Jaringan Komputer

(Digunakan di lingkungan sendiri, sebagai buku ajar mata kuliah Jaringan Komputer)

Fakultas Teknik dan Ilmu Komputer

Program Studi Sistem Informasi

Universitas Komputer Indonesia

1. Pertemuan 1

1.1. Pengantar Jaringan Komputer

Apa itu jaringan komputer

Jaringan komputer merupakan suatu sistem yang terdiri dari komputer-komputer dan perangkat-perangkat jaringan lainnya yang terhubung satu sama lain, bekerja sama untuk mencapai suatu tujuan. Perangkat jaringan sangat penting untuk berlangsungnya hubungan atau komunikasi antar komputer.

Informasi berpindah dari komputer ke komputer lainnya dengan menggunakan jaringan daripada melalui perantara manusia. Sehingga membuat pertukaran informasi menjadi lebih mudah dan cepat.

Kebanyakan jaringan dasar memiliki dua buah komputer yang berkomunikasi satu sama lain dengan medium kabel ataupun medium lainnya. Ketika komputer Anda terhubung ke komputer lain, Anda dapat memindahkan informasi dengan cepat dan efisien.

Pada buku ”Networking Complete” dijelaskan bahwa sekumpulan komputer dan peralatan lainnya yang terhubung bersama-sama disebut network, sedangkan konsep dari komputer yang terkoneksi dan saling berbagi sumber (resources) disebut networking.

Network Building Blocks

Semua jaringan, baik itu besar maupun kecil, membutuhkan hardware khusus jaringan. Untuk jaringan kecil, hardware mungkin dapat terdiri dari tidak lebih dari network interface card (NIC) pada setiap komputer, kabel untuk setiap komputer, dan switch jaringan dimana semua komputer tersambung. Jaringan besar mungkin tedapat komponen tambahan seperti router atau repeater.

Kecil atau besar, semua jaringan dibangun dari building block dasar berikut:

Komputer client
Komputer yang digunakan oleh end user untuk mengakses sumber daya yang ada dijaringan. Komputer client terkadang ditunjuk sebagai workstation.

Komputer server
Komputer yang menyediakan sumber daya yang digunakan untuk bersama, seperti disk storage dan printer, dan juga layanan jaringan, seperti e-mail dan akses Internet. Komputer server khususnya menjalankan sistem operasi khusus jaringan seperti Windows Server 2003, NetWare, atau Linux, beserta software khusus untuk menyediakan layanan jaringan. Sebagai contoh, server mungkin menjalankan Microsoft Exchange untuk menyediakan layanan e-mail bagi jaringan, atau menjalankan Apache Web Server sehingga komputer dapat menyajikan halaman Web.

Network interface card (NIC)
Network interface card yang terpasang dalam komputer memungkinkan komputer untuk berkomunikasi melalui jaringan. Hampir setiap NIC mengimplementasikan standar networking yang dinamakan Ethernet. Setiap komputer client dan server harus
memiliki network interface card (atau built-in network port) jika ingin menjadi bagian dari jaringan.

Kabel
Komputer dalam jaringan biasanya secara fisik terhubung satu sama lain dengan menggunakan kabel. Meskipun terdapat beberapa tipe kabel yang populer, kabel yang biasa dipakai saat ini adalah twisted pair atau juga disebut 10BaseT. Tipe kabel lainnya yang juga biasa dipakai adalah coaxial atau juga disebut 10Base2. Untuk koneksi jaringan kecepatan tinggi, terkadang digunakan kabel fiber-optic. Dalam kebanyakan kasus, kabel dibentangkan melalui tembok dan dikumpulkan diruangan pusat

yang dinamakan wiring closet. Tetapi untuk jaringan yang lebih kecil, kabel biasanya hanya dibentangkan di lantai saja.

Switch

Kabel jaringan biasanya tidak dihubungkan secara langsung ke komputer lainnya. Melainkan, setiap komputer dihubungkan dengan kabel ke alat yang dinamakan switch. Switch, sebaliknya, menghubungkannya ke jaringan. Setiap switch memuat beberapa buah port, biasanya 8 atau 16. Dengan demikian kita dapat menggunakan
switch 8 port untuk menghubungkan delapan buah komputer.

Switch dapat dihubungkan satu sama lain untuk membangun jaringan yang lebih besar. Jaringan lama mungkin masih ada yang menggunakan alat yang dinamakan hub selain switch. Hub menyediakan fungsi yang sama seperti switch tetapi tidak seefesien switch.

Jaringan wireless

Pada jaringan wireless komputer berkomunikasi dengan komputer lainnya melalui sinyal radio. Dalam jaringan wireless, radio transmitter dan radio receiver menggantikan kabel. Keuntungan utama dari jaringan wireless adalah fleksibilitas. Dengan jaringan wireless, kita tidak perlu menarik kabel melalui dinding atau langitlangit, dan komputer client dapat ditempatkan dimana saja selama masih dalam jarak network broadcast. Ketidakuntungan yang utama dari jaringan wireless adalah kurang aman dari jaringan yang menggunakan kabel.

Software jaringan

Meskipun hardware jaringan penting sekali, sebenarnya yang benar-benar menjalankan jaringan adalah software. Banyak software yang harus di-set up sesuai perintah agar jaringan dapat bekerja. Komputer server khususnya menggunakan sistem operasi khusus jaringan (network operating system atau NOS) agar berfungsi secara efisien, dan komputer client membutuhkan setting jaringannya dikonfigurasi dengan benar agar dapat mengakses jaringan.

Tujuan dan manfaat membangun jaringan komputer

Dalam membangun jaringan komputer tentunya memiliki tujuan dan manfaat yang sangat membantu bagi kita yaitu:

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.

Pengembangan dan pemeliharaan menjadi mudah dan menghemat biaya.
Misalnya pada suatu perusahaan dapat menghemat peralatan yang harus digunakan.

Aplikasi Berbasis Jaringan

Jaringan digunakan untuk menyediakan layanan jaringan bagi pengguna jaringan. Aplikasi jaringan yang tersedia pada umumnya yaitu file service, print service, web service, e-mail, file transfer service.

File Service

Komputer dimana file tersimpan disebut file server. Komputer lain (yang mengakses) disebut client, dan yang dapat dilakukan adalah membaca dan menulis pada file-file tersebut, tanpa perlu membuat salinan lokal file pada disk drive client. Layanan ini biasanya transparan bagi end user.

Print Service

Printer yang dikoneksikan ke sebuah komputer disebut print server. Komputer client dapat mengirim file ke print server, yang selanjutnya mencetak file pada printer. Server ini biasanya transparan bagi user.

Web Service

Server menyimpan berbagai informasi, termasuk teks, grafis, animasi, gambar, video, dan audio. End user menggunakan browser web untuk meminta informasi dari server. Server mengembalikan informasi yang ditampilkan oleh browser web.

E-mail

End user membuat e-mail dengan menggunakan program e-mail client dan mengirim e-mail ke orang tertentu. E-mail server membantu proses pengiriman e-mail.

File Transfer Service

File juga disimpan pada server. Server ini memungkinkan komputer (client) lain untuk menyalin file-file dari server ke disk drive lokal mereka dan mengganti isi file pada file server dengan file pada disk drive lokal client.

Klasifikasi jaringan komputer berdasarkan area

Jaringan komputer dapat diklasifikasikan berdasarkan besarnya area jaringan tersebut yaitu LAN, MAN, WAN.

LAN (Local Area Networking)

Local Area Network adalah jaringan milik pribadi dalam satu lokasi, biasanya pada satu lantai di sebuah gedung, kampus, atau semua komputer dalam suatu perusahaan. Besarnya cakupan area jaringan LAN mencapai beberapa kilometer.

MAN (Metropolitant Area Networking)

Metropolitan Area Network pada dasarnya merupakan versi yang lebih besar dari LAN dan umumnya menggunakan teknologi yang sama. Dan cakupannya mungkin berupa sekelompok kantor cabang yang letaknya berdekatan.

WAN (Wide Area Networking)

Wide Area Network menjangkau area geografis yang besar, biasanya negara atau benua.

Jaringan Komputer Berdasarkan Peranan (fungsi)

Berdasarkan peranannya maka ada tiga jenis jaringan komputer, yaitu client-server (kadang juga disebut server-based), peer-to-peer, hybrid network:

Client-Server
Yaitu jaringan komputer dimana didalam jaringan tersebut terdapat satu komputer yang didedikasikan khusus sebagai server. Server tersebut mempunyai tanggungjawab untuk memberikan service/layanan yang diberikan ke komputer lainnya.

Layanan yang umum disediakan oleh server biasanya memberikan layanan-layanan seperti file service, print service, web service, e-mail, file transfer service. Dimana nantinya komputer (client) lain dapat mengakses layanan yang diberikan oleh server tersebut.

Peer-to-peer
Merupakan jaringan komputer dimana setiap komputer dapat menjadi server dan juga menjadi client secara bersamaan. Contohnya dalam file sharing antar komputer di Jaringan Windows Network Neighbourhood ada 5 komputer (kita beri nama A,B,C,D dan E) yang memberi hak akses terhadap file yang dimilikinya. Pada satu saat A mengakses file share dari B bernama data_nilai.xls dan juga memberi akses filesoal_uas.doc kepada C. Saat A mengakses file dari B maka A berfungsi sebagai client dan saat A memberi akses file kepada C maka A berfungsi sebagai server. Kedua fungsi itu dilakukan oleh A secara bersamaan maka jaringan seperti ini dinamakan peer to peer.

Hybrid Network
Kebanyakan jaringan sebenarnya sebenarnya merupakan hybrid network. Pada jenis jaringan ini umumnya memiliki active domains dan workgroups. Hybrid network adalah jaringan berbasis client-server dimana di dalam jaringan tersebut selain server menyediakan kebanyakan sumber yang dibutuhkan oleh user, tetapi user juga masih

dapat mengakses sumber-sumber yang disediakan oleh user lain (peer-to-peer) dalam satu workgroup.

Topologi jaringan

Berdasarkan topologi jaringan, jaringan komputer dapat dibedakan atas:

- Topologi Bus
- Topologi Bintang
- Topologi Cincin
- Topologi Mesh (Acak)
- Topologi Pohon (Hirarkies)
- Topologi Linier

1.2. Topologi Jaringan Komputer dan Jaringan Komunikasi Data

Komunikasi Data dan Jaringan Komputer

a. Jaringan Komputer

Jaringan komputer adalah kumpulan komputer, printer dan peralatan lainnya yang terhubung dalam satu kesatuan. Setiap komputer printer atau peripheral yang terhubung dengan jaringan disebut node.

Secara umum jaringan komputer dibagi atas lima jenis, yaitu :

1. Local Area Network (LAN) , merupakan jaringan milik pribadi di dalam sebuah gedung atau kampus yang berukuran sampai beberapa kilometer.

2. Metropolitan Area Network (MAN) , pada dasarnya merupakan versi LAN yang berukuran lebih besar dan biasanya menggunakan teknologi yang sama dengan LAN. MAN dapat mencakup kantor-kantor perusahaan yang letaknya berdekatan atau juga sebuah kota.

3. Wide Area Network (WAN) , jangkauannya mecakup daerah geografis yang luas, seringkali mencakup sebuah negara bahkan benua. WAN terdiri dari kumpulan mesin-mesin yang bertujuan untuk menjalankan program-program (aplikasi) pemakai.

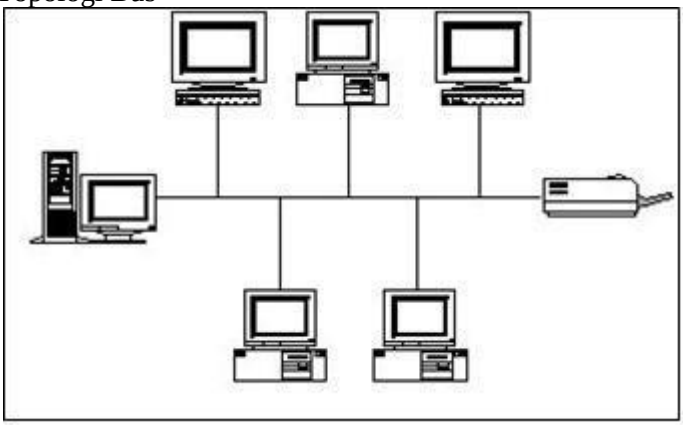
4. Internet , pada dasarnya internet merupakan kumpulan jaringan yang terinterkoneksi. Hal ini terjadi karena orang yang

terhubung ke jaringan sering berharap untuk bisa berkomunikasi dengan orang lain yang terhubung jaringan lainnya. Untuk melakukan hal ini diperlukan sebuah mesin yang disebut gateway guna melakukan hubungan dan melaksanakan terjemahan yang diperlukan, baik perangkat keras maupun perangkat lunaknya.

5. Jaringan Tanpa Kabel , merupakan solusi terhadap komunikasi yang tidak bisa dilakukan dengan jaringan yang menggunakan kabel.

Topologi adalah suatu cara menghubungkan komputer yang satu dengan komputer lainnya sehingga membentuk jaringan. Cara yang saat ini banyak digunakan adalah bus, token-ring, dan star. Masing-masing topologi ini mempunyai ciri khas, dengan kelebihan dan kekurangannya sendiri.

1. Topologi Bus



Keuntungan

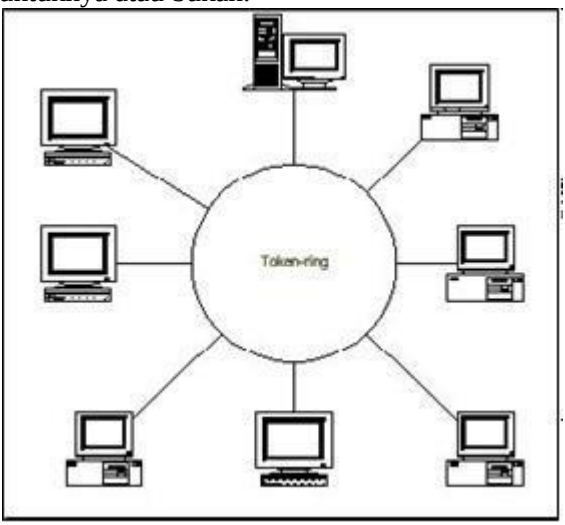
• Hemat kabel
• Layout kabel sederhana
• Mudah dikembangkan

Kerugian

• Deteksi dan isolasi kesalahan sangat kecil
• Kepadatan lalu lintas
• Bila salah satu client rusak, maka jaringan tidak bisa berfungsi.
• Diperlukan repeater untuk jarak jauh

2. Topologi Token Ring

Metode token-ring (sering disebut ring saja) adalah cara menghubungkan komputer sehingga berbentuk ring (lingkaran). Setiap simpul mempunyai tingkatan yang sama. Jaringan akan disebut sebagai loop, data dikirimkan kesetiap simpul dan setiap informasi yang diterima simpul diperiksa alamatnya apakah data itu untuknya atau bukan.



Keuntungan

• Hemat Kabel

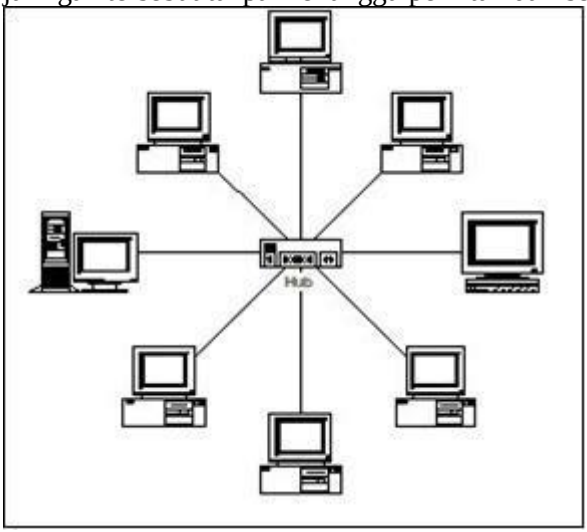
Kerugian

• Peka kesalahan

• Pengembangan jaringan lebih kaku

3. Topologi Star

Kontrol terpusat, semua link harus melewati pusat yang menyalurkan data tersebut kesemua simpul atau client yang dipilihnya. Simpul pusat dinamakan stasiun primer atau server dan ainnya dinamakan stasiun sekunder atau client server. Setelah hubungan jaringan dimulai oleh server maka setiap client server sewaktu-waktu dapat menggunakan hubungan jaringan tersebut tanpa menunggu perintah dari server.



Keuntungan

• Paling fleksibel

• Pemasangan stasiun sangat mudah dan tidak mengganggu bagian jaringan lain

• Kontrol terpusat

• Kemudahan deteksi dan isolasi kesalahan/kerusakan

• Kemudahaan pengelolaan jaringan

Kerugian

• Boros kabel

• Perlu penanganan khusus

• Kontrol terpusat (HUB) jadi elemen kritis

a. Komunikasi Data

Komunikasi data adalah bagian dari telekomunikasi yang secara khusus berkenaan dengan transmisi atau pemindahan data dan informasi diantara komputer-komputer dan piranti-piranti yang lain dalam bentuk digital yang dikirimkan melalui media komunikasi data. Data berarti informasi yang disajikan oleh isyarat digital.

1. Penghantar/pengirim, adalah piranti yang mengirimkan data
2. Penerima, adalah piranti yang menerima data
3. Data, adalah informasi yang akan dipindahkan
4. Media pengiriman, adalah media atau saluran yang digunakan untuk mengirimkan data
5. Protokol, adalah aturan-aturan yang berfungsi untuk menyelaraskan hubungan

Protokol adalah sebuah aturan yang mendefinisikan beberapa fungsi yang ada dalam sebuah jaringan komputer, misalnya mengirim pesan, data, informasi dan fungsi lain yang harus dipenuhi oleh sisi pengirim dan sisi penerima agar komunikasi dapat berlangsung dengan benar, walaupun sistem yang ada dalam jaringan tersebut berbeda sama sekali.

Standar protokol yang terkenal yaitu OSI (Open System Interconnecting) yang ditentukan oleh ISO (International Standart Organization).

