



JARINGAN KOMPUTER

Kopetensi Dasar: Memahami Pengertian Jaringan Komputer, Koneksi peer to peer dan client-server, serta memahami defenisi LAN, MAN, WAN.

Tiga abad sebelum sekarang, masing-masing ditandai dengan dominasi yang berbeda. Abad ke-18 didominasi oleh perkembangan sistem mekanik yang mengiringi revolusi industri. Abad ke-19 merupakan jaman mesin uap. Abad ke-20, teknologi radio, tv dan komputer memegang peranan untuk pengumpulan, pengolahan dan media distribusi informasi. Abad ke-21 saat ini atau era-informasi, dimana teknologi jaringan komputer global yang mampu menjangkau seluruh wilayah dunia, pengembangan sistem dan teknologi yang digunakan, penyebaran informasi melalui media internet, peluncuran satelit-satelit komunikasi dan perangkat komunikasi wireless/selular menandai awal abad millenium.

Sejak me-masyarakat-nya internet dan dipasarkannya sistem operasi Windows95 oleh Microsoft Inc., menghubungkan beberapa komputer baik komputer pribadi (PC) maupun server dengan sebuah jaringan dari jenis LAN (*Local Area Network*) sampai WAN (*Wide Area Network*) menjadi sebuah hal yang mudah dan biasa. Demikian pula dengan konsep "downsizing" maupun "lightsizing" yang bertujuan menekan anggaran belanja (efisiensi anggaran) khususnya peralatan komputer, maka kebutuhan akan sebuah jaringan komputer merupakan satu hal yang tidak bisa terelakkan.

1.1 Pengertian Jaringan Komputer

Jaringan komputer adalah "interkoneksi" antara 2 komputer *autonomous* atau lebih, yang terhubung dengan media transmisi kabel atau tanpa kabel (wireless).

Autonomous adalah apabila sebuah komputer tidak melakukan kontrol terhadap komputer lain dengan akses penuh, sehingga dapat membuat komputer lain, restart, shutdowns, kehilangan file atau kerusakan sistem.

Dalam defenisi networking yang lain *autonomous* dijelaskan sebagai jaringan yang independent dengan manajemen sistem sendiri (punya admin sendiri), memiliki topologi jaringan, hardware dan software sendiri, dan dikoneksikan dengan jaringan *autonomous* yang lain. (Internet merupakan contoh kumpulan jaringan *autonomous* yang sangat besar.)

Dua unit komputer dikatakan terkoneksi apabila keduanya bisa saling bertukar data/informasi, berbagi resource yang dimiliki, seperti: file, printer, media penyimpanan (hardisk, floppy disk, cd-rom, flash disk, dll). Data yang berupa teks, audio maupun video, bergerak melalui media kabel atau tanpa kabel (wireless) sehingga memungkinkan pengguna komputer dalam jaringan komputer dapat saling bertukar file/data, mencetak pada printer yang sama dan menggunakan hardware/software yang terhubung dalam jaringan bersama-sama

Tiap komputer, printer atau periferal yang terhubung dalam jaringan disebut dengan "node". Sebuah jaringan komputer sekurang-kurangnya terdiri dari dua unit komputer atau lebih, dapat berjumlah puluhan komputer, ribuan atau bahkan jutaan node yang saling terhubung satu sama lain.

Didalam jaringan komputer dikenal sistem koneksi antar node (komputer), yakni:



