal ini memungkinkan sejumlah besar potongan-potongan data dari berbagai sumber dikirimkan secara bersamaan melalui saluran yang sama, untuk kemudian diurutkan dan diarahkan ke rute yang berbeda melalui router.

Packet Switching tidak mempergunakan kapasitas transmisi yang melewati jaringan. Data dikirim keluar dengan menggunakan rangkaian potongan-potongan kecil secara berurutan yang disebut *paket*. Masing-masing paket melewati jaringan dari satu titik ke titik lain dari sumber ke tujuan. Pada setiap titik seluruh paket diterima, disimpan dengan cepat dan ditransmisikan ke titik berikutnya. Fungsi utama dari jaringan packet-switched adalah menerima paket dari stasiun pengirim untuk diteruskan ke stasiun penerima.

Dalam Packet Switching, data yang ditransmisikan dibagi-bagi ke dalam paket-paket kecil. Jika source mempunyai message yang lebih panjang untuk dikirim, message itu akan dipecah ke dalam barisan-barisan paket. Tiap paket berisi data dari user dan info control. Info control berisi minimal adalah info agar bagaimana paket bisa melalui jaringan dan mencapai alamat tujuan. Umumnya header berisi :

— Source (sender's) address

— Destination (recipient's) address

— Packet size

— Sequence number

— Error checking information

Beberapa keuntungan yang diperoleh dari packet switching :

– Efisiensi line sangat tinggi; hubungan single node-to-node dapat dishare secara dinamis oleh banyak paket. Paket-paket diqueue dan ditransmisikan secepat mungkin. Secara kontras, dalam circuit switching, waktu pada link node-to-node adalah dialokasikan terlebih dahulu

menggunakan time-division multiplexing.

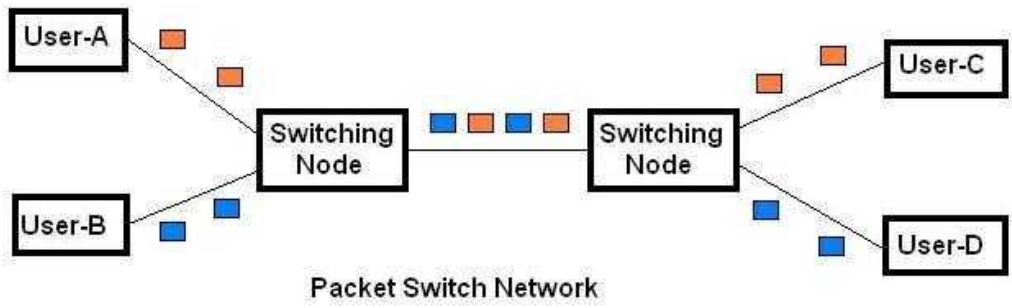
– Jaringan packet-switched dapat membuat konversi data-rate. Dua buah station yang berbeda data-ratenya dapat saling menukar paket.
– Ketika traffic mulai padat, beberapa call diblok, yang menunjukkan jaringan menolak permintaan koneksi tambahan sampai beban di jaringan menurun. Dalam packet switchied network, paket masih dapat diterima akan tetapi delay delivery bertambah.
– Prioritas dapat digunakan. Jadi kalau sebuah node mempunyai sejumlah queued packet untuk ditransmisikan, paket dapat ditransmisikan pertama kali berdasarkan prioritas yang lebih tinggi. Paket-paket ini mempunyai delay yang lebih kecil daripada lower-priority packets.

Packet Switching juga meiliki kelemahan, yaitu :

– Tidak memberikan garansi Quality of service: delay antrian, jitter, loss packet, dan throughput

Contoh Teknologi Layanan Packet Switched:

– Public data network
– Frame relay
– Internet (connectionless)
– LAN (connectionless)



Gambar 7.2 Skema Packet Switching

Ada dua pendekatan yang berhubungan dengan jaringan Packet Switching, yaitu:

- Datagram

Node-node jaringan memroses tiap paket secara independen. Jika host A megirim dua paket berurutan ke host B pada sebuah jaringan paket datagram, jaringan tidak dapat menjamin bahwa kedua paket tersebut akan dikirim bersamaan, kenyataannya kedua paket tersebut dikirimkan dalam rute yang berbeda Paket-paket tersebut disebut datagram,

Implikasi dari switching paket datagram :

- Urutan paket dapat diterima dalam susunan yang berbeda ketika dikirimkan

- Tiap paket header harus berisi alamat tujuan yang lengkap

Kelebihan Datagram Packet Switching:

- Tidak ada waktu call setup

- Adaptasi yang cepat jika terjadi congestion/network overload.

- Adaptasi yang cepat jika terjadi node failure

Kelemahan Datagram Packet Switching:

- Kedatangan paket bisa tidak sesuai dengan urutannya.

- Adanya beban pemrosesan karena setiap paket di proses di setiap node

- Receiver tidak memiliki persiapan terhadap paket yang dating

- Virtual Switching

Virtual circuit packet switching adalah campuran dari circuit switching dan paket switching. Seluruh data ditransmisikan sebagai paket-paket. Seluruh paket dari satu deretan paket dikirim setelah jalur ditetapkan terlebih dahulu (virtual circuit). Urutan paket yang dikirimkan dijamin diterima oleh penerima. Paket-paket dari virtual circuit yang berbeda masih dimungkinkan terjadi interleaving.

Pengirim data dengan virtual circuit melalui 3 fase :

- Penetapan VC
- Pentransferan data
- Pemutusan VC

Kelebihan Virtual Circuit Packet Switching :

- Kedatangan paket sesuai urutannya.

- Terdapat mekanisme error control.

- Penetapan satu rute untuk satu koneksi.

- Penerima telah bersiap untuk menerima paket yang dating

Kelemahan Virtual Circuit Packet Switching :

- Adanya delay saat connection setup.

- Adaptasi terhadap node failure kurang baik.

- Adaptasi terhadap network overload kurang baik

Perbedaan Datagram dan Virtual Circuit:

- Datagram *(Connectionless)*
  - Tiap paket memiliki alamat tujuan yang lengkap
  - Penentuan routing dilakukan terhadap setiap paket di setiap node
  - Paket-paket yang berbeda namun berasal dari pesan yang sama dapat menggunakan rute yang berbeda, tergantung kepadatan jalur.
  - Paket-paket akan mencari alternatif routing dimana akan mengabaikan node yang gagal
- Virtual Circuit (Connection Oriented)
  - Sebuah route antara station dikonfigurasi sebelum terjadi transfer data
  - Setiap paket memiliki VC identifier.
  - Penetapan routing dilakukan sekali untuk semua paket.
  - Semua paket akan melalui rute yang sama
  - Apabila ada node yang gagal, semua virtual circuit yang mendefinisikan lewat node tersebut akan lenyap