Fungsi dari protokol adalah untuk menghubungkan sisi pengirim dan sisi penerima dalam berkomunikasi serta dalam bertukar informasi agar dapat berjalan dengan baik dan benar.

2. Pertemuan 2

2.1. Definisi dan Jenis-jenis Network Layer

Network Layer Jaringan Komputer

Sebuah jaringan komputer, baik jaringan komputer yang besar maupun jaringan komputer yang kecil, memiliki sebuah struktur yang simple, namun kompleks. Untuk penyusunan perangkat kerasnya, mungkin jaringan komputer memiliki struktur yang cukup simple, karena hanya menghubungkan antar perangkat keras saja.

Akan tetapi, secara logic dan dari segi softwarenya, jaringan komputer memiliki struktur yang sangat kompleks dan cenderung rumit, karena terdiri dari banyak sekali struktur, dan banyak sekali proses yang harus dilewati oleh sebuah data di dalam jaringan komputer tersebut.

Salah satu struktur kompleks yang harus dilalui oleh sebuah data di dalam jaringan komputer adalah lapisan – lapisan atau layer jaringan. Layer jaringan mengacu pada OSI layer, yangmerupakan sebuah sistem jaringan yang terdiri dari 7 buah lapisan logic yang harus dilalui oleh setiap paket data di dalam jaringan komputer agar bisa ditransmisikan dari satu komputer ke komputer lainnya.

Singkatnya, ketika anda akan mengirimkan sebuah data melalui jaringan komputer, data yang anda kirimkan akan melewati proses yang panjang, yaitu dengan melewati 7 buah sistem lapisan logic, yang terdiri dari :

1. Application Layer
2. Presentation Layer
3. Session Layer
4. Transport Layer
5. Network Layer
6. Data Link Layer
7. Physical layer

Ketujuh lapisan logic inilah yang memiliki peran penting dalam proses transmisi data yang berlangsung di dalam sebuah

jaringan komputer, yang tentu saja bekerja secara logic, dan tidak bisa kita lihat secara kasat mata.

Network Layer

Salah satu layer atau lapisan yang terdapat di dalam sistem lapisan OSI layer yang cukup memiliki peran penting adalah network layer. Lapisan yang bekerja pada tingkat ke 5 ini merupakan lapisan yang memiliki peran penting dalam proses transmisi jaringan komputer. Penjelasan lebih lengkap mengenai network layer dapat dilihat pada penjelasan di bawah ini.

Apa itu Network Layer?

Network layer jaringan komputer atau yang bisa juga kita kenal dengan istilah lapisan jaringan merupakan salah satu bagian layer pada keseluruhan sistem OSI Layer Reference Model yang terdiri dari 7 buah lapisan atau layer. Network layer adalah layer atau lapisan yang bekerja di antara data link layer dan transport layer, tergantung pada proses yang sedang berlangsung.

Network layer merupalan sistem logic yang sangat erat kaitannya dengan proses transmisi data, karena menghubungkan komputer ke dalam berabagai jaringan – jaringan yang sudah ada. MAC address juga memiliki peran penting dalam lapisan ini, bersamaan dengan pendefinisian dari IP address (Internet Protocol).

Fungsi dari Network Layer

Network layer, yang merupakan lapisan ke lima pada keseluruhan sistem jaringan OSI Layer memiliki beberapa fungsi dalam jarignan komputer. Berikut ini adalah beberapa fungsi dari network layer :

1. Menentukan tujuan data pada sebuah jaringan

Sebuah data dan juga paket data tentu saja memiliki tujuan. Tujuan dari paket data tersebut adalah komputer lainnya yang juga sudah terhubung ke dalam jaringan. Untuk dapat menentukan komputer mana yang akan ditransmisikan paket datanya, maka network layer memiliki peran yang sangat penting. Network layer akan menentukan kemana sebuah paket data akan ditransmisikan, sesuai dengan perintah yang sdah diberikan kepadanya.

2. Mendefinisikan alamat IP

Untuk dapat menentukan komputer mana yang akan menjadi tujuan dan juga menerima paket data yang akan ditransmisikan, maka network layer kemudian akan mendefinisikan masing – masing alamat IP atau IP address. IP address merupakan sebuah alamat unik yang dimiliki oleh setiap komputer yang terhubung ke dalam suatu jaringan komputer.

Dengan begitu, nantinya network layer akan lebih mudah menentukan tujuan dari paket data yang akan dikirimkan olehnya. IP address ini akan secara otomatis didefinisikan dan dicari oleh network layer, sebagai alamat tujuan paket data tersebut.

3. Membuat header pada peket – paket data yang ada

Header diibaratkan seperti sebuah ‘judul’ pada paket data. Dengan adanya header ini, paka paket data (yang merupakan bagian atau fragmen dari sebuah data) akan memiliki header tersendiri dan tidak akan terpecah belah. Misalnya, sebuah data bernama X, akan dipecah ke dalam bentuk paket data, dengan masing – masing header “X1, X2, X3, dst”.

Dengan adanya header ini, maka setiap paket data akan memiliki header yang sama, sehingga ketika nantinya paket data akan disatukan kembali menjadi sebuah data yang utuh, paket data tersebut dapat disatukan kembali dengan mudah, dan bisa terdeteksi apabila ada paket data yang hilang ataupun mengalami kerusakan.

4. Melakukan proses routing

Proses routing merupakan proses pemberian rute dari sebuah paket data. Selain membantu mendefinisikan IP address, network layer juga memilki fungsi yang sangat penting untuk meneruskan paket data yang sudah ada menuju penerimanya melalui rute – rute tertentu. namun demikian, rute – rute tersebut sudah terlebih dahulu didefinisikan melalui apa yang kita kenal dengan nama tabel routing.

Dengan demikian tiap paket data akan dikirmkan ke alamt yang sudah didefinisikan sebelumnya, sehingga dapat mencegah terjadinya salah alamat.

Perangkat keras yang berhubungan dan digunkan dalam network layer

Sama seperti lapisan logic lainnya, network layer merupakan lapisan yang tidak dapat dilihat dan diraba secara fisik, namun memiliki asosiasi dan keterkaitan kerja yang erat dengan perangkat keras jaringan komputr secara fisik. Salah satu perangkat keras yang bekerja dengan network layer adalah router.

Router merupakan perangkat keras jaringan komputer yang memiliki fungsi sangat penting dalam meneruskan paket data dari satu lokasi ke lokasi lainnya dengna menggunakan rute – rute tertentu. Dalam router, kita juga mengenal istilah tabel routing, yaitu merupakan sebuah sistem tebel, yang mirip seperti sistem peta atau sistem penjadwalan, yang berisi jalur atau rute mana saja yang bisa dilewati oleh sebuah paket data, rute atau jalan mana yang sdah tidak bisa digunakan, serta pembuatan rute baru.

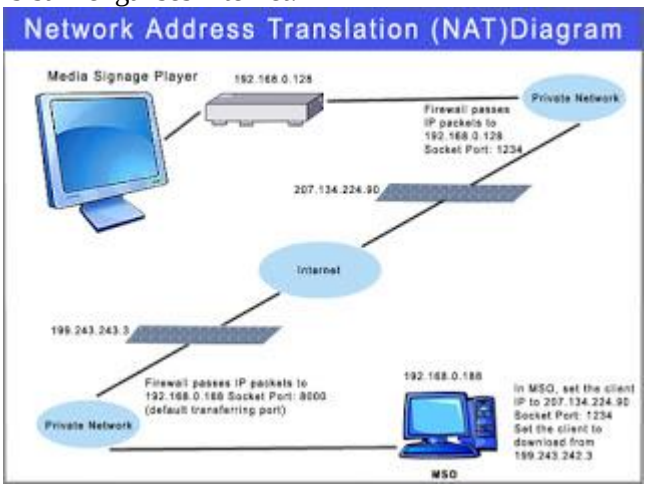
Dalam prosesnya, network layer menggunakan protocol yang mendukung pengalamatan secara hierarkis, dimana protocol tersebut mengijinkan adanya alamat unik dan batasan wilayah, serta metode untuk melakukan pemilihan jalur di saat sebuah data ingin berhubungan dengan jaringan lain.

3. Pertemuan 3

3.1. Network address translation

NAT (Network Address Translation) adalah adalah sebuah proses pemetaan alamat IP dimana perangkat jaringan komputer akan memberikan alamat IP public ke perangkat jaringan local sehingga banyak IP private yang dapat mengakses IP public.

Dengan kata lain NAT akan mentranslasikan alamat IP sehingga IP address pada jaringan local dapat mengakses IP public pada jaringan WAN. NAT mentranslasikan alamat IP private untuk dapat mengakses alamat host diinternat dengan menggunakan alamat IP public pada jaringan tersebut. Tanpa hal tersebut(NAT) tidaka mungkin IP private pada jaringan local bisa mengakses internet.



Apa Fungsi dari NAT (Network Address Translation) pada jaringan komputer?

NAT (Network Address Translation) pada jaringan komputer berfungsi sebagai translasi alamat IP public ke alamat IP private atau sebaliknya sehingga dengan adanya NAT ini setiap komputer pada jaringan LAN dapat mengakses internet dengan mudah.

Kita tahu bahwa alamat IP Public didunia ini sudah semakin menipis sehingga penggunaan dati NAT ini dirasa sangatlah efisien dan efektif terutama dalam alokasi alamat IP.

Jenis - jenis dari NAT (Network Address Translation)

Pada jaringan komputer terdapat 2 jenis NAT, diantaranya:
Dnat atau Destiantion Network Address Translation adalah sebuah NAT yang berfungsi untuk meneruskan paket dari IP public melalui firewall ke suatu host dalam jaringan. Dnat hanya bekerja pada tabel nat dan didalam tabel NAT berisi 3 bagian yang disebut dengan CHAIN, ketiga CHAIN tersebut meliputi prerouting, postrouting dan output.
SNAT atau Source Network Address Translation yaitu sebuah NAT yang bertugas untuk merubah source address dari suatu paket data. SNAT hanya berlaku pada postrouting.
Baca Juga: Pengertian dan Fungsi Proxy pada Jaringan Komputer

Kelebihan dan Kelemahan NAT (Network Address Translation)
Sebuah sistem tentunya akan memiliki kelebihan dan kelemahan, sehingga dengan memahami kelebihan dan kelemahan dan sistem tersebut kita bisa tahu kenapa kita harus menggunakan atau tidak menggunakannya, Berikut adalah kelebihan dan kelemahan menggunakan NAT pada jaringan:

Kelebihan dari NAT (Network Address Translation)
Dengan adanya NAT dapat mengurangi adanya duplikasi IP address pada jaringan atau biasanya dikenal dengan conflict IP Address
Dengan adanya NAT akan menghindari pengalamatan ulang pada saat jaringan tersebut berubah.
Dapat menghemat IP Legal yang diberikan oleh ISP (Internet Service Provider)
Dapat meningkatkan fleksibelitas untuk koneksi jaringan internet.
Kelemahan dari NAT (Network Address Translation)

NAT dapat menyebabkan keterlambatan proses, ini disebabkan karena data yang dikirim harus melalui perangkat NAT terlebih dahulu.
NAT dapat menyebabkan beberapa aplikasi yang tidak bisa berjalan dengan normal
Dengan adanya NAT dapat menghilangkan kemampuan untuk melacak data karena data tersebut akan melewati firewall.
Baca Juga: Pengertian dan Fungsi VPN (Virtual Private Network)

Cara Kerja NAT (Network Address Translation) pada Jaringan Komputer

NAT mempunyai fungsi yaitu sebagai translasi sebuah IP address, sehingga dengan adanya NAT ini IP address private dapat dengan mudah mengakses alamat IP public. Berikut adalah cara kerja dari NAT:
>Didalam IP address terdapat sebuah bagian yang mana di dalam IP tersebut terdapat informasi-informasi berupa alamat asal, alamat tujuan, TTL, dll. Bagian ini disebut dengan header.
>Sebagai contoh adalah sebuah komputer client dengan IP 192.168.1.2 akan mengakses atau melakukan request ke alamat www.google.co.id dengan IP 216.239.61.104, maka proses yang akan terjadi adalah sebagai berikut :
Pada header, informasi yang tersimpan antara lain alamat asal > 192.168.1.2
Sehingga ketika paket telah sampai pada router (gateway dari client), maka isi dari header akan dirubah menjadi : alamat asal > 192.168.1.1
>Sebelum paket keluar (menuju internet), maka header tersebut akan kembali berubah menjadi, alamat asal > 200.100.50.2, demikian seterusnya.
>Proses di atas merupakan mekanisme dari SNAT (source NAT), dimana IP asal (komputer client) akan dirubah disesuaikan dengan IP ketika paket telah berpindah. Ketika server google melakukan response / balasan, maka akan terjadi DNAT (destination NAT), dimana IP tujuan akan berubah

disesuaikan dengan tujuan paket (komputer client). Prosesnya adalah sebagai berikut :

Pada header, ketika paket telah sampai pada Router, informasi IP tujuan >200.100.50.20

Ketika paket berada pada gateway, IP tujuan >192.168.1.1

Di sini header akan kembali mengalami perubahan, IP tujuan > 192.168.1.2

Sehingga Paket dapat dikirim dan bisa sampai pada komputer client.

3.2. Port Address Translation

Port Address Translation (PAT)

Port Address Translation (PAT) adalah suatu fitur dari sebuah jaringan perangkat yang menerjemahkan TCP atau UDP komunikasi yang dibuat antara host di jaringan pribadi dan host pada jaringan publik.. Hal ini memungkinkan sebuah masyarakat tunggal alamat IP untuk digunakan oleh banyak host pada jaringan pribadi, yang biasanya Local Area Network atau LAN. Perangkat PAT transparan memodifikasi IP paket saat mereka melewatinya. Modifikasi membuat semua paket yang mengirim ke jaringan publik dari beberapa host di jaringan pribadi tampaknya berasal dari satu host , (perangkat PAT) pada jaringan publik.

Hubungan antara NAT dan PAT

PAT adalah himpunan bagian dari NAT, dan erat terkait dengan konsep Network Address Translation . Dalam PAT ada umumnya hanya satu alamat IP publik yang terbuka dan menghubungkan beberapa host swasta melalui alamat terkena. Masuk paket dari jaringan publik diarahkan ke tujuan mereka di jaringan pribadi dengan mengacu pada meja yang diselenggarakan dalam perangkat PAT yang melacak pasangan pelabuhan umum dan swasta.

Dalam PAT, baik pengirim pribadi IP dan nomor port yang diubah; perangkat PAT memilih nomor port yang akan dilihat oleh host di jaringan publik. Dengan cara ini, PAT beroperasi pada lapisan 3 (jaringan) dan 4 (transportasi) dari model OSI , sedangkan NAT dasar hanya beroperasi pada lapisan 3.

Pelaksanaan PAT

Membangun Komunikasi Dua Arah

Setiap paket TCP dan UDP berisi sumber alamat IP dan nomor port sumber serta tujuan alamat IP dan nomor port tujuan. Alamat port / bentuk pasangan alamat IP sebuah socket yaitu alamat port sumber dan bentuk alamat IP sumber sumber stopkontak.

Untuk layanan yang dapat diakses publik seperti server web dan mail server nomor port penting. Sebagai contoh, port 80 terhubung ke web server software dan port 25 untuk mail server's SMTP daemon . Alamat IP dari server publik juga penting, serupa dalam keunikan global ke alamat pos atau nomor telepon. Kedua alamat IP dan port harus benar dikenal oleh semua host yang ingin berhasil berkomunikasi.

Swasta alamat IP seperti yang dijelaskan di RFC 1918 yang signifikan hanya pada jaringan pribadi di mana mereka digunakan, yang juga berlaku untuk port host. Port endpoints unik komunikasi pada host, sehingga koneksi melalui perangkat PAT dipertahankan oleh gabungan pemetaan port dan alamat IP.

PAT menyelesaikan konflik yang akan timbul melalui dua host yang berbeda menggunakan sumber nomor port yang sama untuk membangun hubungan yang unik pada saat yang sama.

Terjemahan dari Endpoint

Dengan PAT, komunikasi semua dikirim ke host eksternal benar-benar berisi alamat IP eksternal dan informasi port perangkat PAT bukannya IP internal host atau nomor port.

- Ketika komputer pada pribadi (internal) jaringan mengirimkan paket ke jaringan eksternal, perangkat PAT menggantikan alamat IP internal dalam bidang sumber header paket (alamat pengirim) dengan alamat IP eksternal dari perangkat PAT. Kemudian memberikan sambungan nomor port dari kolam pelabuhan yang tersedia, memasukkan nomor port ini di bidang port sumber (seperti kotak nomor kantor pos), dan meneruskan paket ke jaringan eksternal. Perangkat PAT kemudian membuat entri dalam tabel terjemahan berisi alamat IP internal, port sumber asli, dan port

sumber diterjemahkan. Setelah paket dari koneksi yang sama diterjemahkan ke nomor port yang sama.

- Komputer menerima paket yang telah mengalami PAT mengadakan sambungan ke port dan alamat IP yang ditetapkan dalam paket diubah, tidak menyadari fakta bahwa alamat yang diberikan adalah yang diterjemahkan (analog dengan menggunakan nomor kotak kantor pos).
- Sebuah paket yang datang dari jaringan eksternal dipetakan ke alamat IP internal yang sesuai dan nomor port dari tabel terjemahan, menggantikan alamat IP eksternal dan nomor port pada header paket yang datang (mirip dengan terjemahan dari kotak pos nomor alamat jalan) . paket tersebut kemudian diteruskan melalui jaringan di dalamnya. Jika tidak, jika jumlah port tujuan paket yang masuk tidak ditemukan pada tabel terjemahan, paket akan dibuang atau ditolak karena perangkat PAT tidak tahu di mana untuk mengirimnya.

PAT hanya akan menterjemahkan alamat IP dan port dari host internal, menyembunyikan titik akhir sebenarnya dari sebuah host pada jaringan internal pribadi.

Operasi Visibilitas

Operasi PAT biasanya transparan bagi kedua penghuni internal dan eksternal.