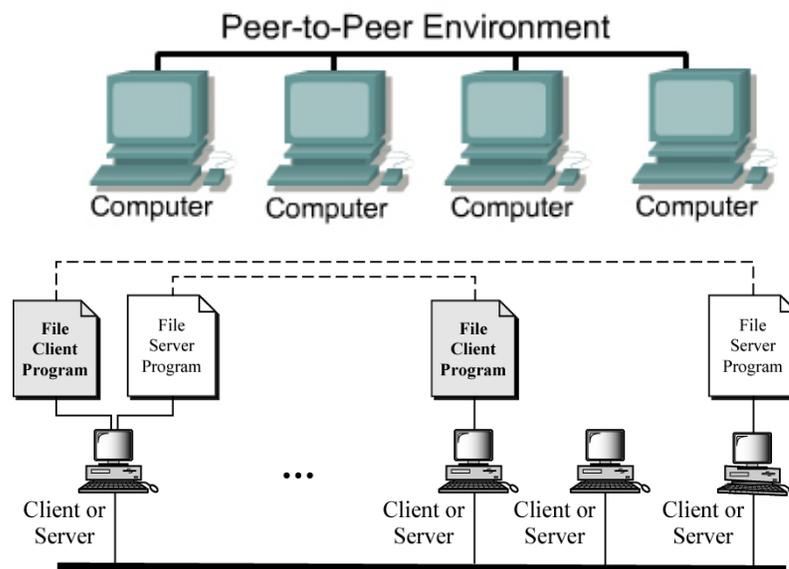
1.1.1 Peer to peer

Peer artinya rekan sekerja. Peer-to-peer network adalah jaringan komputer yang terdiri dari beberapa komputer, terhubung langsung dengan kabel crossover atau wireless atau juga dengan perantara hub/switch.

Komputer pada jaringan peer to peer ini biasanya berjumlah sedikit dengan 1-2 printer. Untuk penggunaan khusus, seperti laboratorium komputer, riset dan beberapa hal lain, maka model peer to peer ini bisa saja dikembangkan untuk koneksi lebih dari 10 hingga 100 komputer.

Peer to peer adalah suatu model dimana tiap PC dapat memakai resource pada PC lain atau memberikan resource-nya untuk dipakai PC lain, Tidak ada yang bertindak sebagai server yang mengatur sistem komunikasi dan penggunaan resource komputer yang terdapat di jaringan, dengan kata lain setiap komputer dapat berfungsi sebagai client maupun server pada periode yang sama.

Misalnya terdapat beberapa unit komputer dalam satu departemen, diberi nama group sesuai dengan departemen yang bersangkutan. Masing-masing komputer diberi alamat IP dari satu kelas IP yang sama agar bisa saling sharing untuk bertukar data atau resource yang dimiliki komputer masing-masing, seperti printer, cdrom, file dan lain-lain.



Gambar 1.1. Peer to peer

1.1.2 Client - Server

Client Server merupakan model jaringan yang menggunakan satu atau beberapa komputer sebagai server yang memberikan resource-nya kepada komputer lain (client) dalam jaringan, server akan mengatur mekanisme akses resource yang boleh digunakan, serta mekanisme komunikasi antar node dalam jaringan.

Selain pada jaringan lokal, sistem ini bisa juga diterapkan dengan teknologi internet. Dimana ada suatu unit komputer) berfungsi sebagai server yang hanya memberikan pelayanan bagi komputer lain, dan client yang juga hanya meminta layanan dari server. Akses dilakukan secara transparan dari client dengan melakukan login terlebih dulu ke server yang dituju.