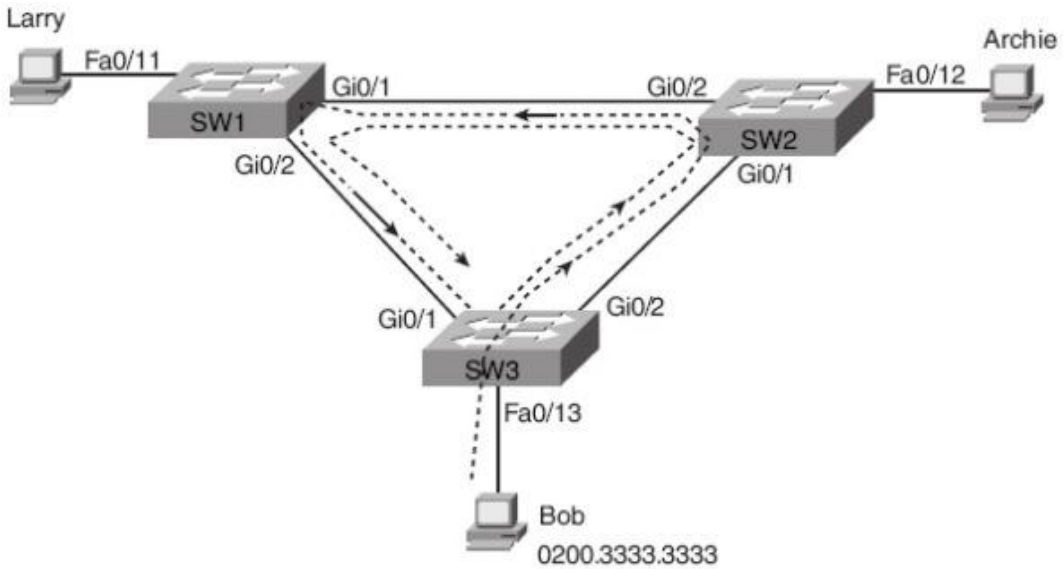
Protocol Spanning Tree (STP)

Protokol Pohon Rentangan (bahasa Inggris: Spanning Tree Protocol (disingkat STP)) adalah protokol jaringan yang

menjamin topologi jaringan bebas-perulangan untuk penghubung Ethernet LAN. Fungsi dasar dari STP adalah untuk mencegah pengulangan penghubung dan radiasi siaran yang dihasilkan dari mereka. Pohon rentang juga memungkinkan desain jaringan untuk memasukkan cadang tautan (redundan) untuk menyediakan jalur cadangan otomatis jika tautan aktif gagal, tanpa bahaya dari perulangan yang tidak diinginkan dalam jaringan, atau kebutuhan untuk panduan mengaktifkan / menonaktifkan cadangan tautan ini.

Spanning Tree Protocol (STP) distandarisasi sebagai IEEE 802.1D. Seperti namanya, protokol ini bisa menciptakan pohon rentang dalam jaringan bertautan dari lapisan 2 layer penghubung (biasanya switch ethernet), dan menonaktifkan tautan tersebut yang bukan bagian dari pohon rentang, meninggalkan jalur aktif tunggal antara dua node jaringan. STP ini berdasarkan algoritma yang ditemukan oleh Radia Perlman

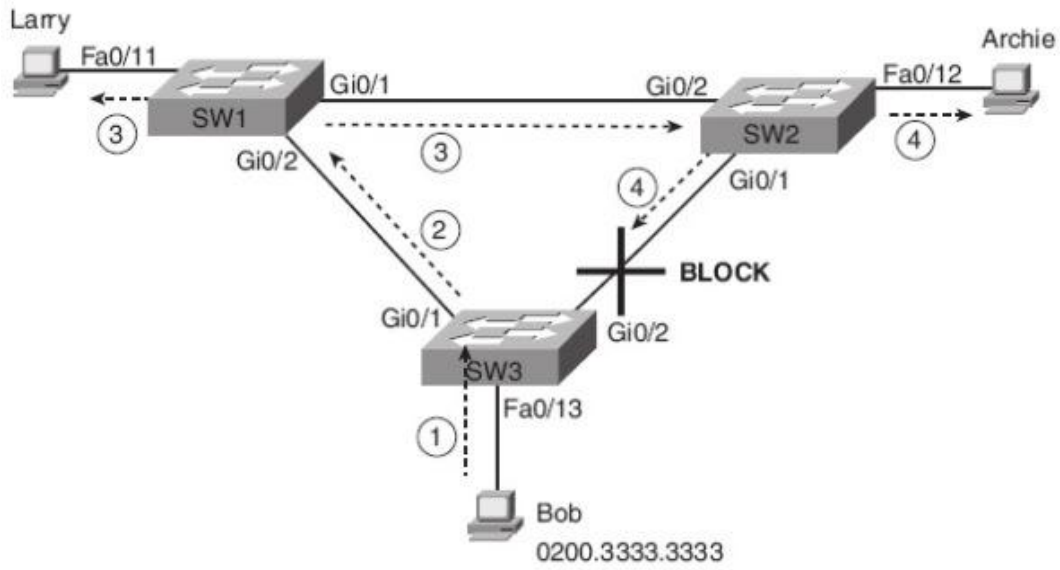
Tanpa adanya Spanning Tree Protocol (STP), LAN dengan link yang redundant mengakibatkan adanya frame yang looping tanpa henti didalam network. Dengan STP, beberapa switch akan mem-block interface/port-nya agar port tersebut tidak bisa lagi mem-forward frames keluar. STP akan menentukan port mana yang harus di block sehingga hanya 1 link saja yang aktif dalam satu segment LAN. Hasilnya, frame tetap bisa ditransfer antar-komputer tanpa menyebabkan gangguan akibat adanya frame yang looping tanpa henti di dalam network. Problem utama yang bisa dihindari dengan adanya STP adalah broadcast storms. Broadcast storms menyebabkan frame broadcasts (atau multicast atau unicast yang destination addressnya belum diketahui oleh switch) terus berputar-putar (looping) dalam network tanpa henti.



Gambar 7.3 Contoh Jaringan LAN Yang Redundant

Switch akan mem-flood frame broadcasts keluar melalui semua port/interface dalam satu VLAN kecuali port/interface dimana frame tersebut diterima. Pada gambar diatas, SW3 akan mem-forward frame dari Bob ke SW2; SW2 mem-forwardnya ke SW1; SW1 mem-forwardnya kembali ke SW3; SW3 ke SW2 lagi, dan seterusnya dan seterusnya.

Problem lain yang bisa dihindari dengan STP adalah dalam satu network yang memiliki link redundant, komputer-komputer yang aktif akan menerima kopi-an dari frame yang sama berkali-kali. STP mencegah terjadinya looping dengan menempatkan setiap port switch pada salah satu status : Forwarding atau Blocking. Interface dengan status forwarding bertingkah normal, mem-forward dan menerima frame, sedangkan interface dengan status blocking tidak memproses frame apapun kecuali pesan-pesan STP. Semua port yang berada dalam status forwarding disebut berada pada jalur spanning tree (topology STP), sekumpulan port-port forwarding membentuk jalur tunggal dimana frame ditransfer antar-segment.



Gambar 7.4 Contoh Jaringan LAN Yang Sudah Menggunakan STP

Dengan begini, saat Bob mengirimkan frame broadcast, frame tidak mengalami looping. Bob mengirimkan frame ke SW3 (step 1), kemudian SW3 mem-forward frame hanya ke SW1(step 2), karena port Gi0/2 dari SW3 berada pada status blocking. Kemudian, SW1 mem-flood frame keluar melalui Fa0/11 dan Gi0/1 (step 3) . SW2 mem-flood frame keluar melalui Fa0/12 dan Gi0/1 (step4). Namun, SW3 akan mengabaikan frame yang dikirmkan oleh SW2, karena frame tersebut masuk melalui port Gi0/2 dari switch SW3 yang berada pada status blocking.

Dengan topology STP seperti pada gambar diatas, switch-switch tidak mengaktifkan link antara SW2 dan SW3 untuk keperluan traffick dalam VLAN. Namun, jika link antara SW1 dan SW3 mengalami kegagalan dalam beroperasi, maka STP akan

membuat port Gi0/2 pada SW3 menjadi forwarding sehingga link antara SW3 dan SW2 menjadi aktif dan frame tetap bisa ditransfer secara normal dalam VLAN.