Biasanya host internal menyadari benar alamat IP dan port TCP atau UDP pada host eksternal. Biasanya perangkat PAT dapat berfungsi sebagai gateway default untuk host internal. Namun tuan rumah eksternal hanya menyadari alamat IP publik untuk perangkat PAT dan port tertentu yang sedang digunakan untuk berkomunikasi atas nama host internal tertentu.

PAT

Software firewall dan broadband perangkat akses jaringan (misalnya ADSL router) adalah contoh-contoh teknologi jaringan yang mungkin mengandung implementasi PAT. Ketika mengkonfigurasi perangkat tersebut, jaringan eksternal adalah internet dan jaringan internal adalah LAN .

Contoh PAT

Sebuah host pada alamat IP 192.168.0.2 pada jaringan pribadi dapat meminta untuk koneksi ke host remote pada jaringan publik. Paket awal diberikan alamat 192.168.0.2:15345. Perangkat PAT (yang kita asumsikan memiliki IP publik 1.2.3.4) sewenang-wenang dapat menerjemahkan alamat sumber: sepasang port untuk 1.2.3.4:16529, membuat sebuah entri dalam tabel internal port 16529 yang digunakan untuk koneksi dengan 192,168. 0,2 pada jaringan pribadi. Ketika sebuah paket diterima dari jaringan publik dengan perangkat PAT untuk alamat 1.2.3.4:16529 paket diteruskan ke 192.168.0.2:15345.

Keuntungan dari PAT

In keuntungan yang disediakan oleh NAT:

- PAT memungkinkan host beberapa internal untuk berbagi alamat IP eksternal tunggal.

Kekurangan PAT

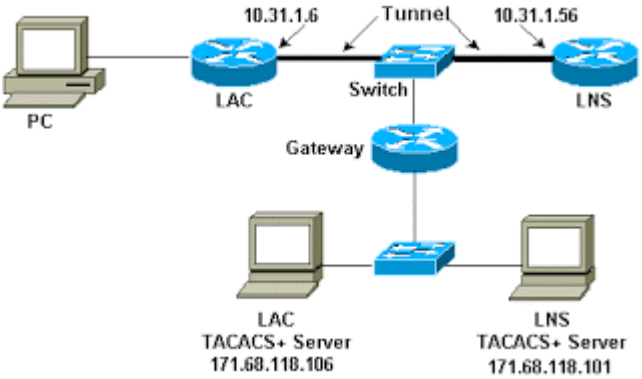
- Skalabilitas - Banyak host di jaringan swasta membuat banyak koneksi ke jaringan publik. Karena hanya ada sejumlah port yang tersedia, perangkat PAT akhirnya mungkin tidak cukup ruang dalam tabel penerjemahan. Walaupun ada ribuan port yang tersedia, dan mereka daur ulang dengan cepat, beberapa jaringan komunikasi mengkonsumsi beberapa port hampir bersamaan dalam transaksi logis tunggal (sebuah HTTP permintaan untuk halaman web dengan obyek tertanam banyak; beberapa VoIP aplikasi). Cukup-besar LAN yang sering mempertahankan jenis lalu lintas secara berkala bisa mengkonsumsi semua port yang tersedia.
- kompleksitas Firewall - Karena alamat di dalam semua disamarkan di belakang satu alamat yang dapat diakses publik, adalah mustahil untuk mesin di luar untuk memulai sambungan ke dalam mesin tertentu tanpa konfigurasi khusus pada firewall

untuk koneksi ke depan ke port tertentu. Ini memiliki dampak yang cukup besar pada aplikasi seperti VOIP, video conference, dan lainnya peer-to-peer aplikasi.

4. Pertemuan 4

4.1. Point to Point Protocol

Network - Point-to-Point Protocol (sering disingkat menjadi PPP) adalah sebuah protokol enkapsulasi paket jaringan yang banyak digunakan pada wide area network (WAN). Protokol ini merupakan standar industri yang berjalan pada lapisan data-link (layer 2) dan dikembangkan pada awal tahun 1990-an sebagai respons terhadap masalah-masalah yang terjadi pada protokol Serial Line Internet Protocol (SLIP), yang hanya mendukung pengalamatan IP statis kepada para kliennya. Dibandingkan dengan pendahulunya (SLIP), PPP jauh lebih baik, mengingat kerja protokol ini lebih cepat, menawarkan koreksi kesalahan, dan negosiasi sesi secara dinamis tanpa adanya intervensi dari pengguna. Selain itu, protokol ini juga mendukung banyak protokol-protokol jaringan secara simultan.



PPP Komponen dan Fitur

PPP menyediakan metode untuk transmisi datagram lebih link point-to-point serial. PPP terdiri dari tiga komponen utama:
Sebuah metode untuk encapsulating datagrams atas link serial.

PPP menggunakan Tingkat Tinggi Data Link Control (HDLC) protokol sebagai dasar untuk encapsulating datagrams lebih link point-to-point.
Sebuah LCP extensible untuk membangun, mengkonfigurasi, dan menguji koneksi data link.
Sebuah keluarga NCPs untuk menetapkan dan mengkonfigurasi protokol jaringan lapisan yang berbeda.
PPP protocol beroperasi melalui koneksi interface piranti Data Communication Equipment (DCE) dan piranti Data Terminal Equipment (DTE).
PPP protocol dapat beroperasi pada kedua modus synchronous (dial-up) ataupun asynchronous dan ISDN.
Tidak ada batas transmission rate
Keseimbangan load melalui multi-link
LCP dipertukarkan saat link dibangun untuk mengetest jalur dan setuju karenanya
PPP protocol mendukung berbagai macam protocol layer diatasnya seperti IP; IPX; AppleTalk dan sebagainya.
PPP protocol mendukung authentication kedua jenis clear text PAP (Password Authentication Protocol) dan enkripsi CHAP (Chalange Handshake Authentication Protocol)
NCP meng-encapsulate protocol layer Network dan mengandung suatu field yang mengindikasikan protocol layer atas
PPP mengandung Header yang mengindikasikan pemakaian protocol layer Network.PPP protocol Link Control Protocol (LCP) merupakan satu set layanan yang melaksanakan setup link dan memiliki Fase sebagai berikut :
Link Entablisment and Negotiation, mencoba untuk membentuk link dengan router lawan (pembentukan link) request link dan router tetangga mengirim acnowlegment dengan isi [setuju atau tidak]. Pada fase ini akan menawarkan opsi :
Authentication, mengirim dalam persetujuan PAP atau CHAP
Compression, setiap mengirim dalam bentuk di kompres atau tidak
Multilink, dalam satu interface dalpat membuat beberapa virtual link

Determination Link Qualitiy, menentukan kualitas linknya (optional)
NCP (Network Control Protocol) berfungsi mengontrol establisment

PPP protocol dapat berjalan pada bermacam-macam standard physical synchronous dan asynckronous termasuk :
Serial Asynchronous seperti dial-up
ISDN
Serial synchronous
HIgh Speed Serial Interface (HSSI)

Konfigurasi PPP protocol

Default protocol point-to-point untuk router Cisco adalah HDLC (High-Level Data Link Control) yang mana umum dipakai pada leased line seperti T1; T3 dll, akan tetapi HDLC tidak support authentication. KDLC adalah patennya Cisco jadi bukan standard industri, jadi hanya bisa dipakai sesama Cisco saja.

Berikut ini adalah implementasi PPP protocol :

Router# configure terminal
Router(config)# interface serial 0
Router(config-if) # encapsulation ppp
Router(config-if) # exit

PPP protocol diinisialisasi dan di enable pada interface serial 0. Langkah selanjutnya adalah men-set jenis authentication yang dipakai

Router(config) # int s0
Router(config-if) # ppp authentication pap
Or you can use the CHAP authentication method.
Router(config-if) # ppp authentication chap
Router # show int s0

CHAP direkomendasikan sebagai metoda authentication PPP protocol, yang memberikan suatu authentication terenkripsi dua arah yang mana lebih secure daripada PAP. Jika jalur sudah tersambung, kedua server di masing-masing ujung saling mengirim pesan ‘Challenge’. Segera setelah pesan ‘Challenge’ terkirim, sisi remote yang diujung akan merespon dengan fungsi ‘hash’ satu arah menggunakan Message Digest 5 (MD5) dengan memanfaatkan user dan password mesin local. Kedua sisi ujung router harus mempunyai konfigurasi yang sama dalam hal PPP protocol ini termasuk metoda authentication yang dipakai.

```
Router(config)# username router password cisco
Router(config)# interface serial 0
Router(config-if)# encapsulation ppp
Router(config-if)# ppp chap hostname router
Router(config-if)# ppp authentication chap
```

PPP protocol - CHAP authenticating :

- Konfigurasi kedua router dengan username dan password
- Username yang dipakai adalah hostname dari router remote
- Password yang dikonfigurasikan harus sama

4.2. DDR

Dalam komputer, Dial-on-demand routing (DDR) adalah suatu teknik di mana sebuah host atau router akan secara otomatis melakukan koneksi dial-up melalui ISDN atau biasa jaringan telepon diaktifkan publik line ketika akses jaringan diperlukan, dan menutup koneksi ketika tidak ada lebih banyak data perlu dikirim atau diterima. Garis hanya akan digunakan bila diperlukan, yang mengurangi biaya dimana circuit-switched (telepon) koneksi ditagih oleh menit.

DDR biasanya digunakan oleh pengguna PC rumahan ketika komputer secara otomatis akan memanggil ke penyedia layanan

Internet kapan permintaan program TCP / IP koneksi. Lebih maju mungkin fitur setup sebuah router yang dibentuk untuk menyediakan fungsi yang sama untuk seluruh jaringan komputer. Dalam situasi lain, router mungkin dikonfigurasi untuk menggunakan saluran dial-out untuk koneksi cadangan jika jalur utama komunikasi entah bagaimana telah diputus.

Perawatan harus diambil untuk memastikan paket hanya relevan menyebabkan sambungan harus dibentuk. Untuk tujuan ini, router DDR biasanya memiliki daftar penyaring khusus diterapkan pada permintaan-fungsi panggilan, misalnya satu yang mencegah paket-paket broadcast dari sambungan memicu proses. Beberapa jaringan, e.g. IPX, memerlukan tambahan teknik spoofing protokol yang akan digunakan untuk mengakomodasi lalu lintas secara berkala tetapi wajib.

4.3. ISDN

1 . PENGERTIAN ISDN

ISDN (Integrated Services Digital Network) adalah suatu sistem telekomunikasi di mana layanan antara data, suara, dan gambar diintegrasikan ke dalam suatu jaringan, yang menyediakan konektivitas digital ujung ke ujung untuk menunjang suatu ruang lingkup pelayanan yang luas.

ISDN diprakarsai oleh H. Shimada pada suatu pertemuan CCITT tahun 1971. Kemudian, aplikasi ISDN segera terwujud setelah CCITT merekomendasikan standar Red Book (1985) dan standar Blue Book (1988) dalam wujud Narrow Band (N-ISDN).

2 . KOMPONEN / alat dalam ISDN

Sistem ISDN terdiri dari lima buah komponen terminal utama yang bertugas untuk menjalankan proses layanannya, yaitu terminal

Equipment, terminal Adapter , Network Termination, Line Termination, dan Local Exchange.

v TE1 : Terminal dg kemampuan protokol yang relevan dengan interface pada titik referensi S & T dan dapat dihubungkan langsung ke sistem passive bus NT.

Contoh : Telepon ISDN; Video phone.

v TE2 : Terminal yg tidak dilengkapi dengan protokol ISDN dan hanya dapat dihubungkan ke NT dengan bantuan terminal adapter.

Contoh : Telepon konvensional (terminal a/b) Terminal X- 25.

v NT1 : Menyediakan fungsi-fungsi yg ekivalen dg fungsi layer 1 model OSI, memastikan bahwa TE secara pisik & elektrik sesuai dengan jaringan akses sentralisasi pemeliharaan.

Contoh : titikterminasi fisik 2 kawat ke 4 kawat.

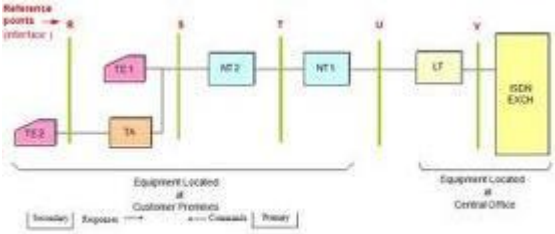
v NT2 : Menyediakan fungsi-fungsi yg ekivalen dengan layer 2 dan layer di atasnya.

Contoh : PABX; LAN

v LT : Titik terminasi antara jaringan akses dengan sentral ISDN. LT dapat membentuk fungsi-fungsi seperti NT, test loop, pembangkitan sinyal dan konversi kode.

v ET : Titik terminasi jaringan akses dg sentral ISDN dimana sinyal kontrol diproses,di mana data informasi dan data pensinyalan diproses. Juga bertugas untuk menangani data link layer protokol DSS 1, data yg diterima diubah kedalam format lain misal SS7 sebelum dikirim keluar ET.

v TA : Perangkat interface terminal non- ISDN, agar TE2 bisa mengakses ke ISDN.



Gambar . Model Referensi ISDN

ISDN menspesifikasikan sejumlah point reference yang mendefinisikan logical interface antara kelompok-kelompok fungsional, seperti TA dan NT. Point-point reference tersebut adalah sebagai berikut :

- R : Point reference antara perangkat non-ISDN dan TA
- S : Point reference antara terminal pemakai dengan NT2
- T : Point reference antara perangkat NT2 dengan NT1

- U : Point reference antara perangkat NT1 dengan LTE

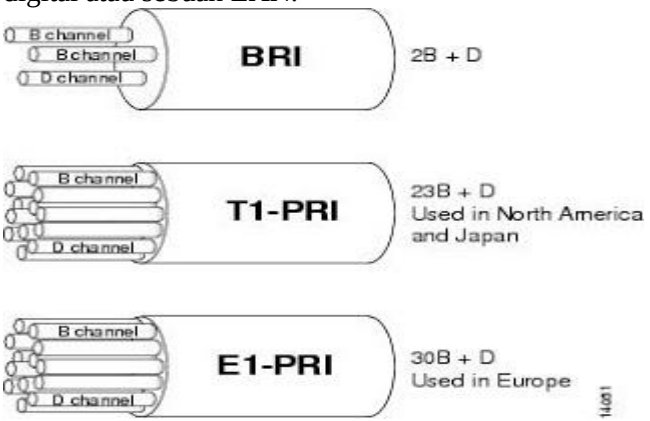
3 . METODE AKSES ISDN

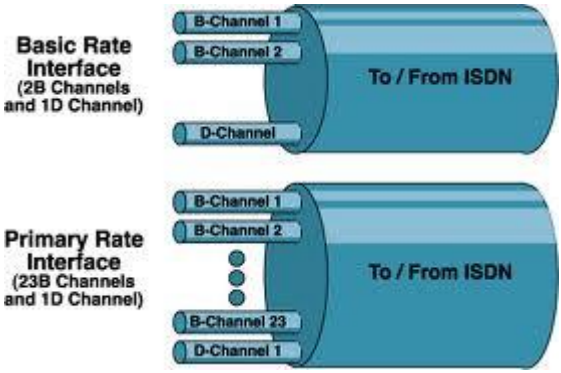
Di dalam ISDN terdapat dua jenis pelayanan, yaitu:

v Basic Rate Interface (BRI) Terdiri dari 2B + D kanal. Yang mewakili 2 Bearer kanal dengan masing-masing 64 kbps untuk data dan 1 kanal D dengan 16 kbps untuk handshaking dan kontrol. Kanal pemisah untuk handshaking dan kontrol disebut sinyal “out of band”. Kanal 2B dapat ditahan bersama-sama untuk sebuah kanal data tunggal dengan transfer rate 128 kbps. Servis utamanya didasarkan pada keperluan-keperluan individual user, termasuk pelanggan perumahan maupun kantor-kantor kecil.

v Primary Rate Interface (PRI) Terdiri dari 23B + D kanal. Yang mewakili 23 Bearer dengan masing-masing 64 kbps untuk data dan 1 kanal D dengan 64 kbps untuk handshaking dan kontrol. Kanal Bearer dapat ditahan pada beberapa kombinasi yang diperlukan.

Ditujukan untuk user-user user-user yang dengan keperluan kapasitas yang lebih besar, seperti kantor yang memiliki PBX digital atau sebuah LAN.





4 . MENGAKSES ISDN

Akses Broadcast-ISDN muncul akibat dari usaha Jerman melengkapi perumahan dan perkantoran. Ada dua cara untuk memperbesar kapasitas pengiriman data lewat ISDN.

SDH, yaitu alat untuk beban 150 Mbps dengan pelayanan yang berbeda dari laju data yang bervariasi

ATM, yaitu pengembangan penyambungan paket yang memakai ukuran paket yang sama yang diesebut dengan istilah sel

Pelayanan Broadcast ISDN hampir mirip dengan pelayanan ISDN, yaitu mempunyai:.

Bearer Service, yaitu pemberian kanal informasi melalui pita lebar tertentu

TeleService, yaitu pengembangan dari jenis layanan yang pertama, yang bertumpu pada kemampuan switch dan CPE. TeleService dibagi menjadi dua kelompok besar yaitu Pelayanan Interaktif (mencakup Conversational, Message, dan Retrieval Service), dan Pelayanan Distributif (mencakup distribusi dengan kemampuan kontrol penerimaan dan tanpa kemampuan kontrol penerimaan)

Para pemakai ISDN diberikan keuntungan berupa fleksibilitas dan penghematan biaya, karena biaya untuk sistem yang terintegrasi ini akan jauh lebih murah apabila menggunakan sistem yang terpisah.

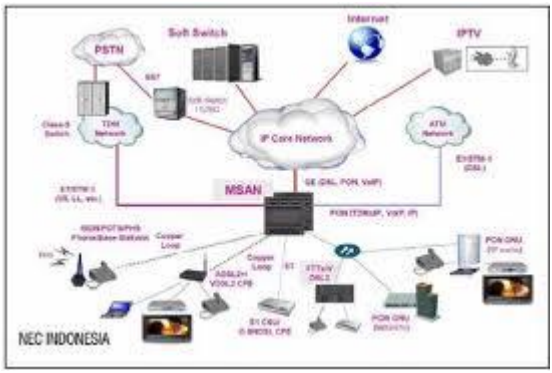
Para pemakai juga memiliki akses standar melalui satu set interface pemakai jaringan multiguna standar.