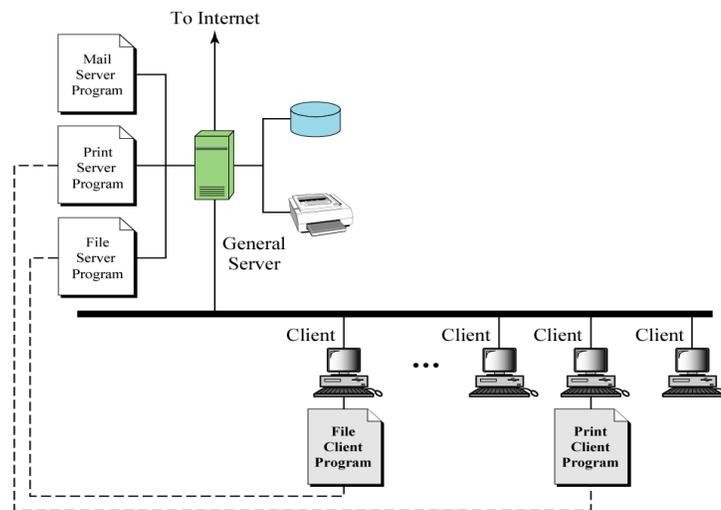




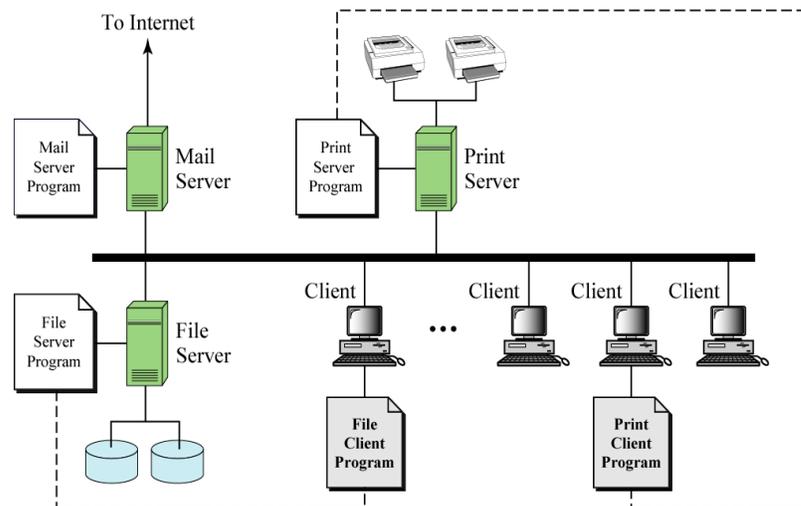
Client hanya bisa menggunakan resource yang disediakan server sesuai dengan otoritas yang diberikan oleh administrator. Aplikasi yang dijalankan pada sisi client, bisa saja merupakan resource yang tersedia di server. namun hanya bisa dijalankan setelah terkoneksi ke server. Pada implementasi software aplikasi yang di-install disisi client berbeda dengan yang digunakan di server.

Jenis layanan Client-Server antara lain :

- ❖ **File Server** : memberikan layanan fungsi pengelolaan file.
- ❖ **Print Server** : memberikan layanan fungsi pencetakan.
- ❖ **Database Server** : proses-proses fungsional mengenai database dijalankan pada mesin ini dan stasiun lain dapat minta pelayanan.
- ❖ **DIP (Document Information Processing)** : memberikan pelayanan fungsi penyimpanan, manajemen dan pengambilan data.



Gambar 1.2. Model Client-Server dengan sebuah Server yang berfungsi umum





Gambar 1.3. Model Client-Server dengan Dedicated Server

1.1.3 Kelebihan jaringan peer to peer

- ✓ Implementasinya murah dan mudah
- ✓ Tidak memerlukan software administrasi jaringan yang khusus
- ✓ Tidak memerlukan administrator jaringan

1.1.4 Kekurangan jaringan peer to peer

- ✓ Jaringan tidak bisa terlalu besar (tidak bisa memperbesar jaringan)
- ✓ Tingkat keamanan rendah
- ✓ Tidak ada yang memajemen jaringan
- ✓ Pengguna komputer jaringan harus terlatih mengamankan komputer masing-masing
- ✓ Semakin banyak mesin yang disharing, akan mempengaruhi kinerja komputer

1.1.5 Kelebihan jaringan client server

- ✓ Mendukung keamanan jaringan yang lebih baik
- ✓ Kemudahan administrasi ketika jaringan bertambah besar
- ✓ Manajemen jaringan terpusat
- ✓ Semua data bisa disimpan dan di backup terpusat di satu lokasi

1.1.6 Kekurangan jaringan client server

- ✓ Butuh administrator jaringan yang profesional
- ✓ Butuh perangkat bagus untuk digunakan sebagai komputer server
- ✓ Butuh software tool operasional untuk mempermudah manajemen jaringan
- ✓ Anggaran untuk manajemen jaringan menjadi besar
- ✓ Bila server down, semua data dan resource diserver tidak bisa diakses

1.2 Jaringan Komputer dan Sistem Terdistribusi

Sebelum jaringan komputer populer, user komputer pernah mengenal sistem terdistribusi. Terdapat hal yang cukup membingungkan dalam pemakaian istilah jaringan komputer dan sistem terdistribusi (distributed system).