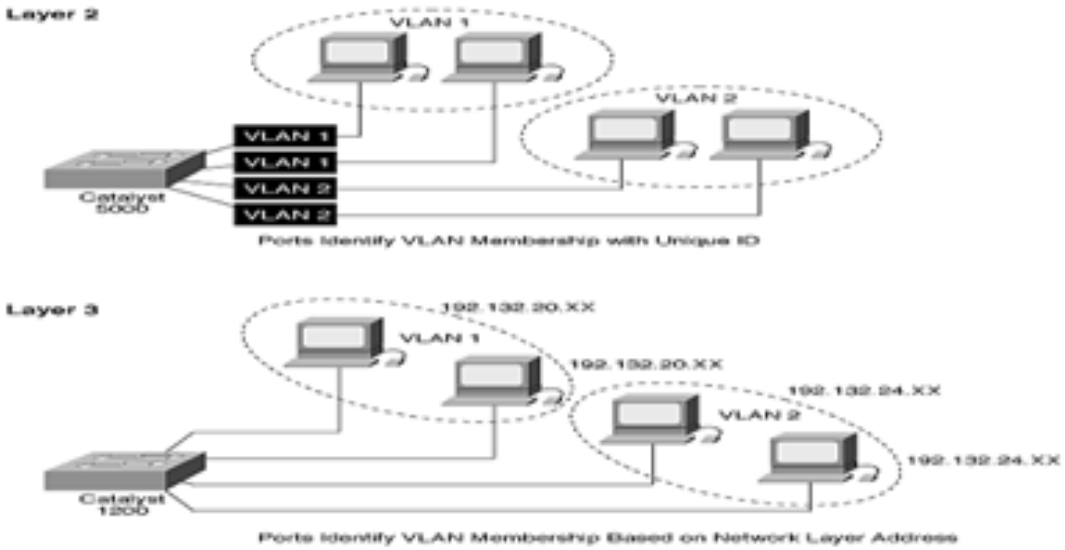
STP menggunakan 3 kriteria untuk meletakkan port pada status forwarding :

– STP memilih root switch. STP menempatkan semua port aktif pada root switch dalam status Forwarding.
– Semua switch non-root menentukan salah satu port-nya sebagai port yang memiliki ongkos (cost) paling kecil untuk mencapai root switch. Port tersebut yang kemudian disebut sebagai root port (RP) switch tersebut akan ditempatkan pada status forwarding oleh STP.
– Dalam satu segment Ethernet yang sama mungkin saja ter-attach lebih dari satu switch. Diantara switch-switch tersebut, switch dengan cost paling sedikit untuk mencapai root switch disebut designated bridge, port milik designated bridge yang terhubung dengan segment tadi dinamakan designated port (DP). Designated port juga berada dalam status forwarding. Semua port/interface selain port/interface diatas berada dalam status Blocking.

Switch-switch akan memilih root switch berdasarkan Bridge ID dalam BPDU. Root switch adalah switch dengan Bridge ID paling rendah. Kita ketahui bahwa 2-byte pertama dari switch digunakan untuk priority, karena itu switch dengan priority paling rendah akan terpilih menjadi root switch. Namun kadangkala, ada beberapa switch yang memiliki nilai priority yang sama, untuk hal ini maka pemilihan root switch akan ditentukan berdasarkan 6-byte System ID berikutnya yang berbasis pada MAC address, karena itu switch dengan bagian MAC address paling rendah akan terpilih sebagai root switch. Selanjutnya dalam proses STP adalah, setiap non-root switch akan menentukan salah satu port-nya sebagai satu-satunya root port miliknya. Root port dari sebuah switch adalah port dimana dengan melalui port tersebut switch bisa mencapai root switch dengan cost paling kecil.

Identifikasi Dan Konfigurasi VLAN

VLAN merupakan suatu model jaringan yang tidak terbatas pada lokasi fisik seperti LAN , hal ini mengakibatkan suatu network dapat dikonfigurasi secara virtual tanpa harus menuruti lokasi fisik peralatan. Penggunaan VLAN akan membuat pengaturan jaringan menjadi sangat fleksibel dimana dapat dibuat segmen yang bergantung pada organisasi atau departemen, tanpa bergantung pada lokasi workstation.



Gambar 7.5 Contoh Skema VLAN

VLAN diklasifikasikan berdasarkan metode (tipe) yang digunakan untuk mengklasifikasikannya, baik menggunakan port, MAC addresses dan sebagainya. Semua informasi yang mengandung penandaan/pengalamatan suatu VLAN (tagging) di simpan dalam suatu database (tabel), jika penandaannya berdasarkan port yang digunakan maka database harus mengindikasikan port-port yang digunakan oleh VLAN. Untuk mengaturnya maka biasanya digunakan switch/bridge yang manageable atau yang bisa di atur. Switch/bridge inilah yang bertanggung jawab menyimpan semua informasi dan konfigurasi suatu VLAN dan dipastikan semua switch/bridge memiliki informasi yang sama. Switch akan menentukan kemana data-data akan diteruskan dan sebagainya. atau dapat pula digunakan suatu software pengalamatan (bridging software) yang berfungsi mencatat/menandai suatu VLAN beserta workstation yang didalamnya.untuk menghubungkan antar VLAN dibutuhkan router.

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

- Berdasarkan Port

Keanggotaan pada suatu VLAN dapat di dasarkan pada port yang di gunakan oleh VLAN tersebut. Sebagai contoh, pada bridge/switch dengan 4 port, port 1, 2, dan 4 merupakan VLAN 1 sedang port 3 dimiliki oleh VLAN 2. Kelemahannya adalah user tidak bisa untuk berpindah pindah, apabila harus berpindah maka Network administrator harus mengkonfigurasikan ulang.

- Berdasarkan MAC Address

Keanggotaan suatu VLAN didasarkan pada MAC address dari setiap workstation /komputer yang dimiliki oleh user. Switch mendeteksi/mencatat semua MAC address

yang dimiliki oleh setiap Virtual LAN. MAC address merupakan suatu bagian yang dimiliki oleh NIC (Network Interface Card) di setiap workstation. Kelebihannya apabila user berpindah pindah maka dia akan tetap terkonfigurasi sebagai anggota dari VLAN tersebut.Sedangkan kekurangannya bahwa setiap mesin harus di konfigurasikan secara manual , dan untuk jaringan yang memiliki ratusan workstation maka tipe ini kurang efissien untuk dilakukan.

- Berdasarkan Tipe Protokol Yang Digunakan

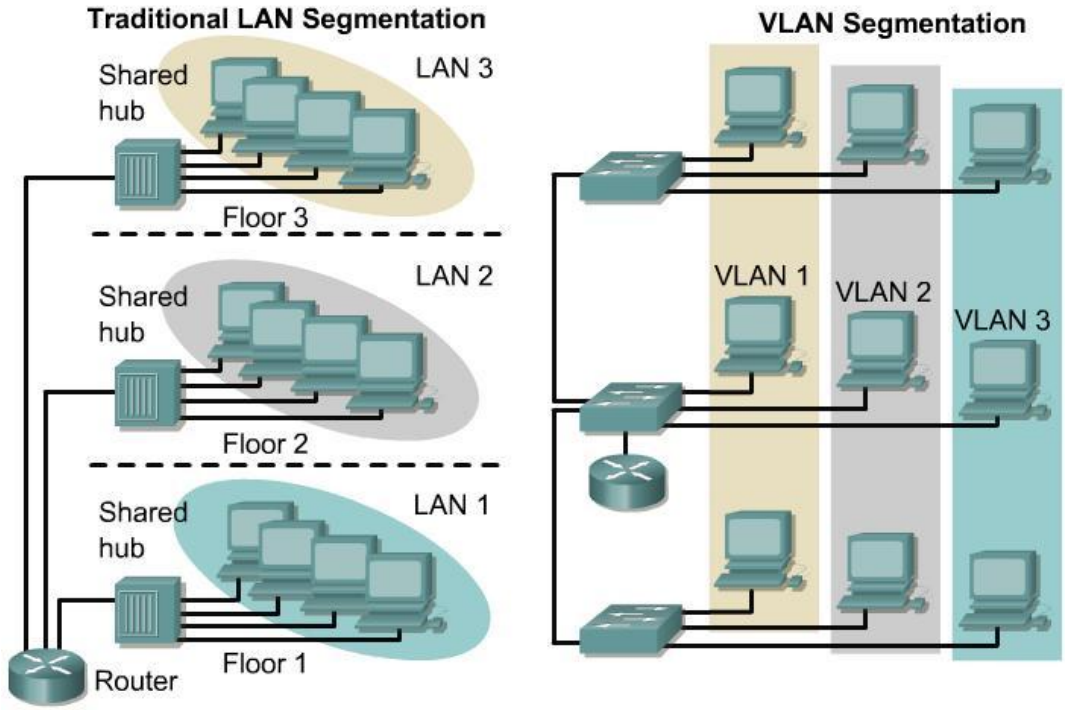
  Keanggotaan VLAN juga bisa berdasarkan protocol yang digunakan.