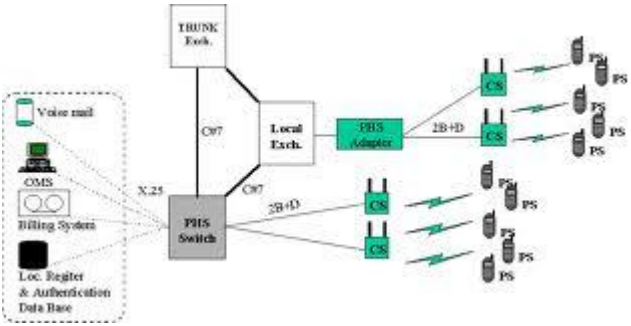
ISDN merupakan sebuah bentuk evolusi telepon local loop yang memepertimbangkan jaringan telepon sebagai jaringan terbesar di dunia telekomunikasi.

5 . Pembentukan awal ISDN

Jaringan-jaringan konvensional (PSTN, PDN , PSTX) digabungkan menjadi jaringan digital yang terintegrasi dengan cara mendigitalisasi jaringan konvensional tersebut, kemudian jaringan-jaringan yang telah memenuhi konsep Integrated Digital Network diintegrasikan sehingga pada akhirnya kita dapat mengintegrasikan semua jaringan konvensional ini menjadi sebuah jaringan terpadu yang memiliki konsep digital sampai ke pengguna akhir. Awalnya, telepon jaringan menggunakan kawat atau kabel untuk sarana koneksinya.

Namun pada permulaan tahun 1960-an, sistem telepon ini mulai dikonversi dari sistem analog menggunakan kabel, ke sambungan paket sistem digital. Asal mula munculnya ISDN pita lebar bermula ketika pembuatan trial broadband rampung pada jaringan lokal Bigfon di Berlin pada tahun 1984 hingga kemudian pada tahun yang sama penggunaaan ISDN mulai disosialisasikan ke masyarakat. Sosialisasi ini dimulai oleh CCITT (sekarang ITU), yaitu sebuah organisasi dibawah naungan PBB yang menangani bidang standarisasi telekomunikasi.





6 . Cara menggunakan ISDN

Layanan ISDN di Indonesia .
Aplikasi layanan ISDN di Indonesia disediakan oleh PT Telkom .
Direct Dialling In = Telepon yang tersambung ke jaringan PSTN/ISDN dapat secara langsung memanggil pesawat cabang STLO.
Call Diversion = Pelanggan yang tidak dapat menerima panggilan dapat mengalihkan panggilannya ke nomor lain atau ke layanan penjawab(answeringservice)
Do Not Disturb = Pelanggan yang memang sengaja tidak ingin menerima panggilan untuk suatu periode waktu tertentu dapat mengalihkan panggilannya ke nomor lain.
PBX Line Hunting Service = Seleksi otomatis dari suatu bundel saluran yang melayani pelanggan ke nomor direktori umum pelanggan tersebut.
Three Party Service = Pelanggan yang sedang melakukan percakapan telepon dapat menahan percakapannya dan melakukan panggilan dengan pihak ketiga.
Freephone = Sebuah nomor khusus dapat dialokasikan kepada pelanggan dan beban atas setiap panggilan yang dilakukan kepada nomor ini biayanya dibebankan kepada pelanggan, bukan kepada pihak yang memanggil.
Speed Dialling = Pelanggan dapat melakukan panggilan hanya dengan memutar suatu kode singkat atas

sebuah nomor tertentu yang sudah diset dan tidak perlu memutar seluruh nomor lengkap.

Call Waiting = Pelanggan yang sedang melakukan percakapan diberikan tanda bahwa ada panggilan masuk lainnya.

Centrex Service = Layanan ini umunya hanya terdpat pada PABX dengan menggunakan sentral telepon PSTN/IDN yang diperlengkap secarakhusus.

Malicious Call Identification = Pelanggan dapat meminta identifikasi panggilan yang diterimanya.

5. Pertemuan 5

5.1. Integrity

Integrity atau Integritas adalah pencegahan terhadap kemungkinan amandemen atau penghapusan informasi oleh mereka yang tidak berhak. Secara umum maka integritas ini berarti bahwa informasi yang tepat, memang tepat dimana-mana dalam sistem – atau mengikuti istilah “messaging” – tidak terjadi cacad maupun terhapus dalam perjalananya dari penyaji kepada para penerima yang berhak.

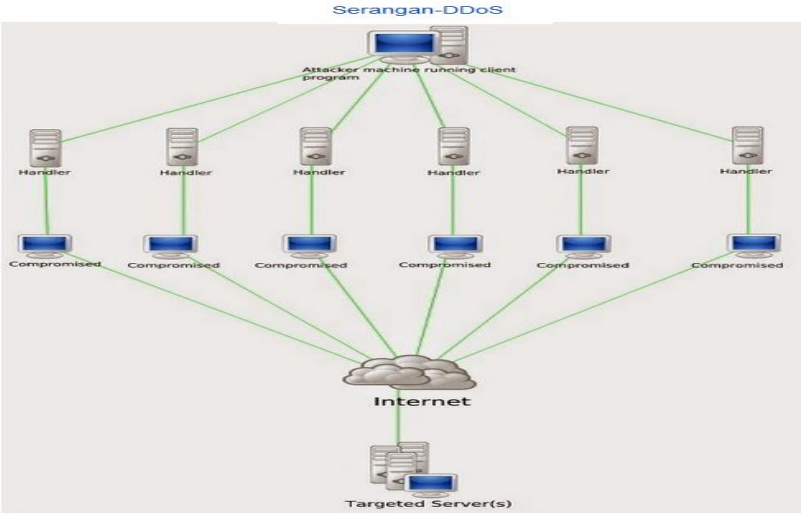
5.2. Confidentiality

Confidentiality atau kerahasiaan adalah pencegahan bagi mereka yang tidak berkepen-tingan dapat mencapai informasi . Secara umum dapat disebutkan bahwa kerahasiaan mengandung makna bahwa informasi yang tepat terakses oleh mereka yang berhak (dan bukan orang lain), sama analoginya dengan e-mail maupun data-data perdagangan dari perusahaan.

5.3. Denial of service

Denial Of Service Attack (DoS Attack) adalah jenis serangan terhadap sebuah komputer atau server di dalam jaringan internet dengan cara menghabiskan sumber (resource) yang dimiliki oleh komputer tersebut sampai komputer tersebut tidak dapat menjalankan fungsinya dengan benar sehingga secara tidak langsung mencegah pengguna lain untuk memperoleh akses layanan dari komputer yang diserang tersebut.

Cara kerja DoS (Denial Of Service Attack)



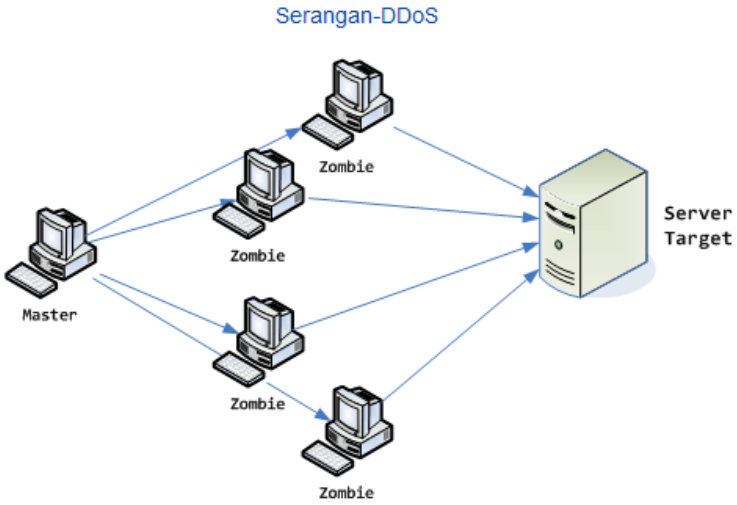
Dalam sebuah serangan Denial of Service Attack, si penyerang akan mencoba untuk mencegah akses seorang pengguna terhadap sistem atau jaringan dengan menggunakan beberapa cara, yakni sebagai berikut:

1. Membanjiri lalu lintas jaringan dengan banyak data sehingga lalu lintas jaringan yang datang dari pengguna yang terdaftar menjadi tidak dapat masuk ke dalam sistem jaringan. Teknik ini disebut sebagai traffic flooding.
2. Membanjiri jaringan dengan banyak request (permintaan) terhadap sebuah layanan jaringan yang disedakan oleh sebuah host sehingga request yang datang dari pengguna terdaftar tidak dapat dilayani oleh layanan tersebut. Teknik ini disebut sebagai request flooding.
3. Mengganggu komunikasi antara sebuah host dan kliennya yang terdaftar dengan menggunakan banyak cara, termasuk dengan mengubah informasi konfigurasi sistem atau bahkan perusakan fisik terhadap komponen dan server.

Penolakan Layanan secara Terdistribusi (Distributed Denial of Service (Ddos)) adalah salah satu jenis serangan Denial of Service Attack yang menggunakan banyak host penyerang (baik itu menggunakan komputer yang didedikasikan untuk melakukan penyerangan atau komputer yang dipaksa menjadi zombie) untuk menyerang satu buah host target dalam sebuah jaringan.

Serangan Denial of Service Attack bersifat “satu lawan satu”, sehingga dibutuhkan sebuah host yang kuat (baik itu dari kekuatan pemrosesan atau sistem operasinya) demi membanjiri lalu lintas host target sehingga mencegah klien yang valid untuk mengakses layanan jaringan pada server yang dijadikan target serangan. Sedangkan serangan DdoS menggunakan teknik yang lebih canggih dibandingkan dengan serangan Denial of Service, yakni dengan meningkatkan serangan beberapa kali dengan menggunakan beberapa buah komputer sekaligus, sehingga dapat mengakibatkan server atau keseluruhan segmen jaringan dapat menjadi tidak berguna sama sekali bagi klien.

Cara kerja Ddos (Distributed Denial Of Service Attack)



5.4. Authentication

Autentikasi adalah suatu langkah untuk menentukan atau mengonfirmasi bahwa seseorang (atau sesuatu) adalah autentik atau asli. Melakukan autentikasi terhadap sebuah objek adalah melakukan konfirmasi terhadap kebenarannya. Sedangkan melakukan autentikasi terhadap seseorang biasanya adalah untuk memverifikasi identitasnya. Pada suatu sistem komputer, autentikasi biasanya terjadi pada saat login atau permintaan akses.

5.5. Secure Socket Layer dan Firewall

A. SSL

SSL adalah kependekan dari Secure Socket Layer yang merupakan suatu protocol layer transport yang digunakan dalam koneksi internet secara aman. Jika anda menginginkan suatu koneksi komunikasi lewat internet dengan cara yang secure, maka gunakan koneksi SSL.
SSL menawarkan tiga tingkat keamanan, yaitu:

Authentication: Memastikan bahwa message yang diterima berasal dari seseorang yang tersurat
Confidentiality: Melindungi pesan dari suatu usaha pembacaan oleh penerima yang tidak berhak disepanjang perjalanannya.
Integrity: Memastikan bahwa pesan asli, tidak mengalami perubahan dalam perjalanannya.
SSL dikembangkan oleh Netscape Communications agar bisa mengirim data secara aman lewat internet. Jika anda pernah memperhatikan di browser internet dengan menggunakan HTTPS, maka koneksi internet ini adalah menggunakan SSL yang umum digunakan pada suatu transaksi online. Jadi HTTPS adalah suatu protocol untuk melakukan transfer data yang terinkripsi melalui web.

Apa bedanya HTTPS dan HTTP:
HTTPS melakukan koneksi melalui port 443, sementara HTTP menggunakan port 80

HTTPS mengirim / menerima data dengan inkripsi lewat protocol SSL, sementara HTTP mengirim data dengan plain text
Jadi dalam transaksi online, maka pastikan anda melihat online store anda menggunakan HTTPS dalam bertransaksi keuangan lewat internet.

Jika anda mempunyai website, apa yang diperlukan agar bisa di host disuatu host yang bisa SSL.

Web server haruslah support inkripsi SSL
IP address public yang unik agar penyedia certificate SSL bisa melakukan validasi website anda
Suatu certificate SSL dari penyedia layanan SSL
Dua yang pertama bisa anda dapatkan dari ISP anda, hubungi ISP anda untuk memastikannya.

SSL beroperasi pada antara layer Application dan Transport pada model OSI. SSL tidak bekerja secara transparent automatis, karena hanya bisa kalau memang protocol-protocol applikasi secara explicit memang diimplementasikan.

SSL menggunakan inkripsi public-key untuk maksud authentication dan inkripsi symmetric key untuk inkripsi informasi yang dikirim. Untuk public key inkripsi SSL menggunakan algoritma inkripsi Rivest-Shamir-Adleman (RSA), makanya bergantung pada implementasi dari infrastructure public key (PKI) yang didukung. Integritas pesan dijamin dengan cara mekanisme checking integritas yang disebut sebagai message authentication code (MAC).

B. Firewall
Firewall adalah sistem keamanan jaringan komputer yang digunakan untuk melindungi komputer dari beberapa jenis serangan dari komputer luar. Firewall merupakan suatu cara untuk memastikan bahwa data pada komputer atau server Web yang terhubung tidak akan bisa diakses siapa saja di

Internet. Pihak lain yang mengakses informasi pribadi atau mengubah situs Web anda akan di blokir oleh Firewall.

Firewall yaitu seperangkat program yang saling terhubung, yang beerada di server gateway jaringan, yang berfungsi untuk melindungi sumber daya dari jaringan pribadi dari pengguna dari jaringan lain. Dengan intranet suatu perusahaan memungkinkan pekerjanya mengakses ke Internet lebih luas menginstal firewall untuk mencegah orang luar mengakses sumber daya pribadi untuk mengendalikan data.

Firewall, pada dasarnya bekerja sama dengan program router yang memeriksa setiap paket jaringan supaya dapat menentukan apakah akan maju ke arah tujuannya. Firewall juga bekerja dengan proxy server yang membuat permintaan jaringan atas nama pengguna workstation. Komputer yang dirancang khusus terpisah dari sisa jaringan sering diinstal Firewall, sehingga tidak ada permintaan yang masuk bisa langsung pada sumber daya jaringan pribadi.

FUNGSI FIREWALL

Mengontrol dan mengawasi arus paket data yang mengalir di jaringan.
Firewall berfungsi juga dalam mengaturm memfilter dan mengontrol lalulintas data yang diizinkan untuk mengakses jaringan privat yang dilindungi. Beberapa kriteria yang dilakukan firewall apakah memperbolehkan paket data lewati atau tidak, antara lain :
Alamat IP dari komputer sumber
Port TCP/UDP sumber dari sumber.
Alamat IP dari komputer tujuan.
Port TCP/UDP tujuan data pada komputer tujuan
Informasi dari header yang disimpan dalam paket data.
Melakukan autentifikasi terhadap akses kejaringan.
Applikasi firewall mampu memeriksa lebih dari sekedar header dari paket data.

MANFAAT PENGGUNAAN FIREWALL

Menjaga informasi rahasia dan berharga yang menyelinap keluar tanpa sepengetahuan.
Sebagai filter yang digunakan untuk mencegah lalu lintas tertentu mengalir ke subnet jaringan.
Memodifikasi paket data yang data di firewall, proses tersebut Network Address Translation (NAT).
Sebagai Akurasi data seperti informasi keuangan, spesifikasi produk, harga produk dll.
CARA KERJA FIREWALL

Sistem firewall bekerja dengan cara menganalisis paket data yang keluar dan masuk ke dalam lingkungan aman yang dilindungi oleh sistem firewall tersebut. Paket data yang tidak lolos analisis akan ditolak untuk masuk ataupun keluar jaringan atau komputer yang dilindungi.
Penyaring atau filter firewall akan bekerja melakukan pemeriksaan sumber dari paket data yang masuk dengan kebijakan yang dibuat untuk mengontrol paket dari mana saja yang boleh masuk. Sistem juga dapat melakukan pemblokiran pada jenis jaringan tertentu serta melakukan pencatatan pada lalu lintas paket data yang mencurigakan.

6. Pertemuan 6

6.1. Protocol Attack

Spoofing adalah " Teknik yang digunakan untuk memperoleh akses yang tidak sah ke suatu komputer atau informasi, dimana penyerang berhubungan dengan pengguna dengan berpura-pura memalsukan bahwa mereka adalah host yang dapat dipercaya" hal ini biasanya dilakukan oleh seorang hacker/ cracker.

Macam-Macam Spoofing
IP-Spoofing adalah serangan teknis yang rumit yant terdiri dari beberapa komponen. Ini adalah eksploitasi keamanan yang bekerja dengan menipu komputer dalam hubungan kepercayaan bahwa anda adalah orang lain. Terdapat banyak makalah ditulis oleh daemon9, route, dan infinity di Volume Seven, Issue Fourty-Eight majalah Phrack.

DNS spoofing adalah mengambil nama DNS dari sistem lain dengan membahayakan domain name server suatu domain yang sah.

Identify Spoofing adalah suatu tindakan penyusupan dengan menggunakan identitas resmi secara ilegal. Dengan menggunakan identitas tersebut, penyusup akan dapat mengakses segala sesuatu dalam jaringan.

Contoh Web Spoofing

Web Spoofing melibatkan sebuah server web yang dimiliki penyerang yang diletakkan pada internet antara pengguna dengan WWW, sehingga akses ke web yang dituju pengguna akan melalui server penyerang. Cara seperti ini dikenal dengan sebutan "man in the middle attack" [2,5]. Hal ini dapat terjadi dengan beberapa jalan, tapi yang paling mungkin adalah :

- Akses ke situs web diarahkan melalui sebuah proxy server : ini disebut (HTTP) application proxy. Hal ini memberikan pengelolaan jaringan yang lebih baik untuk akses ke server. Ini merupakan teknik yang cukup baik yang digunakan pada banyak situs-situs di internet, akan tetapi teknik ini tidak mencegah Web Spoofing.
- Seseorang menaruh link yang palsu (yang sudah di-hack) pada halaman web yang populer.