Persamaannya adalah keduanya merupakan sekumpulan komputer yang saling terkoneksi dengan dengan media transmisi yang relatif tidak jauh berbeda, sama-sama harus memindahkan file. Perbedaan yang lebih spesifik antara Jaringan Komputer dan Sistem Distribusi sbb:





Tabel 1.1. Perbedaan Jaringan Komputer & Sistem Terdistribusi

JARINGAN KOMPUTER	SISTEM TERDISTRIBUSI
Komputer yang terhubung merupakan gabungan yang terdiri dari beberapa workstation atau juga gabungan komputer server dan client	Komputer yang terhubung terdiri dari host (komputer utama) dan terminal-terminal (komputer yang terhubung dengan komputer host)
Beberapa komputer terhubung agar dapat sharing, namun tiap pekerjaan ditangani sendiri sendiri oleh komputer yang meminta dan dimintai layanan. Server hanya melayani permintaan sesuai antrian yang sudah diatur sistem.	Beberapa host komputer terhubung agar dapat mengerjakan sebuah atau beberapa pekerjaan besar bersama. Host melayani beberapa terminal dan melakukan proses berdasarkan input dari terminal-terminal
Kualitas komunikasi data dipengaruhi oleh media transmisi yang digunakan. Lamanya suatu proses dipengaruhi oleh spesifikasi hardware masing-masing station yg meminta layanan. User dapat mengetahui proses yang sedang berlangsung (di komp station atau di server).	Kualitas komunikasi data dipengaruhi oleh sistem. Lamanya suatu proses tergantung Sistem Operasi yang akan memilih prosesor komputer mana yang akan digunakan. User tidak dapat mengetahui proses yang sedang berlangsung di host.
Metode komunikasi antar komputer dengan model Peer to Peer atau Client Server .	Metode komunikasi antar komputer tersentralisasi (terpusat pada komputer utama/host)
Masing-masing node atau workstation (pada metode peer to peer) tidak membutuhkan komputer server khusus untuk menangani seluruh pekerjaan. Antar node bisa saling bertukar file atau resource yang dimiliki, sesuai keinginan/permission yg diatur pemilik komputer.	Masing-masing terminal membutuhkan host (komputer utama) untuk dapat aktif melakukan pekerjaan dan berkomunikasi dengan terminal lain. Antar terminal tidak dapat saling sharing file atau resource tanpa campur tangan host (supervisor host).
Masing-masing user disetiap workstation (client) sadar betul akan proses yang sedang terjadi apabila ia meminta layanan atau mengirimkan data keserver. User secara eksplisit (nyata) harus "login" pada server, kalau ingin memanfaatkan resource yang dimiliki oleh server. Secara eksplisit menyampaikan tugasnya dari jauh, secara eksplisit memindahkan file-file, namun secara umum menangani sendiri seluruh manajemen jaringan.	Masing-masing user disetiap terminal tidak dapat menyadari proses yang berlangsung pada sistem User tidak perlu melakukan pekerjaan secara eksplisit, karena semua proses dan manajemen dilakukan/ ditangani secara otomatis oleh sistem tanpa diketahui user. Meskipun secara umum seorang user pada tiap terminal juga harus login untuk bisa memanfaatkan resource host.
Tiap user memiliki identitas & password yang unik untuk dapat login serta menggunakan resource yang terdapat di server. Umumnya user tidak bisa menggunakan ID yang sama, untuk login ke server, namun policy seorang Admin dapat merubah aturan ini agar sebuah ID dapat digunakan bersama-sama secara terbatas.	Tiap user juga memiliki ID dan password untuk dapat login ke host & menggunakan resource yang disediakan. Umumnya beberapa terminal dapat menggunakan ID yang sama untuk login ke komp host, namun Admin/Supervisor sistem dapat merubah dengan hanya mengijinkan satu ID untuk tiap terminal.