- Berdasarkan Alamat Subnet IP Subnet IP address pada suatu jaringan juga dapat digunakan untuk mengklasifikasi suatu VLAN

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

- Berdasarkan aplikasi atau kombinasi lain Sangat dimungkinkan untuk menentukan suatu VLAN berdasarkan aplikasi yang dijalankan, atau kombinasi dari semua tipe di atas untuk diterapkan pada suatu jaringan. Misalkan: aplikasi FTP (file transfer protocol) hanya bisa digunakan oleh VLAN 1 dan Telnet hanya bisa digunakan pada VLAN 2.

Perbedaan yang sangat jelas dari model jaringan Local Area Network dengan Virtual Local Area Network adalah bahwa bentuk jaringan dengan model Local Area Network sangat bergantung pada letak/fisik dari workstation, serta penggunaan hub dan repeater sebagai perangkat jaringan yang memiliki beberapa kelemahan. Sedangkan yang menjadi salah satu kelebihan dari model jaringan dengan VLAN adalah bahwa tiap-tiap workstation/user yang tergabung dalam satu VLAN/bagian (organisasi, kelompok dsb) dapat tetap saling berhubungan walaupun terpisah secara fisik.



Gambar 7.6 Perbedaan Antara LAN Dan VLAN

Perbandingan VLAN Dan LAN

- Perbandingan Tingkat Keamanan

Penggunaan LAN telah memungkinkan semua komputer yang terhubung dalam jaringan dapat bertukar data atau dengan kata lain berhubungan. Kerjasama ini semakin berkembang dari hanya pertukaran data hingga penggunaan peralatan secara bersama (resource sharing atau disebut juga hardware sharing).10 LAN memungkinkan data tersebar secara broadcast keseluruh jaringan, hal ini akan mengakibatkan mudahnya pengguna yang tidak dikenal (unauthorized user) untuk dapat mengakses semua bagian dari broadcast. Semakin besar broadcast, maka semakin besar akses yang didapat, kecuali hub yang dipakai diberi fungsi kontrol keamanan.

VLAN yang merupakan hasil konfigurasi switch menyebabkan setiap port switch diterapkan menjadi milik suatu VLAN. Oleh karena berada dalam satu segmen, port-port yang bernaung dibawah suatu VLAN dapat saling berkomunikasi langsung. Sedangkan port-port yang berada di luar VLAN tersebut atau berada dalam naungan VLAN lain, tidak dapat saling berkomunikasi langsung karena VLAN tidak meneruskan broadcast.

VLAN yang memiliki kemampuan untuk memberikan keuntungan tambahan dalam hal keamanan jaringan tidak menyediakan pembagian/penggunaan media/data dalam suatu jaringan secara keseluruhan. Switch pada jaringan menciptakan batas-batas yang hanya dapat

digunakan oleh komputer yang termasuk dalam VLAN tersebut. Hal ini mengakibatkan administrator dapat dengan mudah mensegmentasi pengguna, terutama dalam hal penggunaan media/data yang bersifat rahasia (sensitive information) kepada seluruh pengguna jaringan yang tergabung secara fisik.

Keamanan yang diberikan oleh VLAN meskipun lebih baik dari LAN,belum menjamin keamanan jaringan secara keseluruhan dan juga belum dapat dianggap cukup untuk menanggulangi seluruh masalah keamanan .VLAN masih sangat memerlukan berbagai tambahan untuk meningkatkan keamanan jaringan itu sendiri seperti firewall, pembatasan pengguna secara akses perindividu, intrusion detection, pengendalian jumlah dan besarnya broadcast domain, enkripsi jaringan, dsb.

Dukungan Tingkat keamanan yang lebih baik dari LAN inilah yang dapat dijadikan suatu nilai tambah dari penggunaan VLAN sebagai sistem jaringan. Salah satu kelebihan yang diberikan oleh penggunaan VLAN adalah control administrasi secara terpusat, artinya aplikasi dari manajemen VLAN dapat dikonfigurasikan, diatur dan diawasi secara terpusat, pengendalian broadcast jaringan, rencana perpindahan, penambahan, perubahan dan pengaturan akses khusus ke dalam jaringan serta mendapatkan media/data yang memiliki fungsi penting dalam perencanaan dan administrasi di dalam grup tersebut semuanya dapat dilakukan secara terpusat. Dengan adanya pengontrolan manajemen secara terpusat maka administrator jaringan juga dapat mengelompokkan grup-grup VLAN secara spesifik berdasarkan pengguna dan port dari switch yang digunakan, mengatur tingkat keamanan, mengambil dan menyebar data melewati jalur yang ada, mengkonfigurasi komunikasi yang melewati switch, dan memonitor lalu lintas data serta penggunaan bandwidth dari VLAN saat melalui tempat-tempat yang rawan di dalam jaringan.

- Perbandingan Tingkat Efisiensi

Untuk dapat mengetahui perbandingan tingkat efisiensinya maka perlu di ketahui kelebihan yang diberikan oleh VLAN itu sendiri diantaranya:

  – Meningkatkan Performa Jaringan LAN yang menggunakan hub dan repeater untuk menghubungkan peralatan komputer satu dengan lain yang bekerja dilapisan physical memiliki kelemahan, peralatan ini hanya meneruskan sinyal tanpa memiliki pengetahuan mengenai alamat-alamat yang dituju. Peralatan ini juga hanya memiliki satu domain collision sehingga bila salah satu port sibuk maka port-port yang lain harus menunggu. Walaupun peralatan dihubungkan ke port-port yang berlainan dari hub.
  – Protokol ethernet atau IEEE 802.3 (biasa digunakan pada LAN) menggunakan mekanisme yang disebut Carrier Sense Multiple Accsess Collision Detection (CSMA/CD) yaitu suatu cara dimana

peralatan memeriksa jaringan terlebih dahulu apakah ada pengiriman data oleh pihak lain. Jika tidak ada pengiriman data oleh pihak lain yang dideteksi, baru pengiriman data dilakukan. Bila terdapat dua data yang dikirimkan dalam waktu bersamaan, maka terjadilah tabrakan (collision) data pada jaringan. Oleh sebab itu jaringan ethernet dipakai hanya untuk transmisi half duplex, yaitu pada suatu saat hanya dapat mengirim atau menerima saja.