Kita menggunakan browser mengakses sebuah Web. Semua yang ada pada NET (baik Internet maupun Intranet) direferensikan dengan Universal Resource Locator (URL). Pertama-tama penyerang harus menulis-ulang URL dari halaman web yang dituju sehingga mereka mengacu ke server yang dimiliki penyerang daripada ke server web yang sebenarnya. Misalnya, server penyerang terletak di www.attacker.com, maka penyerang akan menulis-ulang URL dengan menambahkan http://www.attacker.com didepan URL yang asli.

7. Pertemuan 7

8. **Pertemuan 8**
9. **Pertemuan 9**

9.1. Algoritma Routing (OSPF, RIP)

A. Routing Information Protocol (RIP)

Routing Information Protocol (RIP) adalah routing protocol yang sangat sederhana dan masuk dalam kategori Interior Gateway Protocol. RIP merupakan routing protocol dengan algoritma routing distance vector atau routing protocol yang hanya melihat arah dan jarak untuk menuju suatu jaringan tujuan. RIP tidak memiliki peta yang lengkap tentang jaringan yang ada. RIP menggunakan hop count sebagai metric dan link dengan hop count terkecil yang akan menjadi link terbaik (best path). Router-router yang menjalankan RIP akan saling bertukar informasi dengan router tetangganya (neighbor). Informasi yang akan dipertukarkan adalah tabel routing miliknya, dengan kata lain sebuah router akan mengirimkan atau meneruskan tabel routingnya kedalam neighbour router.

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.

A. Routing Information Protocol (RIP) Versi 1

RIPv1 merupakan routing protocol jenis classfull yang akan mengirimkan tabel routingnya secara broadcast. 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.

B. Routing Information Protocol (RIP) Versi 2

RIPv2 merupakan routing protocol jenis classless, akan mengirimkan tabel routingnya secara multicast dan memiliki fitur authentication. Karena kekurangan RIP asli spesifikasi, RIP versi 2 dikembangkan pada tahun 1993 dan standar terakhir pada tahun 1998. Ini termasuk kemampuan untuk membawa informasi subnet, sehingga mendukung Classless Inter-Domain Routing (CIDR). 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.

B. Protokol Routing OSPF (Open Shortest Path First)

Open Shortest Path First (OSPF) adalah salah satu protocol routing link-state yang dikembangkan sebagai pengganti distance vector routing protocol RIP. RIP adalah routing protocol yang cocok pada awal perkembangan jaringan dan internet. Tetapi ini tergantung pada hop count sebagai pengukuran dalam memilih rute terbaik dan tercepat, tapi kemudian ini tidak sesuai lagi seiring dengan bertambah luasnya jaringan yang memerlukan solusi routing yang sangat cepat. OSPF adalah classless routing protocol yang menggunakan konsep area untuk scalabilitas.RFC 2328 mendefinisikan OSPF metric sebagai nilai penentu yang biasa dikenal sebagai cost. CISCO IOS menggunakan bandwith sebagai OSPF cost metric.

Keuntungan utama OSPF dibandingkan RIP adalah OSPF dapat melakukan konvergensi yang cepat dan skalabilitas lebih luas untuk implementasi jaringan yang lebih besar.TIPE Paket OSPF

1. Hello – Paket hello digunakan untuk membangun dan memelihara adjacency dengan router OSPF lainnya.

2. DBD – Database Description (DBD) berisi daftar-daftar dari database link state router pengirim dan digunakan oleh router penerima untuk memeriksa dan dibandingkan dengan database link state local.

3. LSR – Receiving Routers kemudian bisa meminta informasi lebih lanjut tentang isi di dalam DBD dengan mengirim Link-State Request (LSR)

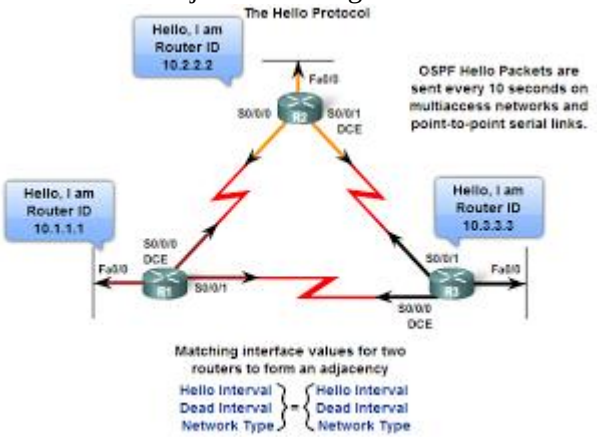
4. LSU – Link State Update (LSU) paket digunakan untuk mereply ke LSRs serta mengumumkan informasi baru. LSUs berisi tujuh jenis Link-State Advertisements (LSAs) yang berbeda.

5. LSAck – Ketika sebuah LSU diterima, router mengirim sebuah Link-state Acknowledgement(LSAck) sebagai konfirmasi penerimaan LSU.

Neighbor Establishment.

Sebelum sebuah router OSPF bisa menyebarkan link-state ke router yang lain, pertama kali router ini harus memastikan apakah ada OSPF neighbor lain pada setiap link di router ini. OSPF router mengirimkan paket Hello pada semua interface OSPF yang enabled untuk memeriksa apakah ada neighbor di link tersebut. Informasi dalam OSPF Hello mencakup OSPF Router ID dari router yang mengirimkan paket Hello tersebut. Penerima OSPF Hello paket kemudian mereply bahwa ada router OSPF lain pada link ini. OSPF kemudian membentuk adjacency dengan

neighbor ini. Sebagai contoh, dalam gambar berikut , R1 akan mendirikan adjacencies dengan R2 dan R3.



OSPF Hello dan Dead Intervals

Sebelum dua router dapat membentuk OSPF neighbor adjacency , mereka harus setuju pada tiga nilai: Halo interval, dead interval, dan tipe jaringan. Halo OSPF Interval yang menunjukkan seberapa sering sebuah router OSPF mengirimkan paket Hello. Secara default, paket OSPF Halo dikirimkan setiap 10 detik pada segment multiaccess dan point-to-point dan setiap 30 detik untuk segmen non-broadcast multiaccess (NBMA) (Frame Relay, X.25, ATM).

Dalam kebanyakan kasus, OSPF Halo paket akan dikirim sebagai multicast ke reserved address untuk semua OSPFRouters di 224.0.0.5. Menggunakan alamat multicast memungkinkan sebuah perangkat untuk mengabaikan paket OSPF jika interfacenya tidak diaktifkan. Ini menghemat waktu proses CPU untuk device yang non-OSPF.

Periode Dead Interval, yang dinyatakan dalam detik, bahwa router akan menunggu untuk menerima paket Halo sebelum menyatakan bahwa neighbor “down”. Cisco menggunakan default empat kali Hello interval. Untuk multiaccess dan

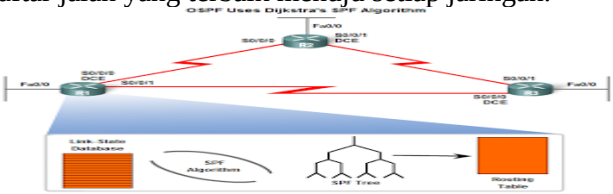
point-to-point segmen, periode ini adalah 40 detik. Untuk NBMA jaringan, Dead Interval adalah 120 detik.

Jika Dead interval berakhir sebelum router menerima paket Hello, OSPF akan menghapus neighbor ini dari link-state database. Router kemudian menyebarkan informasi link-state tentang neighbor yang “down” melalui semua OSPF interface yang aktif.

Pemilihan DR(Designated Router) dan BDR
Untuk mengurangi jumlah lalu lintas di multi-access jaringan OSPF, OSPF memilih sebuah Designated Router (DR) dan Backup Designated Router (BDR). DR bertanggung jawab untuk memperbarui semua router OSPF yang lain (disebut DROthers) ketika terjadi perubahan pada jaringan multiaccess. BDR akan memonitor DR dan mengambil alih sebagai DR jika terjadi kegagalan pada DR.

Dalam gambar, R1, R2, dan R3 dihubungkan melalui titik point-to-point link. Oleh karena itu, tidak terjadi pemilihan DR / BDR.

Algoritma OSPF
Setiap router OSPF menjaga sebuat link-state database berisi LSAs (Link-state advertisement) yang diterima dari semua router yang lain. Satu kali router menerima semua LSAs dan membuat local link-state databasenya, OSPF menggunakan algoritma Dijkstra shortest path first (SPF) untuk membuat pohon SPF. Pohon SPF kemudian digunakan untuk membuat tabel IP routing yang berisi daftar jalan yang terbaik menuju setiap jaringan.



9.2. Algoritma Kontrol Kemacetan

Network layer berfungsi untuk pengendalian operasi subnet, mendefinisikan alamat-alamat IP, membuat header untuk paket-paket, dan kemudian melakukan routing melalui internetworking dengan menggunakan router. Masalah desain yang penting adalah bagaimana caranya menentukan route pengiriman paket dari sumber ke tujuannya. Route dapat didasarkan pada table statik yang dihubungkan ke network. Route juga dapat ditentukan pada saat awal percakapan, misalnya session terminal. Terakhir, route dapat juga sangat dinamik, dapat berbeda bagi setiap paketnya. Oleh karena itu, route pengiriman sebuah paket tergantung beban jaringan saat itu.

Bila pada saat yang sama dalam sebuah subnet terdapat terlalu banyak paket, maka ada kemungkinan paket-paket tersebut tiba pada saat yang bersamaan. Hal ini dapat menyebabkan terjadinya bottleneck. Pengendalian kemacetan seperti itu juga merupakan tugas network layer.

Tugas utama dari layer network adalah menyediakan fungsi routing sehingga paket dapat dikirim keluar dari segment network lokal ke suatu tujuan yang berada pada suatu network lain. IP, Internet Protocol, umumnya digunakan untuk tugas ini. Protocol lainnya seperti IPX, Internet Packet eXchange. Perusahaan Novell telah memprogram protokol menjadi beberapa, seperti SPX (Sequence Packet Exchange) & NCP (Netware Core Protocol). Protokol ini telah dimasukkan ke sistem operasi Netware.

9.3. Internetworking

Internetworking adalah merupakan suatu abstraksi yang kuat yang memperbolehkan pembahasan kompleksitas dari teknologi komunikasi beragam di bawahnya. Dengan menyembunyikan detail dari setiap perangkat keras jaringan dan menyediakan sua tu lingkungan komunikasi tingkat tinggi.

Internetworking umumnya dibangun menggunakan tiga elemen yang berbeda:

Hubungan data LAN biasanya terbatas dalam satu bangunan atau kampus dan beroperasi menggunakan sistem pengkabelan private hubungan data WAN umumnya menggunakan saluran telekomunikasi data public, seperti X.25 PSDN, Frame Relay, ISDN, ATM devais penghubung jaringan device ini secara umum dibagi dalam beberapa kategori :

1. repeater
2. bridge
3. router
4. switch

converter

Dari kelima katagori device di atas, lebih mudah menentukan kapan menggunakan repeater, switch, dan konverter dalam situasi internetwork. Keputusan mengenai pemilihan penggunaan router atau bridge merupakan keputusan yang lebih sulit.

Berikut ini perbandingan elemen-elemen internetworking mengacu kepada layer-layer arsitektur jaringan komputer:

1.Repeater

Fasilitas paling sederhana dalam internetwork adalah repeater. Fungsi utama repeater adalah menerima sinyal dari satu segmen kabel LAN dan memancarkannya kembali dengan kekuatan yang sama dengan sinyal asli pada segmen (satu atau lebih) kabel LAN yang lain. Repeater beroperasi pada Physical layer dalam model jaringan OSI. Jumlah repeater biasanya ditentukan oleh implementasi LAN tertentu.

Penggunaan repeater antara dua atau lebih segmen kabel LAN mengharuskan penggunaan protocol Physical layer yang sama antara segmen-segmen kabel tersebut. Sebagai contoh, repeater dapat menghubungkan dua buah segmen kabel Ethernet 10BASE2.

2.Brigde

Sebuah bridge juga meneruskan paket dari satu segmen LAN ke segmen lain, tetapi bridge lebih fleksibel dan lebih cerdas

daripada repeater. Bridge menghubungkan segmen-segmen LAN di Data Link layer pada model OSI. Beberapa bridge mempelajari alamat Link setiap devais yang terhubung dengannya pada tingkat Data Link dan dapat mengatur alur frame berdasarkan alamat tersebut. Semua LAN yang terhubung dengan bridge dianggap sebagai satu subnetwork dan alamat Data Link setiap devais harus unik. LAN yang terhubung dengan menggunakan bridge umum disebut sebagai Extended LAN.

Bridge dapat menghubungkan jaringan yang menggunakan metode transmisi berbeda dan/atau medium access control yang berbeda. Misalnya, bridge dapat menghubungkan Ethernet baseband dengan Ethernet broadband. Bridge mungkin juga menghubungkan LAN Ethernet dengan LAN token ring, untuk fungsi ini, bridge harus mampu mengatasi perbedaan format paket setiap Data Link.

Bridge mampu memisahkan sebagian trafik karena mengimplementasikan mekanisme pemfilteran frame (frame filtering). Mekanisme yang digunakan di bridge ini umum disebut sebagai store and forward sebab frame yang diterima disimpan sementara di bridge dan kemudian di-forward ke worksation di LAN lain. Walaupun demikian, broadcast traffic yang dibangkitkan dalam LAN tidak dapat difilter oleh bridge.

3.Router

Router memberikan kemampuan melalukan paket dari satu sistem ke sistem lain yang mungkin memiliki banyak jalur di antara keduanya. Router bekerja pada lapisan Network dalam model OSI. Umumnya router memiliki kecerdasan yang lebih tinggi daripada bridge dan dapat digunakan pada internetwork dengan tingkat kerumitan yang tinggi sekalipun. Router yang saling terhubung dalam internetwork turut serta dalam sebuah algoritma terdistribusi untuk menentukan jalur optimum yang dilalui paket yang harus lewat dari satu sistem ke sistem lain.

Router dapat digunakan untuk menghubungkan sejumlah LAN (dan extended LAN) sehingga trafik yang dibangkitkan oleh sebuah LAN terisolasikan dengan baik dari trafik yang dibangkitkan oleh LAN lain dalam internetwork. Jika dua atau

lebih LAN terhubung dengan router, setiap LAN dianggap sebagai subnetwork yang berbeda. Mirip dengan bridge, router dapat menghubungkan data link yang berbeda. Seperti contoh, router dapat menghubungkan dua LAN yang berbeda atau untuk menghubungkan data link LAN dengan data link WAN.

4.Switch

Di samping repeater, bridge, dan router, terdapat sejumlah tipe peralatan switching lain yang dapat digunakan dalam membangun internetwork. Tujuan utama menghubungkan LAN menggunakan repeater dan bridge adalah meningkatkan keleluasaan atas beberapa keterbatasan media komunikasi LAN. Alat penghubung ini mampu menambah jumlah perangkat jaringan yang terhubung dalam LAN.

Peralatan switch didesain dengan tujuan yang berbeda dengan repeater, bridge, dan router. Jika perangkat jaringan yang terhubung dalam sebuah LAN menjadi terlalu banyak maka kebutuhan transmisi meningkat melebihi kapasitas yang mampu dilayani oleh medium komunikasi jaringan. Salah satu ide penggunaan router adalah mengisolasikan group fisik jaringan dengan yang lain. Penggunaan router cocok pada sistem internetwork dengan kelompok-kelompok kerja yang terletak dalam lokasi yang kecil. Lalu lintas data dalam jaringan kelompok-kelompok kerja ini tentu lebih besar dibandingkan dengan lalu lintas antar kelompok kerja.

Dalam kasus kelompok-kelompok kerja yang terletak terpisah secara geografis, penggunaan router tetap tidak dapat mengisolasikan lalu lintas data. Lalu lintas data dalam kelompok kerja yang tinggi akan menyebabkan beban di router tetap tinggi karena lalu lintas tersebut selalu melewati router. Cara mengatasi hal ini adalah dengan menggunakan beberapa segmen medium tranmisi secara paralel dalam internetwork. Router sendiri tetap dapat digunakan untuk menghubungkan segmen-segmen tersebut dan tetap mampu mengisolasi trafik antarsegmen. Perangkat network dapat dihubungkan ke medium transmisi yang sesuai atau dengan menggunakan hub yang mengimplementasikan fasilitas switching, seperti module assignment hub, bank assignment hub, dan port assignment hub.

5.Converter

Converter dapat dianggap sebagai tipe devais yang berbeda daripada repeater, bridge, router, atau switch dan dapat digunakan bersama-sama. Converter (kadang disebut gateway) memungkinkan sebuah aplikasi yang berjalan pada suatu sistem berkomunikasi dengan aplikasi yang berjalan pada sistem lain yang berjalan di atas arsitektur network berbeda dengan sistem tersebut. Converter bekerja pada lapisan Application pada model OSI dan bertugas untuk melalukan paket antar jaringan dengan protokol yang berbeda sehingga perbedaan tersebut tidak tampak pada lapisan aplikasi.

Di samping menggunakan converter, metode lain untuk menghubungkan jaringan dengan arsitektur berbeda adalah dengan tunelling. Metode ini membungkus paket -termasuk protokolnya- yang akan dilewatkan pada protokol lain. Pembungkusan ini dilakukan dengan menambahkan header protokol pada paket yang akan dilewatkan. Metode ini dapat dilihat sebagai sebuah arsitektur jaringan yang berjalan di atas arsitektur jaringan yang lain. Perangkat tempat terjadinya proses tunnelling ini disebut sebagai portal.

10. Pertemuan 10

10.1. Protocol ALOHA

Protokol yang digunakan untuk menentukan giliran pada saluran multiaccess terdapat pada sublayer dari data link layer yang disebut MAC (media access control) sublayer. Peranan MAC sublayer sangat penting bagi sebuah LAN, hampir semua yang menggunakan saluran multiaccess menentukannya sebagai basis komunikasi. Sebaliknya WAN menggunakan link point to point, kecuali jaringan satelit. Karena saluran multiaccess dan LAN sangat berkaitan erat secara teknik, MAC sublayer merupakan bagian terbawah dari data link layer.