Keberadaan sejumlah komputer dalam jaringan tidak harus transparan disatu lokasi, sehingga secara fisik tidak dapat dilihat oleh user lain yang berada dalam jaringan.	Keberadaan sebuah atau sejumlah komputer atau terminal autonomus, bersifat transparan (jelas) bagi user, biasanya berada dalam suatu area lokasi.
Spesifikasi hardware server tidak harus lebih baik dari hardware client	Spesifikasi hardware host (komputer utama) harus lebih baik dari terminal.
Merupakan sistem yang menggabungkan kinerja perangkat dan aplikasi dari physical layer sampai dengan application layer	Merupakan suatu sistem perangkat lunak yang dibuat dan bekerja pada lapisan atas sebuah sistem jaringan.

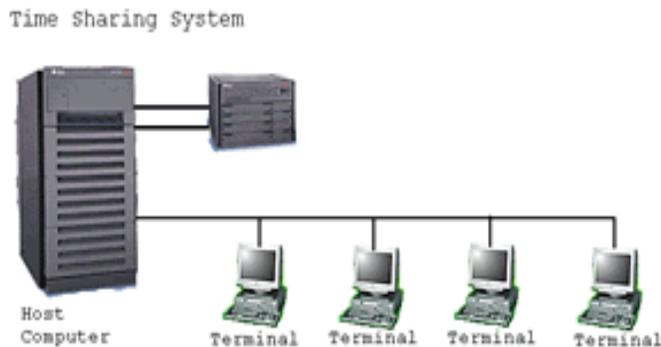
Perbedaan utama antara jaringan komputer dan sistem terdistribusi lebih terletak pada perangkat lunaknya (khususnya sistem operasi) bukan pada perangkat kerasnya, karena perangkat lunaklah yang menentukan tingkat keterpaduan dan transparansi jaringan yang bersangkutan.

1.3 Sejarah Jaringan & Internet

1.3.1 Jaringan Komputer

Ditahun 1950-an ketika jenis komputer mulai membesar sampai terciptanya super komputer, maka sebuah komputer mesti melayani beberapa terminal. (Lihat Gambar 1.4) Untuk itu ditemukan konsep distribusi proses berdasarkan waktu yang dikenal dengan nama TSS (*Time Sharing System*), dan untuk pertama kali terbentuklah jaringan (network) komputer pada lapis aplikasi.

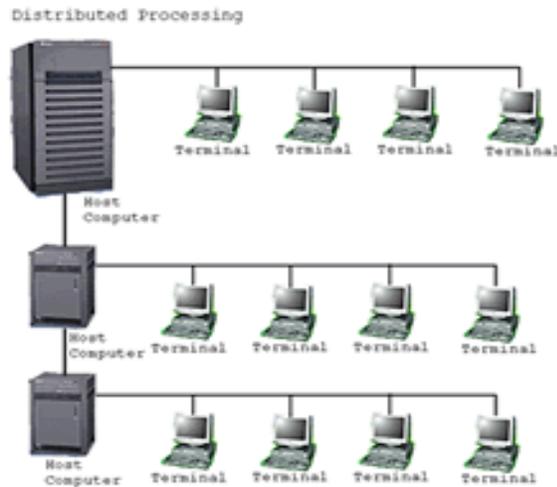
Pada sistem TSS beberapa terminal terhubung ke sebuah host komputer. Dalam proses TSS mulai nampak perpaduan teknologi komputer dan teknologi telekomunikasi yang pada awalnya berkembang sendiri-sendiri.