– Berbeda dari hub yang digunakan pada jaringan ethernet (LAN), switch yang bekerja pada lapisan datalink memiliki keunggulan dimana setiap port didalam switch memiliki domain collision sendiri-sendiri. Oleh sebab itu sebab itu switch sering disebut juga multiport bridge. Switch mempunyai tabel penterjemah pusat yang memiliki daftar penterjemah untuk semua port. Switch menciptakan jalur yang aman dari port pengirim dan port penerima sehingga jika dua host sedang berkomunikasi lewat jalur tersebut, mereka tidak mengganggu segmen lainnya. Jadi jika satu port sibuk, port-port lainnya tetap dapat berfungsi.
– Switch memungkinkan transmisi full-duplex untuk hubungan ke port dimana pengiriman dan penerimaan dapat dilakukan bersamaan dengan penggunakan jalur tersebut diatas. Persyaratan untuk dapat mengadakan hubungan full-duplex adalah hanya satu komputer atau server saja yang dapat dihubungkan ke satu port dari switch. Komputer tersebut harus memiliki network card yang mampu mengadakan hubungan full-duflex, serta collision detection dan loopback harus disable.
– Switch pula yang memungkinkan terjadinya segmentasi pada jaringan atau dengan kata lain switch-lah yang membentuk VLAN. Dengan adanya segmentasi yang membatasi jalur broadcast akan mengakibatkan suatu VLAN tidak dapat menerima dan mengirimkan jalur broadcast ke VLAN lainnya. Hal ini secara nyata akan mengurangi penggunaan jalur broadcast secara keseluruhan, mengurangi penggunaan bandwidth bagi pengguna, mengurangi kemungkinan terjadinya broadcast storms (badai siaran) yang dapat menyebabkan kemacetan total di jaringan komputer. Administrator jaringan dapat dengan mudah mengontrol ukuran dari jalur broadcast dengan cara mengurangi besarnya broadcast secara keseluruhan, membatasi jumlah port switch yang digunakan dalam satu VLAN serta jumlah pengguna yang tergabung dalam suatu VLAN.

- Terlepas dari Topologi Secara Fisik

Jika jumlah server dan workstation berjumlah banyak dan berada di lantai dan gedung yang berlainan, serta dengan para personel yang juga tersebar di berbagai tempat, maka akan lebih sulit bagi administrator jaringan yang menggunakan

sistem LAN untuk mengaturnya, dikarenakan akan banyak sekali diperlukan peralatan untuk menghubungkannya. Belum lagi apabila terjadi perubahan stuktur organisasi yang artinya akan terjadi banyak perubahan letak personil akibat hal tersebut. Permasalahan juga timbul dengan jaringan yang penggunanya tersebar di berbagai tempat artinya tidak terletak dalam satu lokasi tertentu secara fisik. LAN yang dapat didefinisikan sebagai network atau jaringan sejumlah sistem komputer yang lokasinya terbatas secara fisik, misalnya dalam satu gedung, satu komplek, dan bahkan ada yang menentukan LAN berdasarkan jaraknya sangat sulit untuk dapat mengatasi masalah ini.

Sedangkan VLAN yang memberikan kebebasan terhadap batasan lokasi secara fisik dengan mengijinkan workgroup yang terpisah lokasinya atau berlainan gedung, atau tersebar untuk dapat terhubung secara logik ke jaringan meskipun hanya satu pengguna. Jika infrastuktur secara fisik telah terinstalasi, maka hal ini tidak menjadi masalah untuk menambah port bagi VLAN yang baru jika organisasi atau departemen diperluas dan tiap bagian dipindah. Hal ini memberikan kemudahan dalam hal pemindahan personel, dan tidak terlalu sulit untuk memindahkan pralatan yang ada serta konfigurasinya dari satu tempat ke tempat lain.Untuk para pengguna yang terletak berlainan lokasi maka administrator jaringan hanya perlu menkofigurasikannya saja dalam satu port yang tergabung dalam satu VLAN yang dialokasikan untuk bagiannya sehingga pengguna tersebut dapat bekerja dalam bidangnya tanpa memikirkan apakah ia harus dalam ruangan yang sama dengan rekan-rekannya.

Hal ini juga mengurangi biaya yang dikeluarkan untuk membangun suatu jaringan baru apabila terjadi restrukturisasi pada suatu perusahaan, karena pada LAN semakin banyak terjadi perpindahan makin banyak pula kebutuhan akan pengkabelan ulang, hampir keseluruhan perpindahan dan perubahan membutuhkan konfigurasi ulang hub dan router. VLAN memberikan mekanisme secara efektif untuk mengontrol perubahan ini serta mengurangi banyak biaya untuk kebutuhan akan mengkonfigurasi ulang hub dan router. Pengguna VLAN dapat tetap berbagi dalam satu network address yang sama apabila ia tetap terhubung dalam satu swith port yang sama meskipun tidak dalam satu lokasi. Permasalahan dalam hal perubahan lokasi dapat diselesaikan dengan membuat komputer pengguna tergabung kedalam port pada VLAN tersebut dan mengkonfigurasikan switch pada VLAN tersebut.

- Mengembangkan Manajemen Jaringan

VLAN memberikan kemudahan, fleksibilitas, serta sedikitnya biaya yang dikeluarkan untuk membangunnya. VLAN membuat jaringan yang besar lebih mudah untuk diatur manajemennya karena VLAN mampu untuk melakukan konfigurasi secara terpusat terhadap peralatan yang ada pada lokasi yang terpisah. Dengan kemampuan VLAN untuk melakukan konfigurasi secara terpusat, maka sangat menguntungkan bagi pengembangan manajemen jaringan.

Dengan keunggulan yang diberikan oleh VLAN maka ada baiknya bagi setiap pengguna LAN untuk mulai beralih ke VLAN. VLAN yang merupakan pengembangan dari teknologi LAN ini tidak terlalu banyak melakukan perubahan, tetapi telah dapat memberikan berbagai tambahan pelayanan pada teknologi jaringan.

Program Trunking VLAN (VTP)

VTP digunakan untuk melakukan manajemen VLAN secara terpusat dari suatu network manager. Kelebihan VTP akan terlihat pada suatu jaringan yang besar dan memiliki banyak switch manageable yang terdiri dari beberapa VLAN yang terpisah secara lokasi. VTP hanya bekerja pada VLAN ID normal (1 – 1005) dan tidak dapat bekerja pada VLAN ID Extended (1006 – 4096). Keuntungan VTP :

- Konfigurasi VLAN yang lebih stabil di semua switch di network
- Pengiriman VLAN-advertisement terjadi hanya di trunk-port
- Menambahkan VLAN secara mudah dan terpusat
- Tracking dan monitoring VLAN-VLAN yang akurat.

Mode pada VTP :

- Mode Server, dimana mampu melakukan perubahan VLAN. Setiap perubahan akan disinkronisasi ke VTP client. Cannot create, modify or delete VLAN
- Mode Client, dmana hanya mampu menerima update VLAN dari VTP server. Can create, modify & delete VLAN
- Mode Transparent, dimana hanya meneruskan informasi sinkronisasi VLAN tanpa terpengaruh dengan informasi tersebut. Untuk melakukan perubahan VLAN secara local update. Can create, modify, & delete LOCAL VLAN, Forwards VTP advertisements.

Perbandingan Mode

- Server (default mode) :
  - Membuat, memodifikasi dan menghapus VLANs
  - Mensingkronisasikan konfigurasi VLAN
  - Menyimpan konfigurasi dalam NVRAM
  - Mengirim dan meneruskan advertisements
- Client
  - Tidak dapat membuat, merubah atau menghapus VLAN
  - Mensingkronisasikan konfigurasi VLAN
  - Tidak dapat menyimpan dalam NVRAM
  - Meneruskan advertisements
- Transparent
  - Membuat, memodifikasi dan menghapus lokal VLAN
  - Tidak dapat mensingkronisasikan konfigurasi VLAN
  - Menyimpan konfigurasi dalam NVRAM
- Meneruskan advertisements

Untuk melakukan pertukaran informasi dan sinkronisasi pada VTP hanya

terjadi pada satu domain yang sama. Pertukaran informasi menggunakan VTP advertisements . VTP memiliki VTP pruning yang digunakan untuk melakukan efisiensi bandwidth dengan cara mencegah flooding pada trunking. VTP Pruning VTP pruning meningkatkan ketersediaan bandwidth dengan melarang flooded traffic to those trunk links that the traffic must use to access the appropriate network devices. VLAN 1 selalu tidak dapat dipilih untuk pruning/pemangkasan: trafik dari VLAN 1 tidak dapat dipangkas. Biar lebih jelas mengetahui apa yang dimaksud dengan VTP Pruning ini, maka gambar di bawah perlu dicermati lebih lanjut.