Masalah Lokasi Saluran

Alokasi saluran statik pada LAN dan MAN

Cara tradisional dalam mengalokasikan sebuah saluran misalnya kabel telepon dengan banyak pengguna yang

berkompetisi adalah dengan menggunakan Frequensy Division Multiplexing (FDM).

Saluran Dinamik Pada LAN dan MAN ;

1. Model Stasiun. Model terdiri dari n buah stasiun yang independent (komputer telepon alat komunikasi pribadi, dll) yang masing-masing memiliki program dan pengguna yang menghasilkan frame untuk trasmisi, stasiun akan diblokir dan tidak melakukan apapun juga sampai frame tersebut berhasil ditrasmisikan.

2. Asumsi Saluran Tunggal saluran tersedia bagi semua jenis komunikasi, semua stasiun dapat mentrasmisikan melalui saluran tersebut dan semua dapat menerima melalui saluran itu juga. Selama hardware diperhatikan, semua stasiun adalah ekivalen, walaupun software protokol mungkin memberikan prioritas tertentu padanya.

3. Asumsi Tabrakan bila dua buah frame ditrasmisikan secara bersama, keduaanya bertumpah tindih waktunya dan akan menyebabkan signal yang rusak. kejadian ini dinamakan tabrakan (collision). Semua stasiun dapat mendeteksi tabrakan. Frame yang bertabrakan harus ditranmisikan ulang. Tidak terjadi error lainnya selain yang disebabkan oleh tabrakan.

4. a.Waktu Kontinu. Tranmisi frame dapat dilakukan setiap saat tidak terdapat master clock yang berbagi waktu menjadi interval-interval diskrit.

b.Waktu Slot Waktu dibagi menjadi interval – interval diskrit (slot). Trasmisi frame selalu dimulai pada awal sebuah slot. Sebuah slot dapat berisi 0, 1, atau lebih frame, yang masing-masing berhubungan dengan slot yang idle, transmisi yang berhsil dan tabrakan.

5. a. Carrier Sense. Stasiun dapat mengetahui bahwa suatu saluran sedang dipakai sebelum mencoba menggunakannya, bila saluran sedang sibuk maka tidak akan ada stasiun yang akan mencoba menggunakannya sampai saluran tersebut berada dalam keadaan idle.

b. No Carrier Sense. Stasiun tidak dapat merasakan keaadaan suatu saluran sebelum menggunakanya. Stasiun mencoba menggunakan menggunakan dan menggunakan trasmisi.

Setelah beberapa saat kemudian stasiun akan mengetahui bahwa apakah trasmisi tersebut berhasil atau gagal.

MULTIPLE ACCESS PROTOKOL

ALOHA

Pada 1970-an, Norman Abramson dan rekan sejawatnya di Universitas Hawai membuat sebuah metode untuk menyelesaikan masalah alokasi saluran yang baru dan baik sekali. Setelah itu karya mereka telah dikembangkan oleh para peneliti (abramson, 1985). Walaupun karya abramson, dikenal sebagai sistem Aloha, menggunakan broadcasting radio permukaan, ide dasarnya dapat diterapkan bagi beberapa sistem pengguna-pengguna yang tidak dapat terkoordinasi berkompetisi untuk memakai sebuah saluran tunggal yang dipakai bersama.

ALOHA MURNI

Ide dasar Aloha sangat sederhana : membiarkan pengguna untuk melakukan trasmisi kapan saja bila memiliki data yang akan dikirimkan. Tentu saja akan terjadi tabrakan, dan frame-frame yang bertabrakan akan hancur, akan tetapi sehubungan dengan sifat umpan balik dari broadcasting, pengirim selalu mengetahui apakah frame yang dikirim sudah rusak atau tidak dengan cara mendengarkan saluran, sama seperti cara yang dipakai oleh pengguna lainnya.

Pada LAN, umpan balik bersifat segera: pada satelit, terdapat delay 270 milidetik sebelum pengirim mengetahui keberhasilan sebuah trasmisi. Bila frame telah rusak, maka pengirim perlu menggirim dalam waktu Random dan megirimkannya kembali, waktu tunggu harus random atau frame-frame yang sama akan terus bertabrakan sistem yang memiliki banyak pengguna yang

menggunakan bersama-sama sebuah saluran umum yang pada gilirannya akan manyebabkan konflik dikenal luas sebagai sistem contention (persaingan).

ALOHA Berslot

Pada 1972, Robers menerbitkan metode untuk mengadakan kapasitas sistem ALOHA (Roberts, 1972). Dalam proposalnya ia membagi waktu kedalam interval-interval diskrit, yang masing-masing intervalnya berkaitan dengan sebuah frame.Pendekatan ini memerlukan persetujuan pengguna tantang batas-batas slot.

Satu cara untuk memperoleh sikronisasi harus memiliki sebuah stasiun khusus yang mengemisikan sebuah pipa pada awal setiap interval, sepertihalnya sebuah jam

Dalam metode roberts, yang sekarang dikenal sebagai ALOHA berselot komputer tidak diijinkan untuk mengirimkan sesuatu setiap saat tombol ENTER diketikkan, akan tetapi, pengiriman frame memerlukan waktu tunggu sampai awal slot berikutnya.

10.2. Standar IEEE 802.XX

802 Standar. IEEE 802.2, 802,3, 802,5, 802,11

Lembaga Insinyur Listrik dan Elektronika adalah badan pengaturan standar. Masing-masing standar mereka diberi nomor dan subset dari nomor adalah standar yang sebenarnya. Keluarga 802 adalah standar yang dikembangkan untuk jaringan komputer.

Pada bagian ini, Anda akan belajar:

- Apa yang 802,2, 802,3, 802,5, 802,11 standar mencakup;

- Fitur, topologi, dan kabel jaringan untuk masing-masing standars.

Pertama, mari kita bahas 802. IEEE atau Institute of Electrical dan Electronics Engineers, adalah badan pengaturan standar. Mereka membuat standar untuk hal-hal seperti jaringan sehingga produk dapat kompatibel satu sama lain. Anda mungkin pernah mendengar dari IEEE 802.11b - ini adalah standar yang IEEE telah menetapkan (dalam contoh ini, wireless-b jaringan).

Pada bagian ini, kita akan melihat beberapa teknologi jaringan: 802.2 802.3, 802.5, 802.11, dan FDDI. Masing-masing hanya satu set standar teknologi, masing-masing dengan karakteristik sendiri.

802.2 Kontrol Logical Tautan

Definisi teknis 802.2 adalah "standar untuk sublapisan Data Link Layer atas juga dikenal sebagai lapisan Logical Link Control Hal ini digunakan dengan 802,3, 802,4,. Dan 802,5 standar (lebih rendah DL sublayer)."

802.2 "menentukan antarmuka umum antara lapisan jaringan (IP, IPX, dll) dan link lapisan data (Ethernet, Token Ring, dll).

Pada dasarnya, memikirkan 802.2 sebagai "penerjemah" untuk layer data link. 802.2 berkaitan dengan mengelola lalu lintas melalui jaringan fisik. Hal ini bertanggung jawab untuk aliran dan kontrol kesalahan. Layer Data Link ingin mengirim beberapa data melalui jaringan, 802.2 Logical Link Control membantu membuat ini mungkin. Hal ini juga membantu dengan mengidentifikasi protokol line, seperti NetBIOS, atau Netware.

LLC bertindak seperti bus perangkat lunak yang memungkinkan beberapa protokol lapisan yang lebih tinggi untuk mengakses satu atau lebih jaringan lapisan bawah. Misalnya, jika Anda memiliki sebuah server dengan kartu antarmuka jaringan, LLC akan maju packers dari mereka protokol lapisan atas ke antarmuka jaringan yang sesuai. Hal ini

memungkinkan protokol lapisan atas untuk tidak perlu pengetahuan khusus dari jaringan lapisan yang lebih rendah digunakan.

802.3 Ethernet

Sekarang kita memiliki gambaran dari model OSI, kita dapat melanjutkan pada topik ini. Saya harap Anda memiliki gambaran yang lebih jelas dari model jaringan dan mana hal-hal sesuai di atasnya.

802.3 adalah standar yang Ethernet beroperasi dengan. Ini adalah standar untuk CSMA / CD (Carrier Sense Multiple Access dengan Collision Detection). Standar ini meliputi baik MAC dan standar Physical Layer.

CSMA / CD adalah apa Ethernet menggunakan untuk mengontrol akses ke media jaringan (kabel jaringan). Jika tidak ada data, setiap node mungkin mencoba untuk mengirimkan, jika node mendeteksi tabrakan, baik menghentikan transmisi dan tunggu selama beberapa waktu sebelum mentransmisi data.

Standar 802.3 yang asli adalah 10 Mbps (Megabits per detik). 802.3u mendefinisikan 100 Mbps (Fast Ethernet) standar, 802.3z/802.3ab didefinisikan 1000 Mbps Gigabit Ethernet, dan 802.3ae mendefinisikan 10 Gigabit Ethernet.

Umumnya, jaringan Ethernet mentransmisikan data dalam bentuk paket, atau bit kecil informasi. Sebuah paket dapat menjadi ukuran minimum 72 byte atau maksimum 1518 byte.

Topologi yang paling umum untuk Ethernet adalah topologi star.

802,5 Token Ring

Seperti yang telah disebutkan sebelumnya ketika membahas topologi cincin, Token Ring dikembangkan terutama oleh IBM.

Token ring dirancang untuk menggunakan topologi ring dan menggunakan token untuk mengontrol transmisi data pada jaringan.

Token adalah frame khusus yang dirancang untuk perjalanan dari node ke node sekitar ring.Ketika tidak memiliki data apapun yang melekat padanya, node pada jaringan dapat memodifikasi frame, melampirkan data dan mengirimkan. Setiap node pada jaringan memeriksa token saat lewat untuk melihat apakah data ditujukan untuk node yang, jika, melainkan menerima data dan mentransmisikan token baru. Jika tidak dimaksudkan untuk node itu, mentransmisikan token ke simpul berikutnya.

Jaringan token ring dirancang sedemikian rupa sehingga setiap node pada jaringan dijamin akses ke token di beberapa titik. Ini menyetarakan transfer data pada jaringan. Hal ini berbeda dengan jaringan Ethernet mana setiap workstation memiliki akses yang sama untuk ambil bandwidth yang tersedia, dengan kemungkinan sebuah node menggunakan bandwidth lebih dari node lain.

Awalnya, token ring beroperasi pada kecepatan sekitar 4 Mbps dan 16 Mbps. 802.5t memungkinkan untuk kecepatan 100 Mbps dan 802.5v menyediakan untuk 1 Gbps lebih pembohong.

Token ring dapat dijalankan melalui sebuah topologi bintang serta topologi ring.

Ada tiga jenis kabel utama untuk token ring: twisted Pair (UTP), twisted pair Terlindung (STP), dan pembohong.

Token ring menggunakan Unit Multi-stasiun Access (MAU) sebagai hub kabel pusat. Ini juga kadang-kadang disebut MSAU ketika mengacu pada jaringan token ring.

802.11 Standar Wireless Network

802.11 adalah koleksi dari setup standar untuk jaringan nirkabel. Anda mungkin akrab dengan tiga standar populer: 802.11a, satu 802.11b, 802.11g dan 802.11n terbaru adalah. Setiap standar menggunakan frekuensi untuk terhubung ke jaringan dan memiliki batas atas ditetapkan untuk kecepatan transfer data.

802.11a adalah salah satu standar nirkabel pertama. 802.11a beroperasi pada pita radio 5GHz dan dapat mencapai maksimum 54Mbps. Bukankah sebagai populer sebagai standar 802.11b karena harga yang lebih tinggi dan jangkauan lebih rendah.

802.11b beroperasi di band 2.4Ghz dan mendukung hingga 11 Mbps. Rentang sampai beberapa ratus kaki dalam teori. Konsumen Opsi pertama nyata untuk nirkabel dan sangat populer.

802.11g adalah sebuah standar dalam operasi pita 2.4Ghz pada 54Mbps. Karena beroperasi di band yang sama seperti 802.11b, 802.11g kompatibel dengan peralatan 802.11b. 802.11a tidak langsung kompatibel dengan 802.11b atau 802.11g karena beroperasi di band yang berbeda.

Wireless LAN terutama menggunakan CSMA / CA - Carrier Sense Multiple Access / Collision Avoidance. Memiliki "mendengarkan sebelum berbicara" metode meminimalkan tabrakan pada jaringan nirkabel. Hal ini mengakibatkan kurang perlu untuk mentransmisi data.

Standar nirkabel beroperasi dalam topologi nirkabel.

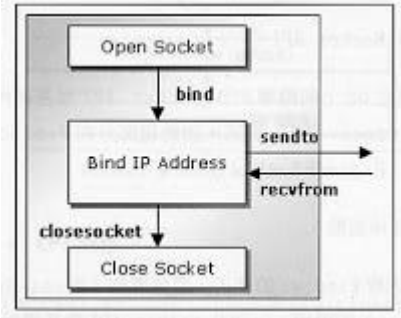
11. Pertemuan 11

11.1. Pendahuluan dan Socket

Mengenal Socket

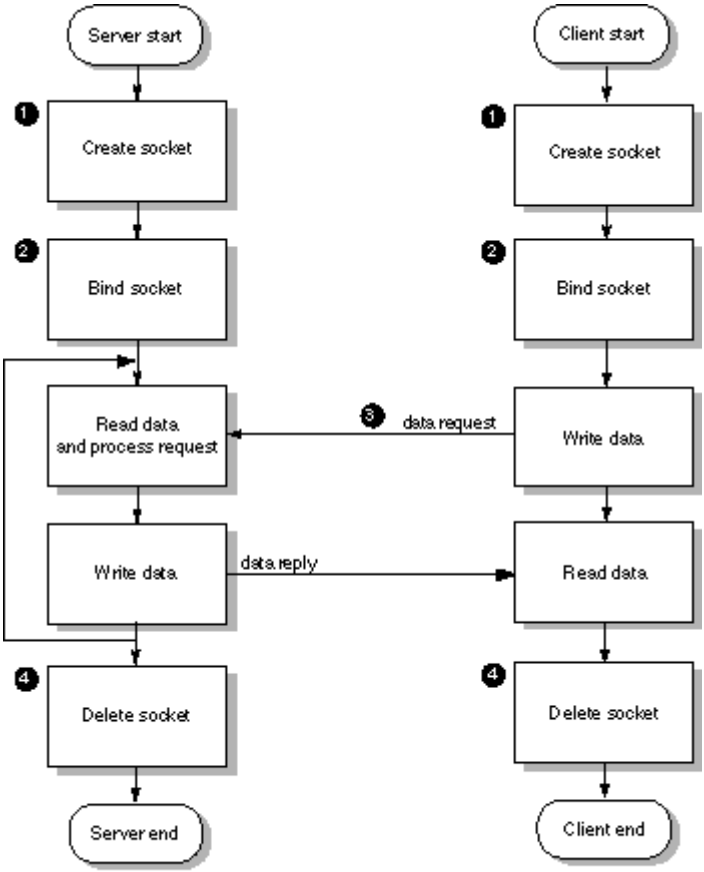
Bayangkan sebuah server game online yang berkomunikasi tanpa henti, dimainkan oleh entah berapa banyak client yang tersebar. Ini merupakan salah satu contoh aplikasi dari sekian

banyak aplikasi yang menggunakan socket jaringan untuk saling berkomunikasi dan bertukar data.



Komunikasi socket jaringan memang tidak mengenal lelah, pertukaran data terjadi terus-

menerus dan memegang peranan vital. Jika oleh karena suatu hal komunikasi berhenti karena maintenance, kerusakan, ataupun sebab lainnya, maka dapat dipastikan para penggunanya akan kecewa.



Maka dari itu, komunikasi jaringan selalu diusahakan tidak terhenti. Demikianlah tugas berat yang harus dilakukan socket jaringan. Sebelum membahas lebih jauh, apakah sebenarnya pengertian socket itu?

Pengertian socket adalah interface pada jaringan yang menjadi titik komunikasi antarmesin pada Internet Protocol, dan tentunya tanpa komunikasi ini, tidak akan ada pertukaran data dan informasi jaringan.

Socket terdiri dari elemen-elemen utama sebagai berikut:

1. Protokol.

2. Local IP.
3. Local Port.
4. Remote IP.
5. Remote Port.

Dalam komunikasi antara dua pihak, tentunya harus digunakan kesepakatan aturan dan format yang sama agar komunikasi dapat dimengerti. Seperti halnya dua orang yang menggunakan bahasa yang sama, maka bahasa di sini berfungsi sebagai protokol. Protokol yang digunakan dalam socket dapat menggunakan TCP ataupun UDP.
Contoh komunikasi sederhana adalah komunikasi antara komputer A dan komputer B. Baik komputer A maupun komputer B harus memiliki identitas unik, yang direpresentasikan oleh IP masing-masing.
Komunikasi yang terjadi melalui port, sehingga baik komputer A maupun komputer B harus memiliki port yang dapat diakses satu sama lain.

12. Pertemuan 12

12.1. Subnetting IP

Subnetting adalah proses memecah suatu IP jaringan ke sub jaringan yang lebih kecil yang disebut "subnet." Setiap subnet deskripsi non-fisik (atau ID) untuk jaringan-sub fisik (biasanya jaringan beralih dari host yang mengandung satu router -router dalam jaringan multi).

Mengapa harus melakukan subnetting? Ada beberapa alasan mengapa kita perlu melakukan subnetting, diantaranya adalah sebagai berikut:
Untuk mengefisienkan alokasi IP Address dalam sebuah jaringan supaya bisa memaksimalkan penggunaan IP Address.
Mengatasi masalah perbedaan hardware dan media fisik yang digunakan daam suatu network, karena Router IP hanya dapat mengintegrasikan berbagai network dengan media fisik yang berbeda jika setiap network memiliki address network yang unik.
Meningkatkan security dan mengurangi terjadinya kongesti akibat terlalu banyaknya host dalam suatu network.