Gambar 1.4. Jaringan komputer model TSS.

Pada tahun 1957 Advanced Research Projects Agency (ARPA) dibentuk oleh Departement of Defence (DoD) USA, 1967 disain awal dari ARPANET diterbitkan dan tahun 1969 DoD menggelar pengembangan ARPANET dengan mengadakan riset untuk menghubungkan sejumlah komputer sehingga membentuk jaringan organik (program ini dikenal dengan nama ARPANET).





Gambar 1.5. Jaringan komputer model distributed processing.

Seperti pada Gambar diatas, dalam proses ini beberapa host komputer mengerjakan sebuah pekerjaan besar secara seri untuk melayani beberapa terminal yang tersambung secara paralel disetiap host komputer. Pada proses distribusi sudah mutlak diperlukan perpaduan yang mendalam antara teknologi komputer dan telekomunikasi, karena selain proses yang harus didistribusikan, semua host komputer wajib melayani terminal-terminalnya dalam satu perintah dari komputer pusat.

Selanjutnya ketika harga-harga komputer kecil sudah mulai menurun dan konsep proses distribusi sudah matang, maka penggunaan komputer dan jaringannya sudah mulai beragam, dari mulai menangani proses bersama-sama maupun komunikasi antar komputer (*Peer to Peer System*) tanpa melalui kendali komputer pusat. Untuk itu mulailah berkembang teknologi jaringan lokal yang dikenal dengan sebutan LAN. Demikian pula ketika Internet mulai diperkenalkan, maka sebagian besar LAN yang berdiri sendiri mulai berhubungan satu sama lain, hingga terbentuklah jaringan raksasa WAN.

1.3.2 Sejarah Singkat Internet dan Web

- 1957:** Advanced Research Projects Agency (ARPA) dibentuk oleh Departement of Defence (DoD) USA.
- 1959:** Len Kleinrock menulis paper tentang packet switching.
- 1967:** Disain awal dari ARPANET diterbitkan.
- 1969:** DoD menggelar pengembangan ARPANET
- 1970:** ARPANET mulai menggunakan Network Control Protocol (NCP)
- 1972:** InterNetworking Working Group(INWG) dibentuk untuk mempromosikan standar yang sudah disepakati bersama. Spesifikasi dari telnet, diusulkan.
- 1973:** Ide ethernet dijabarkan dalam thesis PhD dari Bob Metcalfe. Spesifikasi untuk File Transfer, RFC 454, diusulkan.
- 1974:** Disain dari TCP/IP dijabarkan secara rinci oleh Vint Cerf dan Bob Kahn dalam "A Protocol for Packet Network Intercommunication".
- 1982:** TCP/IP menjadi protokol untuk ARPANET dan ini dispesifikasikan oleh DoD.





1992: Jumlah Internet hosts melampaui 1.000.000. Tim Berners Lee menemukan program editor dan browser. University of Nevada mengeluarkan sistem Veronica. Sebuah WWW browser yang bernama Viola diluncurkan oleh Pei Wei dan didistribusikan bersama CERN WWW.

1993: NSF membuat InterNIC untuk menjalankan Internet service seperti pendaftaran domain. Versi pertama dari Mosaic (untuk X Window) yang dikembangkan oleh Marc Andreessen dikeluarkan oleh NCSA White House online. National Information Infrastructure Act lolos dan pemerintah Amerika Serikat mulai lebih serius dalam penanganan Website.

1994: PizzaHut online, merupakan contoh pertama dari aplikasi komersial Internet. Spam mail menjadi kasus besar setelah sebuah lembaga hukum yang bernama Canter & Siegel menyebarkan mail ke seluruh dunia tentang servis untuk mendapatkan "green card". First Virtual menjalankan "CyberBank" yang pertama. Ditahun 1994 ini **Yahoo!** didirikan dan juga menjadi tahun kelahiran Netscape Navigator 1.0.