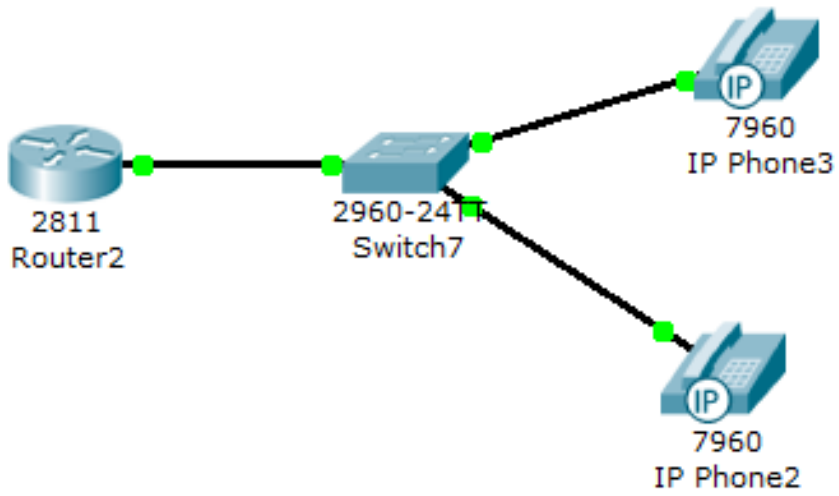
Karena semua switch dalam management domain mempelajari perubahan konvigurasi VLAN yang baru, suatu VLAN hanya perlu dibuat dan dikonfigurasi pada satu VTP server di dalam domain tersebut. Syarat agar antar switch dapat melakukan sinkronisasi:

- Berada dalam domain yang sama
- Memiliki password yang sama

Beberapa konfigurasi yang dapat digunakan pada perangkat Cisco :

- Pembentukan mode VTP
  Switch(config)#vtp mode [server/client/transparent]
- Pembentukan mode VTP domain
  Switch(config)#vtp domain [domain-name]
- Konfigurasi VTP password
  Switch(config)#vtp password [password]
- Verifikasi VTP
  Switch#sh vtp status
- Verifikasi VTP password
  Switch#sh vtp password

Konfigurasi VLAN Untuk IP Telephony Dan Nirkabel



Gambar 7.7 Skema Desain IP Phone

- *Pertama kita akan konfigurasi router. Pertama kita bikin DHCP dulu, biar IP Phone nya dapet IP.*

```
ip dhcp pool VOICE
   network 192.168.10.0 255.255.255.0
   default-router 192.168.10.1
   option 150 ip 192.168.10.1
```

  - Bikin DHCP Pool dengan nama Voice (bebas namanya)
  - IP-IP yang di DHCP pool itu dikasi network 192.168.10.0 /24
  - Option 150 itu untuk memberi tahu peralatan lain yang dapet IP, bahwa ada TFTP Server (mandatory dengan angka 150 default dari Cisco)
  - Option 150 IP 192.168.10.1 artinya TFTP servernya di IP 192.168.10.1

- Kedua kita berikan IP di FastEthernet 0/0 (port tempat router dan switch terhubung)

```
interface FastEthernet0/0
 ip address 192.168.10.1 255.255.255.0
```

  - *IP address ini akan jadi referensi untuk config CME*

- Ketiga kita config CME (call manager express)

```
telephony-service
 load 7960-7940 p00308000500
 max-ephones 5
 max-dn 5
 ip source-address 192.168.10.1 port 2000
 create cnf-files version-stamp Jan 01 2002 00:00:00
 max-conferences 4 gain -6
```

  - CME adalah fitur standar yang ada di DALAM router 2811, untuk CM bukan E, alias Business dan Enterprise digunakan Server sendiri (O/S-nya Linux Red Hat), CME jg bisa dipisahin, jadi Router full untuk network, bukan untuk Voice
  - Telephony-service = untuk aktifin CME itu
  - Karena phone kita adalah 7940, maka kita harus Load [type] [firmware-nya]

Firmware untuk 7940 itu p00308000500, bisa dicek di IP Phone-nya langsung dengan cara tekan tombol Setting di IP Phone –> Model Information (liat di App Load ID). Kemudian unttuk load filenya bisa dari flash router, diberikan settingan default

  - Max-ephones 5 adalah kita set maksimum 5 IP phone, ephone = telepon
  - Max-dn 5 adalah set maksimum ephone-dn 5, ephone-dn = nomor telepon, dimana artinya 1 phone bisa memiliki lebih dari1 nomor
  - IP source-add [ip router] port 2000 = untuk referensi IP Phone mendapatkan IP dan konfigurasi lain-lain, dimana port 2000 = protokol SCCP (Skinny Call Control Protocol), selain SCCP ada SIP dan H.323 (versi IETF)
  - Create cnf = bikin file CNF, alias file .XML buat IP Phone
  - Create cnf-files, Enter dan akan diberikan default cnf
  - Max-conference, itu configurasi otomatis klo tidak diset manual

- Register masing2 IP Phone (untuk mac-address biasanya otomatis)

```
ephone  1
 mac-address 0013.1AE5.C103
 type 7940
 button  1:1
!
!
!
ephone  2
 mac-address 0013.1ACB.F872
 type 7940
 button  1:2
```

  - ephone 1 (atau ephone 2) = masuk ke setting telepon, tergantung jumlah IP Phone yang akan digunakan
  - type [tipe ip phone], jenis IP Phone yang digunakan
  - button 1:2 (atau button 1:1) = untuk assign nomor ke telepon
  - sequential, alias untuk fa0/2 (IP Phone 1) dapet yang nomor pertama; fa0/3 dapet nomor ke dua, dan seterusnya
  - mac-address [mac address], input mac-address IP Phone yang akan digunakan, atau gunakan auto-assign di telephony service-nya

- Assign nomor telepon buat masing2 IP Phone

```
ephone-dn  1
 number 2100
!
!
ephone-dn  2
 number 2200
```

  - Untuk nomor telepon pertama, nomornya 2100
  - Untuk nomor telepon kedua, nomornya 2200

- Konfigurasi Switch
  - Kita set masing-masing interface switch yang ke ip phone ke voice vlan 1 (switchport voice vlan 1)

```
interface FastEthernet0/1
 switchport mode access
 switchport voice vlan 1
 spanning-tree portfast
!
interface FastEthernet0/2
 switchport mode access
 switchport voice vlan 1
 spanning-tree portfast
!
interface FastEthernet0/3
 switchport mode access
 switchport voice vlan 1
 spanning-tree portfast
!
interface FastEthernet0/4
 switchport mode access
 switchport voice vlan 1
 spanning-tree portfast
!
interface FastEthernet0/5
 switchport mode access
 switchport voice vlan 1
 spanning-tree portfast
```

  - Masing-masing port di switch fa0/1 – 5 diset jadi access dan membawa vlan voice 1
  - Bisa aja vlan 10, 20 atau yang lain…kita pake default vlan aja

```
interface Vlan1
 ip address dhcp
```

  - *Set interface vlan 1 dengan IP address-nya dari DHCP*

7.1.2.4 Mengasosiasi

Setelah mengikuti kegiatan belajar 7 ini siswa diharapkan dapat menyimpulkan pelbagai hasil percobaan dan pengamatan terkait dengan prinsip kerja switching dan segmentasi jaringan, prinsip kerja switching multilayer, identifikasi macam-macam switching, keamanan switch, perlindungan jaringan terhadap switching loop, redundansi

pada sebuah jaringan dengan switch, Protocol Spanning Tree (STP), prinsip root bridges, identifikasi spanning tree pada jaringan hirarkikal, Protocol Spanning Tree Cepat (RSTP), identifikasi dan konfigurasi VLAN, rute inter VLAN dan trunking, port trunk, memperluas VLAN melalui switch, routing antara VLAN-VLAN, perawatan VLAN dalam suatu jaringan perusahaan, program trunking VLAN (VTP), konfigurasi VTP, konfigurasi VLAN untuk IP telephony dan nirkabel.