Penghitungan subnetting bisa dilakukan dengan dua cara yaitu binary yang relatif lambat dan cara khusus yang lebih cepat. Penulisan IP address umumnya adalah dengan 192.168.1.2. Namun adakalanya ditulis dengan 192.168.1.2/24. Penjelasanya adalah bahwa IP address 192.168.1.2 dengan subnet mask 255.255.255.0. Kenapa bisa seperti ?maksud /24 diambil dari penghitungan bahwa 24 bit subnet mask diselubung dengan binari 1. Atau dengan kata lain, subnet masknya adalah: 11111111.11111111.11111111.00000000 (255.255.255.0). Konsep ini yang disebut dengan CIDR (Classless Inter-Domain Routing) yang diperkenalkan pertama kali tahun 1992 oleh IEFT. Pada hakekatnya semua pertanyaan tentang subnetting akan berkisar di empat masalah: Jumlah Subnet, Jumlah Host per Subnet, Blok Subnet, dan Alamat Host- Broadcast.

12.2. Subnet mask

Subnet mask adalah istilah teknologi informasi dalam bahasa Inggris yang mengacu kepada angka biner 32 bit yang digunakan untuk membedakan network ID dengan host ID, menunjukkan letak suatu host, apakah berada di jaringan lokal atau jaringan luar.

RFC 950 mendefinisikan penggunaan sebuah subnet mask yang disebut juga sebagai sebuah address mask sebagai sebuah nilai 32-bit yang digunakan untuk membedakan network identifier dari host identifier di dalam sebuah alamat IP. Bit-bit subnet mask yang didefinisikan, adalah sebagai berikut:

* Semua bit yang ditujukan agar digunakan oleh network identifier diset ke nilai 1.
* Semua bit yang ditujukan agar digunakan oleh host identifier diset ke nilai 0.

Setiap host di dalam sebuah jaringan yang menggunakan TCP/IP membutuhkan sebuah subnet mask meskipun berada di dalam sebuah jaringan dengan satu segmen saja. Entah itu subnet mask default (yang digunakan ketika memakai network identifier berbasis kelas) ataupun subnet mask yang dikustomisasi (yang digunakan ketika membuat sebuah subnet

atau supernet) harus dikonfigurasikan di dalam setiap node TCP/IP.

Pengertian Dan Fungsi Default Gateway
Gateway adalah sebuah perangkat yang digunakan untuk menghubungkan satu jaringan komputer dengan satu atau lebih jaringan komputer yang menggunakan protokol komunikasi yang berbeda sehingga informasi dari satu jaringan computer dapat diberikan kepada jaringan komputer lain yang protokolnya berbeda.

Istilah gateway merujuk kepada hardware atau software yang menjembatani dua aplikasi atau jaringan yang tidak kompatibel, sehingga data dapat ditransfer antar komputer yang berbeda-beda.Salah satu contoh penggunaan gateway adalah pada email, sehingga pertukaran email dapat dilakukan pada sistem yang berbeda. Definisi tersebut adalah definisi gateway yang utama. Dalam pengertian teknis, istilah ini mengacu pada pengaturan hardware maupun software yang menerjemahkan antara dua protokol yang berbeda.

Pengertian yang lebih umum untuk istilah ini adalah sebuah mekanisme yang menyediakan akses ke sebuah sistem lain yang tehubung dalam sebuah network. Host yang digunakan untuk mengalihkan lalu lintas jaringan dari satu jaringan ke jaringan lain, juga digunakan untuk melewatkan lalu lintas jaringan dari satu protokol ke protokol lain. Dipergunakan untuk menghubungkan dua jenis jaringan komputer yang arsitekturnya sama sekali berbeda. Jadi gateway lebih kompleks daripada bridge. Gateway dapat diaplikasikan antara lain untuk menghubungkan IBM SNA dengan digital DNA, LAN (Local Area Network) dengan WAN (Wide AreaNetwork).

Seiring dengan merebaknya internet, definisi gateway seringkali bergeser. Tidak jarang pula pemula menyamakan "gateway" dengan "router" yang sebetulnya tidak benar. Kadangkala, kata "gateway" digunakan untuk mendeskripkan perangkat yang menghubungkan jaringan komputer besar dengan jaringan

komputer besar lainnya. Hal ini muncul karena seringkali perbedaan protokol komunikasi dalam jaringan komputer hanya terjadi di tingkat jaringan komputer yang besar. Gateway juga bisa diartikan sebagai komputer yang memiliki minimal 2 buah network interface untuk menghubungkan 2 buah jaringan atau lebih.

Di Internet suatu alamat bisa ditempuh lewat gateway-gateway yang memberikan jalan/rute ke arah mana yang harus dilalui supaya paket data sampai ke tujuan. Kebanyakan gateway menjalankan routing daemon (program yang meng-update secara dinamis tabel routing). Karena itu gateway juga biasanya berfungsi sebagai router. Gateway/router bisa berbentuk Router box seperti yang di produksi Cisco, 3COM, dll atau bisa juga berupa komputer yang menjalankan Network Operating System plus routing daemon. Misalkan PC yang dipasang Unix FreeBSD dan menjalankan program Routed atau Gated. Namun dalam pemakaian Natd, routing daemon tidak perlu dijalankan, jadi cukup dipasang gateway saja.Karena gateway/router mengatur lalu lintas paket data antar jaringan, maka di dalamnya bisa dipasangi mekanisme pembatasan atau pengamanan (filtering) paket-paket data, Mekanisme ini disebut Firewall.

Fungsi Gateway
Salah satu fungsi pokok gateway adalah melakukan protocol converting, agar dua arsitektur jaringan komputer yang berbeda dapat saling berkomunikasi.

Pengertian DNS

DNS (Domain Name System) atau Sistem Penamaan Domain merupakan 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.

13. Pertemuan 13

13.1. HTTP

Pengertian dan HTTP (Hypertext Transfer Protocol) - Bagi kalian yang sering berselancar didunia maya pasti tidak asing dengan istilah HTTP. Ya istilah tersebut memang tidak asing ditelinga kita, tapi apakah kita tahu sebenarnya apa itu HTTP. Nah untuk menjawab ketidak tahuan Anda mengenai HTTP ini, kali ini saya mau berbagi artikel seputar pengertian HTTP.

Pengertian dan HTTP (Hypertext Transfer Protocol)
HTTP singkatan dari Hypertext Transfer Protocol adalah suatu protokol yang digunakan untuk mengirim dokumen atau halamamn dalam WWW atau World Wide Web. Sedangkan pengertian HTTP menurut kamus besar adalah protokol jaringan untuk didistribusikan, kolaboratif, sistem informasi hypermedia. HTTP adalah dasar dari komunikasi data untuk WWW.

Dalam pengertian HTTP tersebut, menetapkan bagaimana pesan diformat dan ditransmisikan dan seperti apa respon dari browser. Sejarah protokol HTTP pertama kali digunakan dalam WWW sekitar tahun 1990. Nah yang dipakai pada masa itu ialah protokol HTTP versi 0.9 yang merupakan protokol transfer data secara mentah, maksud mentah disini yaitu data tersebut dikirimkan tanpa melihat tipe dari dokumen itu sendiri.

6 Tahun kemudian yaitu sekitar tahun 1996, protokol HTTP mengalami perbaikan sehingga menjadi protokol HTTP versi 1.0. Dan pada tahun 1999 dikeluarkan HTTP versi selanjjutnya yaitu 1.1 untuk mengakomodasi proxy, cache dan koneksi yang persisten.

HTTP adalah protoko aplikasi berbasis client server sederhana yang dibangun atas TCP (transmission Control Protocol). Sebuah client HTTP biasanya memulai permintaan dengan menciptkan sebuah hubungan ke port tertentu di sebua hserver

webhosting tertentu. Umumnya port yang digunakan adalah port 80. Klien juga sering dikenal dengan user agent, sedangkan server yang meresponnya dan juga meyimpan sumber daya seperti berkas HTML dan gambar disebut dengan origin server.

Nah diantara keduanya yaitu user agent dan origin server bisa saja ada oenghubung, seperti misalnya geteway, tunnel dan proxy. Nah selanjutnya sumber yang ingin diakses dengan menggunakan HTTP diidentifikasi dengan menggunakan URL (Uniform Resource Locator) dengan skema URL http: atau https:.

Fungsi dan Cara Kerja HTTP

Kalian pasti tahu kalau HTTP muncul diawal setiap alamat web. Ya semua layanan web dijalankan melalui protokol ini. HTTPS adalah variasi dari HTTP dimana dalam hal inibrowser menambah lapisan enkripsi.

Cara kerja protokol ini yaitu untuk mengkomunikasikan satu dengan yang lainnya. Protokol adalah perintah yang harus diikuti oleh setiap komputer untuk bisa mengirim atau menerima pesan. Penggunaan protokol yang paling umum yaitu HTTP, SMTP, FTP, IMAP, POP3, dan masih banyak lagi lainnya.

Fungsi dari HTTP itu sendiri adalah menetapkan bagaimana pesan atau data yang ada diformat dan ditrasmisikan menjadi bentuk yang bisa merespon browser untuk memunculkan data-data tersebut.

13.2. Telnet

Inilah pengertian Telnet dan fungsinya, dapat kamu baca dan pahami pada pembahasan ini. Telnet adalah singkatan dari Telecommunications Network Protocol, merupakan remote login yang terjadi pada jaringan internet disebabkan karena adanya service dari protocol Telnet. Dengan adanya Telnet dapat memungkinkan pengguna dapat mengakses komputer lain secara remote melalui jaringan internet.

A. Penjelasan lain dari Telnet

Atau definisi Telnet yaitu merupakan suatu protocol yang memungkinkan penggunanya dapat login dan bekerja pada sistem jarak jauh, seperti jika terdapat program maupun file yang tersimpan pada komputer jarak jauh tersebut berada di komputer pengguna itu sendiri. Singkatnya Telnet merupakan perangkat lunak (softwere) yang digunakan untuk melakukan kontrol jarak jauh pada sistem komputer.

Telnet digunakan untuk melakukan login ke komputer lain yang ada di jaringan internet dan dapat melakukan akses pada pelayanan umum, termasuk pada berbagai macam database. Penggunanya dapat duduk saja di depan komputer yang terhubung ke jaringan internet. Dengan kata lain dapat terkoneksi ke komputer lain dalam satu gedung, satu ruangan atau bahkan pada komputer di seluruh penjuru dunia. Setelah terhubung atau terkoneksi, input yang diberikan pada keyboard dapat secara langsung mengontrol ke remote komputer tadi, dapat diakses pelayanan apa saja yang telah disediakan oleh remote machine dan hasilnya akan ditampilkan pada terminal lokal. Dengan menggunakan Telnet, pengguna dapat mengakses berbagai layanan misalnya seperti melihat katalog perpustakaan dan masih banyak lagi layanan yang lainnya. Baca juga penjelasan: Pengertian protokol dan jenisnya pada jaringan komputer.
Pada penggunaannya Telnet memakai 2 (dua) program yaitu pada client dan server. Program pada client digunakan untuk meminta layanan pada server, sedangkan program yang terdapat pada server akan memberikan layanan yang diminta oleh client. Baca juga: Pengertian server dan client lengkap.

B. Fungsi utama Telnet (Telecommunications network protocol)

Singkatnya fungsi utama pada Telnet adalah untuk dapat mengakses komputer dari jarak jauh. Karena Telnet dapat

memungkinkan komputer penggunanya menjadi terminal dari komputer yang lain di jaringan internet. Dan Telnet memungkinkan penggunanya dapat melakukan login sebagai pemakai komputer jarak jauh dan menjalankan program komputer layanan yang terdapat pada komputer tersebut. Itulah fungsi utama dari Telnet.

C. Kelebihan dan kekurangan menggunakan Telnet (Telecommunications network protocol)

1. Kelebihan Telnet

Adapun kelebihan jika menggunakan telnet server adalah user interface yang cukup ramah, maksudnya pengguna dapat memberikan perintah dari jarak jauh (remote) jadi seolah-olah penggunanya mengeksekusi perintah pada command line pada komputer.

2. Kekurangan Telnet

Dimana ada kelebihan selalu ada kekurangan, adapun kekurangan dari Telnet yaitu pengguna NTLM authentication tanpa adanya enkripsi sehingga dapat memudahkan pencurian password yang dilakukan oleh sniffers, jika kita administrator sistem maka disarankan untuk menggunakan SSH pada Linux daripada Telnet Server untuk mengkonfigurasikan sistem kita.

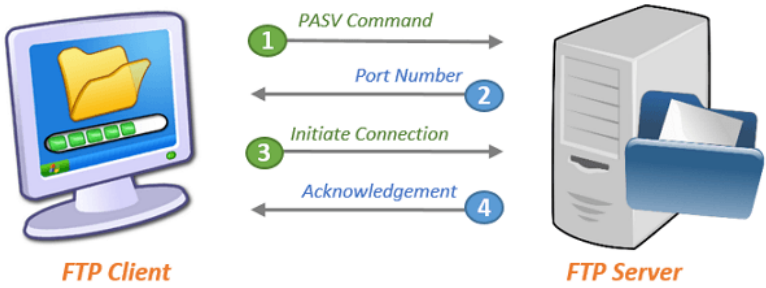
13.3. FTP

Pertukaran data adalah hal yang penting dalam dunia komputer. Dengan adanya pertukaran data, komputer yang satu dapat terhubung dengan komputer lainnya. Seperti misalnya ketika anda mendownload suatu file di internet, pernahkan anda berfikir bagaimana bisa kita mendownload file tersebut? Kemudian ketika anda mengupload suatu file, bagaimana semua itu bisa terjadi? Itu semua karena peran dari FTP.

FTP merupakan solusi bagi dua buah komputer yang ingin melakukan transfer data dengan bantuan koneksi intenet. FTP ini sangat berguna bahkan untuk dua buah komputer yang memiliki sistem operasi berbeda. FTP juga berguna untuk mentransfer data antara dua komputer yang jaraknya berjauhan.

Pengertian FTP

FTP atau File Transfer Protocol merupakan protokol internet yang digunakan untuk urusan pengiriman data dalam jaringan komputer, seperti upload dan download file yang dilakukan oleh FTP client dan FTP server. Layanan FTP bisa diatur menjadi FTP public, dimana semua orang bisa mengakses data-data yang ada di server FTP dengan mudah. Selain dapat diatur menjadi FTP public, layanan FTP ini juga bisa diatur agar tidak semua orang dapat mengakses data-data yang ada di server, jadi hanya pengguna terdaftar saja yang memiliki izin untuk mengakses data-data tersebut.



FTP berkerja menggunakan salah satu protokol yang dapat diandalkan untuk urusan komunikasi data antara client dan server, yaitu protokol TCP (yang menggunakan port nomor 21). Port 21 ini digunakan untuk mengirimkan command (perintah). Oleh karena port 21 dimaksudkan khusus untuk mengirimkan command, maka port ini sering juga disebut dengan nama command port. Dengan adanya protokol ini, antara client dan server dapat melakukan sesi komunikasi sebelum pengiriman data berlangsung. Terdapat beberapa persyaratan untuk menggunakan FTP, yaitu :

Pada komputer pengguna sudah terinstall FTP Client, seperti misalnya FileZilla.

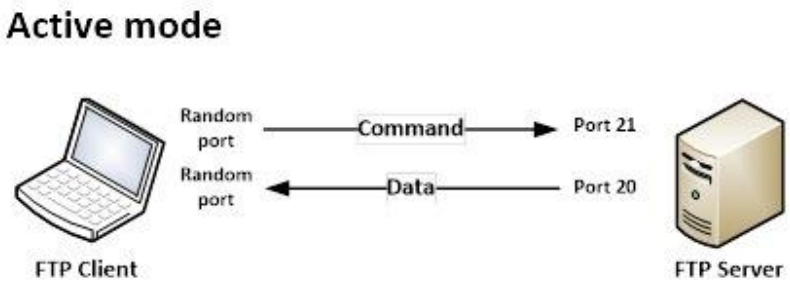
Pengguna memiliki cukup informasi tentang FTP server yang ingin terhubung dengan komputer. Informasi tersebut mencakup :

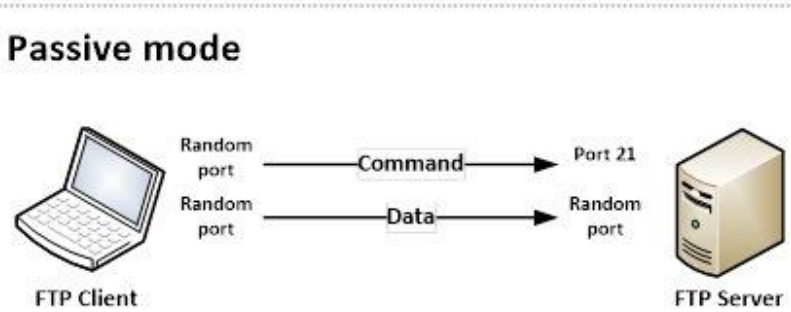
Alamat FTP Server, yang bentuknya mirip dengan alamat domain sebuah website. Alamat FTP Server biasanya diawali dengan kata ftp, misalnya saja : ftp.namadomain.com atau ftp://ftp.namadomain.com. Pada beberapa kasus, alamat FTP Server juga diberikan dalam bentuk IP address, seperti misalnya : 61.185.225.87.

Username dan password. Beberapa FTP server memang membiarkan para client mengakses data secara anonim, namun beberapa memerlukan inputan username dan password yang harus diketahui oleh client.

Perbedaan antara FTP client dan FTP server?

FTP server merupakan server yang bertugas memberikan layanan pengiriman/ tukar menukar data kepada FTP client dengan syarat FTP client harus meminta (request) terlebih dahulu kepada FTP server. Sebuah FTP server dapat bekerja dengan koneksi aktif maupun pasif. Pada koneksi aktif, jika klien membuka sebuah port, maka server secara otomatis terkoneksi dengan aktif. Jika Anda terhubung dengan FTP server secara aktif, maka Anda perlu mengatur firewall untuk menerima koneksi ke sebuah port yang akan dibuka oleh FTP client. FTP server aktif biasanya menggunakan 20 port sebagai port datanya.