7.1.3 Rangkuman

Jaringan yang besar di suatu perusahaan memerlukan perencanaan, implementasi dan pengelolaan yang benar dan dikerjakan oleh tim TI khusus dengan keahlian yang memadai. Setiap anggota tim harus memiliki pengetahuan dan ketrampilan dalam melakukan pengaturan tiap perangkat jaringan yang ada sehingga kelangsungan bisnis perusahaan bisa berjalan dengan lancar tanpa gangguan yang berarti.

Hal ini berarti dalam pembagian atau pengelolaan jaringan perusahaan, pada administrator harus memilih dan menerapkan metoda switching yang tepat untuk mendapatkan hasil yang maksimum. Tentu saja hal ini harus ditunjang juga oleh pemilihan perangkat keras switch dan router yang tepat. Pemilihan dan implementasi yang tidak tepat akan membuat perusahaan merugi karena investasi yang tidak menguntungkan.

7.1.4 Tugas

Buatlah kelompok terdiri atas 2-3 orang. Masing-masing kelompok membuat ringkasan tentang switching pada jaringan perusahaan, kemudian secara bergantian masing-masing kelompok mempresentasikan hasilnya didepan kelas.

1. Bacalah uraian materi diatas dengan teliti dan cermat.
2. Buatlah ringkasan materi menggunakan aplikasi pengolah presentasi.
3. Presentasikan hasil ringkasan di depan kelas.

7.1.5 Penilaian Diri

Setelah mengikuti kegiatan belajar 7 ini siswa diharapkan memiliki wawasan pengetahuan dan dapat menjawab pelbagai hal terkait dengan prinsip kerja switching dan segmentasi jaringan, prinsip kerja switching multilayer, identifikasi macam-macam switching, keamanan switch, perlindungan jaringan terhadap switching loop, redundansi pada sebuah jaringan dengan switch, Protocol Spanning Tree (STP), prinsip root bridges, identifikasi spanning tree pada jaringan hirarkikal, Protocol Spanning Tree Cepat (RSTP), identifikasi dan konfigurasi VLAN, rute inter VLAN dan trunking, port trunk, memperluas VLAN melalui switch, routing antara VLAN-VLAN, perawatan VLAN dalam suatu jaringan perusahaan, program trunking VLAN (VTP), konfigurasi VTP, konfigurasi VLAN untuk IP telephony dan nirkabel.

BAGIAN 3: PENUTUP

Dalam buku pelajaran Rancang Bangun Jaringan Untuk SMK/MAK Kelas XI Semester 2 ini telah dipaparkan materi-materi tentang :

- Konfigurasi peralatan-peralatan jaringan
- Routing jaringan komputer
- Layanan-layanan ISP
- Tugas dan tanggung jawab ISP
- Jaringan di enterprise
- Eksplorasi infrastruktur jaringan perusahaan
- Switching pada jaringan perusahaan

Dengan demikian maka setelah mempelajari buku ini, siswa diharapkan memiliki pengetahuan dan ketrampilan yang berhubungan dengan isi materi-materi tersebut di atas. Hal ini akan dapat membantu pada siswa untuk mengikuti materi-materi selanjutnya di kelas yang lebih tinggi, terutama yang masih dalam ruang lingkup konsentrasi jaringan komputer (TKJ).

DAFTAR PUSTAKA

1. Wagito. 2005. Jaringan Komputer : Teori dan Implementasi Berbasis Linux. Yogyakarta. Penerbit Gava Media.

2. Rafiudin, Rahmat. 2004. Panduan Membangun Jaringan Komputer Untuk Pemula (Edisi Ketiga). Jakarta. Elex Media Komputindo.

3. Sembiring, Jhony H. 2002. Jaringan Komputer Berbasis Linux (Edisi Kedua). Jakarta. Elex Media Komputindo.

4. Tim Penulis. 2001. Buku Pintar Penanganan Jaringan Komputer. Yogyakarta. Wahana Komputer Semarang & Andi Yogyakarta.

5. Tim Penulis. 1999. Pengelolaan Jaringan Komputer Novell Netware 4.1 (Edisi Ketiga). Yogyakarta. Wahana Komputer Semarang & Andi Yogyakarta.

6. Halsall, Fred. 1996. Data Communications, Computer Networks and Open Systems (Fourth Edition). United States of America. Addison Wesley.

7. Supriyanto. 2013. Jaringan Dasar 1 & 2 : Untuk SMK/MAK Kelas X. Jakarta. Kementerian Pendidikan & Kebudayaan.

8. William Stallings. 2011. Network Security Essentials: Applications and Standarts Fourth Edition. Prentice Hall.

9. Garfinkel, Simson and Gene Spafford.1996. Practical UNIX & Internet Security2nd edition. O'Reilly & Associates, Inc.

10. Purbo, Onno W. 1998. Buku Pintar Internet TCP/IP. Jakarta. PT Elex Media Komputindo.

11. Cisco System. 2005. Aironet Wireless LAN Fundamentals: Student Guide. Cisco System, Inc.

GLOSARIUM

Alamat IP Adalah nomor yang digunakan untuk mengindentifikasi komputer, server atau alat lain dalam jaringan internal atau internet lewat TCP/IP. Terdiri dari serangkaian (empat bagian) angka yang dipisah dengan tanda titik (misalnya 123.123.123.1).

Anonymous FTP Adalah metode penggunaan program FTP untuk masuk ke suatu komputer atau server dan mengambil (download) atau mengirim file walaupun anda tidak memiliki account pada komputer itu. Saat anda masuk, anda mengirimkan 'Anonymous' sebagai nama pengguna dan alamat email sebagai password, kemudian anda akan diarahkan ke folder atau direktori yang bisa diakses secara anonim.

Aplikasi Web Adalah aplikasi atau program yang dikirimkan lewat teknologi internet. Aplikasi dijalankan pada server dan disajikan melalui browser, memungkinkan interaktivitas antara pengunjung situs. Contoh aplikasi web adalah CMS (content managment), weblog, forum diskusi, webmail, wiki, toko online, dsb.

Bandwidth Adalah jumlah besaran data (bit) yang bisa dikirimkan (ditransfer/ditransmisikan), yang dihitung dengan satuan bit per detik, kilobit per detik, megabit per detik, dan seterusnya. 1 byte data terdiri dari 8 bit.

Browser Atau web browser (terjemahan Bahasa Indonesia: peramban), adalah program komputer untuk menampilkan file atau halaman dari sebuah situs internet. Saat anda menjelajahi (surfing) internet, anda memulainya dengan menjalankan program browser ini, lalu memerintahkan program ini untuk masuk ke sebuah situs internet. Contoh browser: Mozilla, Firefox, Safari, Opera, Internet Explorer, Konqueror, Lynx, Netscape, dsb.

CGI Atau Common Gateway Interface, adalah program yang menerjemahkan data dari web server dan menampilkannya pada situs internet atau dikirim ke email. Dengan CGI halaman situs internet berinteraksi dengan aplikasi program lain. CGI melibatkan transfer data antara server dan program CGI (disebut juga script), sehingga sebuah situs internet menjadi interaktif dengan input/masukan dari pengunjungnya. Form, buku tamu, forum diskusi, pengiriman komentar dan fitur lainnya bisa dibuat dengan CGI.

CMS Atau content management system. Adalah aplikasi web untuk mengelola konten sebuah (atau lebih) situs internet. Masing-masing CMS memiliki fitur-fitur, diantaranya adalah pengelolaan berita, buku tamu, forum diskusi, sistem komentar, sistem keanggotaan, dsb.

Data Transfer Adalah jumlah data yang

ditransfer, baik transfer masuk atau transfer keluar, lewat suatu jenis koneksi dalam satu kurun waktu tertentu. Lihat juga -> Bandwidth.

DNS Domain Name System (bahasa Indonesia: Sistem Penamaan Domain) adalah sebuah sistem yang menyimpan informasi tentang nama host maupun nama domain dalam bentuk basis data tersebar (distributed database) di dalam jaringan komputer, misalkan: Internet. DNS menyediakan alamat IP untuk setiap nama host dan mendata setiap server transmisi surat (mail exchange server) yang menerima surat elektronik (email) untuk setiap domain. Setiap nama host/komputer memiliki alamat IP (internet protocol) sendiri yang terdiri dari serangkaian angka, DNS memudahkan kita mengingat/mencari alamat situs/email dengan menerjemahkan angka-angka ini menjadi nama yang lebih mudah diingat manusia.

Domain Atau nama domain, seperti www.namakamu.com, adalah cara untuk memudahkan mengingat satu alamat internet. Server DNS mengasosiasikan alamat IP dengan nama domain. Saat anda memerintahkan browser anda membuka www.namakamu.com, browser ini mengarahkannya ke alamat IP yang dimilikinya. Ada beberapa tingkatan domain, diantaranya TLD (top level domain) atau domain internasional seperti .com/.net/.org atau domain negara seperti .or.id/.co.id/.web.id/.com.my/.com.sg/.nl/.de dan sebagainya.

Download Proses transfer data dari server/situs internet ke komputer pribadi (pengguna). Terjemahan Bahasa Indonesia=unduh

FTP Adalah singkatan dari File Transfer Protocol, protokol Internet yang merupakan standar untuk pentransferan file komputer antara mesin-mesin yang menjalankan sistem yang sangat berbeda, misalnya dari komputer rumahan dan/ke server situs anda. Karena berfungsi sebagai file sharing maka kita dapat mendownload dan mengupload file yang kita inginkan. Seperti halnya browsing, FTP juga memiliki alamat. Alamat yang digunakan untuk browsing dapat diawali dengan http misalnya sedangkan FTP diawali dengan ftp.

Homepage Adalah halaman depan atau halaman utama sebuah situs internet.

HTML Hyper Text Markup Language. Sebuah halaman dalam situs internet ditulis dengan bahasa ini, yang kemudian diterjemahkan oleh web browser menjadi seperti tampilan yang anda lihat.

HTTP Hyper Text Transfer Protocol. Adalah protokol untuk mengirim file hyperteks (HTML) pada internet. Membutuhkan program klien HTTP di satu sisi, dan program server HTTP di sisi lainnya. HTTP adalah protokol paling penting yang digunakan di jagat

internet (World Wide Web). Anda akan menggunakannya setiap kali mengunjungi sebuah situs internet.

IP Private Alamat IP yang digunakan untuk jaringan internal (intranet). IP Private tidak bisa diakses dari jaringan internet. Rentang IP yang bisa digunakan untuk jaringan internal adalah: 10.0.0.0 - 10.255.255.255, 172.16.0.0 - 172.31.255.255, dan 192.168.0.0 - 192.168.255.255.

IP Publik Alamat IP yang bisa diakses secara publik lewat jaringan global (internet). Supaya nama domain, email dan web anda bisa diakses oleh pengunjung lain di internet, digunakan IP Publik. Lihat juga - > IP Private

Nameserver Sebuah server yang menyimpan dan melayani sistem penamaan domain dengan protokol DNS, menerjemahkan nama domain ke alamat IP yang terkait dan sebaliknya. Setiap nama domain harus memiliki minimal 2 (dua) nameserver, 1 sebagai nameserver utama dan yang kedua sebagai cadangan jika ada masalah pada nameserver pertama, sehingga domain itu selalu bisa ditemukan.

Propagasi DNS Adalah masa pemberitahuan perubahan atas satu domain, perubahan ini bisa berarti perubahan nameserver atau transfer; atau jika nama domain tersebut baru pertama kali didaftarkan. Dalam masa ini informasi domain anda disebarluaskan ke seluruh nameserver induk di seluruh dunia. Proses ini tampak seperti lama, tetapi pada masing-masing server sebenarnya berlangsung sangat cepat, karena banyaknya nameserver yang harus diberi tahu proses ini bisa memakan waktu sampai 72 jam, tetapi umumnya berlangsung singkat (kurang dari 30 menit). Selama masa propagasi ini nama domain tidak bisa diakses.

Registrar Dalam hal ini dianggap sebagai Domain Registrar adalah organisasi atau perusahaan yang berwenang memberikan sebuah nama domain kepada yang mendaftarkannya menurut TLD (top level domain) tertentu (.com/.net/.org) atau domain negara (.id/.my/.sg, dsb).

SSL Secured Socket Layer, adalah protokol untuk mengirimkan data yang di- enkrip (disamarkan), dengan komunikasi terotentikasi, lewat internet. Pertama kali dirancang oleh Netscape Communication. Kebanyakan digunakan dalam komunikasi antara web browser dan server. URL yang dimulai dengan "https://" menunjukkan bahwa halaman tersebut disajikan dengan jenis koneksi aman ini. SSL menyediakan 3 (tiga) hal penting: Privasi, Otentikasi dan Integritas Pesan. Pada jenis koneksi ini, masing-masing bagian yag berkomunikasi (misalnya browser dan server) harus mempunyai Sertifikat Keamanan (Security Certificate) dan saling mengirimkannya. Masing-masing bagian itu kemudian meng-enkrip (meyandikan) apa yang dikirim dengan informasi yang ada dalam sertifikat itu dan sertifikat

pasangannya, memastikan bahwa hanya penerima yang diinginkan saja yang bisa membaca pesan tersandi (di-enkrip) itu, dan dikirim dari lokasi yang memang seharusnya dan isi pesan yang dikirim tidak diubah. Dengan keamanan seperti ini, SSL banyak digunakan pada situs komersial untuk menjalankan transaksi lewat internet atau situs yang mengirim data sensitif.

TCP/IP Adalah rangkaian protokol komunikasi untuk menghubungkan komputer atau server pada internet.

Upload Proses transfer data/file dari komputer pribadi (komputer pengguna) ke server. Terjemahan Bahasa Indonesia = unggah

Uptime Merujuk pada sejumlah waktu dalam periode 24 jam dimana sebuah sistem atau server aktif menjalankan tugas menyediakan layanan. Misalnya jika uptime 99.9% berarti masa aktif situs tersebut adalah 24 jam dikurang 0.1% (8 detik), dan dalam 1 tahun ada masa tidak aktif selama 48 jam. Masa tidak aktif ini biasanya digunakan untuk perawatan/pemeliharaan server.

URL Kependekan dari Uniform Resource Locator, alamat sebuah sumber pada internet.

Visit/Sesi (Statistik) Serangkaian permintaan (permintaan) ke suatu website dari satu pengunjung unik dalam satu waktu. Sebuah kunjungan (visit) atau sesi kunjungan bisa terdiri dari beberapa hits dan page view.