Sedangkan FTP client merupakan komputer/ perangkat yang meminta layanan tukar-menukar data kepada FTP server. Setelah terkoneksi dengan FTP server, FTP client dapat melakukan proses download, upload dan lain sebagainya sesuai dengan izin yang telah diberikan oleh FTP server sebelumnya. Kebanyakan FPT Client memilih untuk menggunakan koneksi pasif secara default, karena admin server menganggap hal tersebut lebih aman. Dengan menggunakan koneksi pasif, maka semua koneksi yang dimulai dari luar akan langsung terkena blok. Dengan mode pasif, FTP Client lah yang meminta server untuk membuat koneksi.

Beberapa contoh FTP client antara lain coreFTP (Windows), FileZilla (Windows), cuteFTP (Windows), dan CyberDuck (Mac). Sebetulnya, FTP Client hanyalah aplikasi atau tool yang dapat digunakan untuk mengakses FTP. Terdapat tool lainnya yang dapat digunakan pula untuk mengakses FTP, diantaranya :

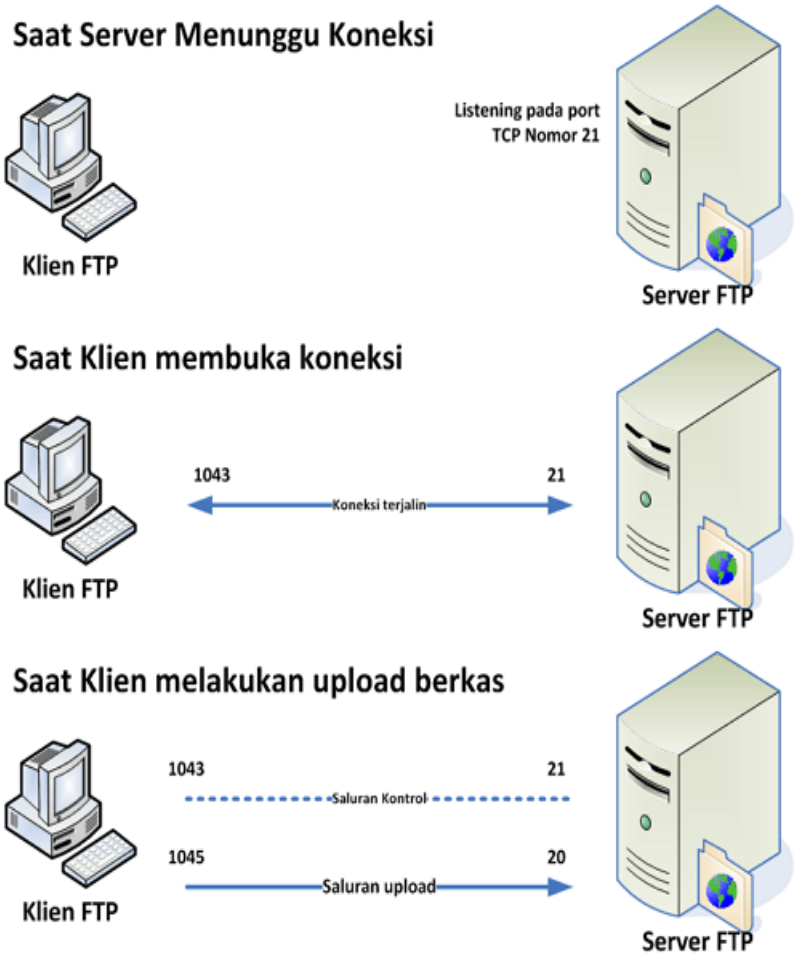
Web browser : Walaupun sebetulnya tidak begitu direkomendasikan, tapi sebetulnya Anda dapat menggunakan FTP pada sebagian besar web browser.
HTML Editor : Misalnya Adobe Dreamweaver yang dapat terhubung dengan FTP sehingga pengguna komputer dapat melakukan pengeditan website pada web server secara langsung.
File Explorer : Anda juga dapat mengakses FTP melalui File Explorer (atau Windows Explorer) dengan terlebih dahulu mengetikkan alamat FTP servernya.
Fungsi FTP

FTP memiliki banyak fungsi atau manfaat yang menguntungkan bagi penggunanya, misalnya saja :

Kita dapat melakukan pertukaran file antar komputer dengan mudah, walaupun file tersebut memiliki ukuran yang besar.
Bagi pemilik website, dengan adanya FTP, mereka dapat melakukan backup website mereka dengan mudah.
Kita dapat melakukan indirect maupun implicit remote computer.
FTP menyediakan transfer data yang reliabel dan efisien, karena setiap pengguna tidak memerlukan tahapan-tahapan yang rumit untuk memperoleh suatu file atau mentransfer suatu file.
FTP memfasilitasi tiap pengguna untuk melakukan transfer data secara dua arah. Artinya, jika FTP digunakan dalam sebuah perusahaan, maka setiap pemimpin perusahaan mampu mengirimkan file kepada karyawannya dan sebaliknya, dengan menggunakan server yang sama.
Progress perpindahan data tidak akan hilang walaupun sambungan terputus.
Transer data/file dapat dilakukan dengan mudah dan terorganisir.
Selain mempunyai manfaat yang besar dalam pertukaran data, FTP juga memiliki beberapa kekurangan, misalnya saja :

Sistem FTP sudah cukup tua, jika seseorang tidak memiliki background IT atau gaptek (orang yang belum familiar dengan dunia IT), akan sedikit sulit untuk menggunakannya.
Jika pengguna tidak begitu paham mengenai FTP, sangat mudah untuk menghapus keseluruhan data dengan sekali klik.
Tidak dapat mengubah kepemilikan dari suatu file.
Tidak begitu aman sebagai media transfer data karena tidak adanya enkripsi, kecuali jika menggunakan alternatif seperti SFTP.
Jika anda ingin memiliki FTP server sendiri, anda harus memiliki komputer server sendiri atau menyewa server dengan biaya yang tidak murah.
Cara Kerja FTP

Satu-satunya metode yang digunakan oleh FTP adalah metode autentikasi standar, dimana diperlukan username dan password untuk mengakses data-data yang ada pada FTP server. Pengguna yang terdaftar (memiliki username dan password) memiliki akses penuh pada beberapa direktori-direktori beserta file-file yang ada di dalamnya sehingga pengguna yang terdaftar tersebut dapat membuat, menyalin, memindahkan atau bahkan menghapus direktori-direktori tersebut.



Untuk cara kerjanya, secara umum terlebih dahulu FTP client harus meminta koneksi kepada FTP server, jika sudah terhubung dengan FTP server maka FTP client dapat melakukan pertukaran data seperti upload dan download data. FTP dapat bekerja dalam mode aktif dan mode pasif, yang menentukan bagaimana koneksi data terbentuk. Pada kedua mode, client membuat sebuah kontrol TCP dari port N menuju FTP server port 21.

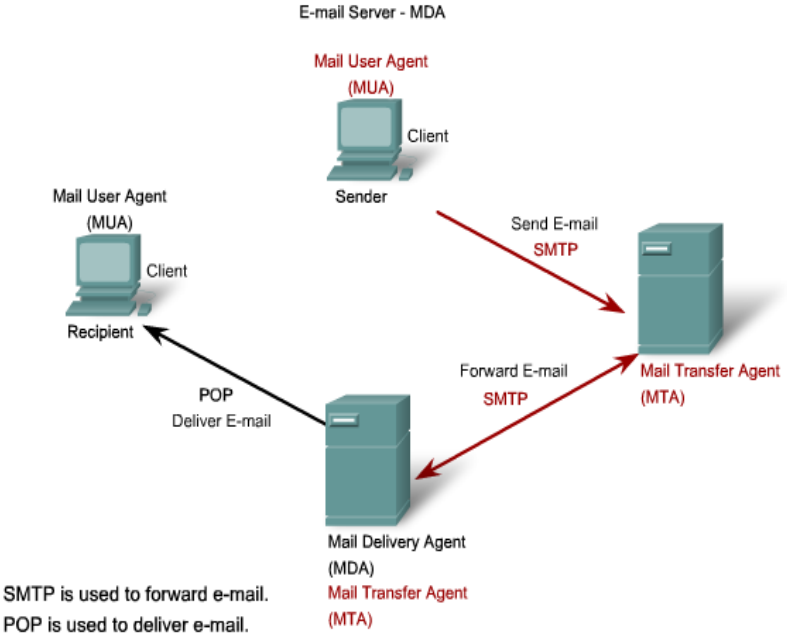
Pada mode aktif, client mulai menyimak koneksi data yang datang dari server pada port M. Kemudian client mengirimkan FTP command port M untuk menginformasikan kepada server, port mana yang harus disimak. Serverk emudian menginisiasi channel data kepada client dari port 20/ port FTP server.
Dalam situasi ketika client berada di balik firewall dan tidak mampu menerima koneksi TCP yang datang, dapat digunakan pasif mode. Dalam mode tersebut, client menggunakan kontrol koneksi untuk mengirimkan perintah PASV kepada server, kemudian menerima alamat IP server, alamat server, dan nomor port server.
Adakah alternatif untuk berbagai file?

Selain FTP, ada beberapa aplikasi lain yang digunakan untuk berbagi atau transfer data, seperti Dropbox, Google Drive atau bisa juga menggunakan OneDrive. Antara FTP dan ketiga aplikasi tersebut memiliki kelebihan dan kekurangan masing-masing, seperti :

Lalu lintas jaringan : FTP atau SFTP melakukan enkripsi terhadap lalu lintas jaringan menggunakan SSL/TLS/SSH, sementara ketiga aplikasi tersebut hanya dapat melakukan enkripsi menggunakan SSL/TLS.
Eksistensi file : Pada FTP, sebuah file tidak mungkin dihapus menggunakan komputer atau perangkat elektronik lainnya yang hilang. Sementara ketiga aplikasi tersebut, file dapat dihapus dari perangkat yang hilang dengan menggunakan penghapusan jarak jauh (remote delete).
Verifikasi dua langkah : Untuk FTP, perlu software pihak ketiga untuk melakukan verifikasi 2 langkah, sementara pada ketiga aplikasi tersebut ada yang sudah terdapat fitur verifikasi dua langkah dan bisa anda gunakan kapanpun tanpa perlu menginstal software pihak ketiga.
Server : Jika pada FTP server harus diamankan dan dirawat oleh ahli IT, pada ketiga aplikasi tersebut, pengguna tidak perlu memusingkan keamanan dan pemeliharaan server (semua sudah diatur oleh aplikasi yang bersangkutan).

13.4. SMTP

Simple Mail Transfer Protocol (SMTP) adalah salah satu protokol yang umum digunakan untuk pengiriman surat elektronik di Internet.



Protokol ini digunakan untuk mengirimkan data dari komputer pengirim surat elektronik ke server surat elektronik penerima. Protokol ini timbul karena desain sistem surat elektronik yang mengharuskan adanya server surat elektronik yang menampung sementara, sampai surat elektronik diambil oleh penerima yang berhak.

SMTP bisa kita katakan sebagai Sebuah Kantor pos, yang pada dasarnya jika kita mengirim sebuah surat pastinya Surat itu akan dibawa Ke Gudang kantor pos untuk di lakukan penyortiran, Gudang inilah yang dimaksud dengan SMTP, Setelah dilakukan penyortiran maka surat siap untuk diantarkan ketujuan, tapi tidak proses tidak berhenti disini, Jadi surat ini akan dibawa oleh si kurir lalu si Kurir Meletakkanya di Kotak Pos yang biasa kita katakan sebagai PO BOX (PO BOX inilah

yang dimaksud dengan POP3) itulah penjelasan singkat tentang SMTP.

SMTP adalah protokol yang cukup sederhana, berbasis teks dimana protokol ini menyebutkan satu atau lebih penerima email untuk kemudian diverifikasi. Jika penerima email valid, maka email akan segera dikirim. SMTP menggunakan port 25 dan dapat dihubungi melalui program telnet. Agar dapat menggunakan SMTP server lewat nama domain, maka record DNS (Domain Name Server) pada bagian MX (Mail Exchange) digunakan.

Setelah Membahas tentang SMTP, kali ini admin mau membagikan Daftar SMTP Provider yang ada di indonesia :

1. Telkomnet/Speedy: stmp.telkom.net
2. Fastnet/First Media/Kabelvision: mail.fast.net.id
3. Indosat: smtp.indosat.net.id
4. Biznet: smtp.biz.net.id
5. Net-zap: smtp.net-zap.com
6. Indonet: smtp.indo.net.id
7. Uninet: smtp.uninet.net.id
8. Linknet: mail1.link.net.id
9. CBN: smtp.cbn.net.id
10. Mynet: smtp.mynet.co.id
11. Jetcoms: smtp.jetcoms.net
12. NusaNet: smtp.nusa.net.id
13. Wasantara: jakarta.wasantara.net.id
14. Radnet: smtp.rad.net.id
15. MelsaNet: smtp.melsa.net.id
16. MitraNet: mail.mitra.net.id
17. Centrin: mail.centrin.net.id
18. VisionNet: pluto.vision.net.id
19. Infoasia: smtp.infoasia.net
20. Pacific: smtp.pacific.net.id
21. Dnet: dnet.net.id

14. Pertemuan 14

14.1. Broadband Network (SONET)

SONET adalah standar komunikasi digital yang baru untuk suatu sistem transmisi serat optik. Transport signal level-1 (STS-1) dengan frekuensi 51,840 Mbps dan multiplex SONET dibentuk dari sejumlah N kali sinyal dasar STS-1 sehingga lebih effisien dibandingkan hirarki yang lain. SONET juga dapat meningkatkan kapasitas bandwidth pada serat optik tanpa perlu melakukan penambahan kabel optik. Keandalan trafik pada SONET akan selalu terjaga pada topologi ring yang menggunakan wavelenght division multiplexing (WDM).
Synchronous Optical Network (SONET) atau Synchronous Digital Hierarchy (SDH) adalah standar protokol multiplexing yang mentransfer beberapa aliran bit digital lebih dari serat optik dengan menggunakan laser atau dioda pemancar cahaya (LED) atau bisa juga diartikan sebagai sebuah jaringan teknologi lapisan fisik dirancang untuk membawa volume besar lalu lintas jarak yang relatif lama pada kabel serat optik. SONET dan SDH prinsip kerjanya hampir sama karena menggunakan data rate yg sama.

SDH yang pertama didefinisikan sebagai standar untuk mentrasfer 1.5/2/6/34/45/140 Mbps dalam tingkat transmisi 155,52 Mbps dan sedang dikembangkan untuk membawa jenis lalu lintas lain, seperti modus transfer asinkron asynchronous transfer mode (ATM) dan Internet protocol (IP), diantara tingkat kelipatan bilangan bulat dari 155,52 Mbps. Unit dasar transmisi SONET adalah pada 51,84 Mbps, tetapi untuk membawa 140 Mbps, SDH saat ini dibedakan berdasarkan pada tiga waktu(yakni, 155,52 Mbps [155 Mbps]). Melalui pilihan-pilihan yang sesuai, subset dari SDH kompatibel dengan subset dari SONET; Oleh karena itu, memungkinkan terjadinya kepadatan interworking. Interworking untuk alarm dan kinerja manajemen pada umumnya tidak mungkin terjadi antara SDH dan SONET sistem. Hal ini hanya mungkin terjadi dalam beberapa kasus untuk beberapa fitur diantara penjual SDH dan sedikit lebih terjadi pada penjual SONET. Meskipun SONET dan SDH yang dikandung awalnya untuk transmisi serat optik,

SDH system radio yang ada di tingkat yang sesuai dengan kedua SONET dan SDH.

SONET didasarkan pada transmisi dengan kecepatan 51,840 Mbps kelipatan, atau STS-1 dan SDH didasarkan pada STM-1 yang memiliki data rate sebesar 155,52 Mbps, setara dengan STS-3. Tabel berikut berisi daftar hirarki SONET / SDH harga yang paling umum data:

SONET Sinyal	Bit Rate (Mbps)	SDH Sinyal	SONET Kapasitas	Kapasitas SDH
STSC1, OCC1	51.840	STMC0	28 DSC1s atau 1 DSC3	21 E1s
STSC3, OCC3	155.520	STMC1	84 DSC1s atau 3 DSC3s	63 E1s atau 1 E4
STSC12, OCC12	622.080	STMC4	336 DSC1s atau 12 DSC3s	252 E1s atau 4 E4s
STSC48, OCC48	2.488.320	STMC16	1.344 DSC1s atau 48 DSC3s	1.008 E1s atau 16 E4s
STSC192, OCC192	9.953.280	STMC64	5.376 DSC1s atau 192 DSC3s	4.032 E1s atau 64 E4s
STS-768, OC-768	39.813.120	STM-256	21.504 DSC1s atau 768 DSC3s	16.128 E1s atau 256 E4s

STS Level	OC Specification	Data Rate (Mbps)
1	OC-1	51.84
3	OC-3	155.52
9	OC-9	466.56
12	OC-12	622.08
18	OC-18	933.12
24	OC-24	1244.16
36	OC-36	1866.23
48	OC-48	2488.32
96	OC-96	4976.64
192	OC-192	9953.28

Pada kesimpulannya adalah:

SONET adalah hirarki antarmuka digital yang dipahami oleh Bellcore dan didefinisikan oleh ANSI untuk digunakan di Amerika Utara. SDH adalah node jaringan antarmuka network node interface (NNI) didefinisikan oleh CCITT / ITU-TS untuk digunakan di seluruh dunia dan digunakan oleh sebagian yang sesuai dengan SONET.

15. Pertemuan 15

DAFTAR PUSTAKA

1. Stallings, William, Data and Computer Communications, Macmillan Publishing Company, New York, 2013
2. E Comer, Douglas, Data and Communications Computer Network, Prentice Hall, 2000
3. Paper-paper terbaru tentang Jaringan Komputer Lanjut pada IEEE, Elsevier dan Springer
4. Computer Networking: A Top Down Approach 4th edition. Jim Kurose, Keith Ross Addison-Wesley, July 2007