1995: Compuserve, America Online, dan Prodiy mulai memberikan servis akses keInternet. Perusahaan Marc Andreessen, Netscape Communication Corporation, menjadi publik dan menjadi nomor 3 tertinggi untuk harga Initial Public Offericng (IPO) share di NASDAQ. NFS tidak lagi meng-gratiskan pendaftaran domain. Pengguna domain mulai membayar untuk sebuah domain yang digunakan dan dihosting ke internet.

1.4 Tujuan / Manfaat Jaringan Komputer

Manfaat jaringan komputer bagi user dapat dikelompokkan menjadi dua, yaitu: untuk kebutuhan perusahaan, dan jaringan untuk umum.

Tujuan utama dari terbangunnya sebuah jaringan pada suatu perusahaan adalah:

Resource sharing yang bertujuan agar seluruh program, peralatan, khususnya data dapat digunakan oleh setiap orang yang ada pada jaringan.

Saving Money (Penghematan uang/anggaran): Perangkat dan data yang dapat dishare akan membuat penghematan anggaran yang cukup besar, karena tidak perlu membeli perangkat baru untuk dipasang ditiap-tiap unit komputer

High reliability (kehandalan tinggi): Sistem Informasi Manajemen Kantor Terpadu atau Sistem Pelayanan Satu Atap dengan teknologi client-server, internet maupun intranet dapat diterapkan pada jaringan komputer, sehingga dapat memberikan pelayanan yang handal, cepat dan akurat sesuai kebutuhan dan harapan.

Manfaat jaringan komputer untuk umum:

Jaringan komputer akan memberikan layanan yang berbeda kepada pengguna di rumah-rumah dibandingkan dengan layanan yang diberikan pada perusahaan. Terdapat tiga hal pokok yang mejadi daya tarik jaringan komputer pada perorangan yaitu:

- access ke informasi yang berada di tempat lain (seperti akses berita terkini, info e-government, e-commerce atau e-business, semuanya up to date).
- komunikasi person to person (seperti e-mail, chatting, video conferene dll).
- hiburan interaktif (seperti nonton acara tv on-line, radio streaming, download film atau lagu, dll).





1.5 Masalah-masalah sosial yang ditimbulkan dari Jaringan Komputer (internet)

Penggunaan jaringan oleh masyarakat luas akan menyebabkan timbulnya masalah-masalah sosial, etika, politik, maupun ekonomi yang tak terelakkan. Internet telah masuk ke segala penjuru kehidupan masyarakat, semua orang dapat memanfaatkannya tanpa memandang status sosial, usia, juga jenis kelamin.

Penggunaan internet tidak akan menimbulkan masalah selama subyeknya terbatas pada topik-topik teknis, pendidikan atau hobi, juga hal-hal yang masih dalam batas norma-norma kehidupan, tetapi kesulitan mulai muncul bila suatu situs di internet mempunyai topik yang sangat menarik perhatian orang, seperti pertentangan politik, agama, sex, dll.

Koneksi jaringan komputer/internet ini juga akan menimbulkan masalah ekonomi yang serius bila teknologinya dimanfaatkan oleh pihak-pihak tertentu yang ingin mengambil keuntungan pribadi namun merugikan pihak lain, misalnya kegiatan carding, download software komersil secara ilegal dll.

Gambar-gambar yang dipasang disitus-situs internet mungkin merupakan sesuatu yang biasa bagi sebahagian orang, namun sangat mengganggu bagi sebagian orang lain (karena bisa menimbulkan masalah SARA).

Selain itu, bentuk pesan-pesan tidaklah terbatas hanya pesan tekstual saja. Foto berwarna dengan resolusi tinggi dan bahkan videoclip singkatpun sekarang sudah dapat dengan mudah disebar-luaskan melalui jaringan komputer.

Sebagian orang dapat bersikap acuh tak acuh, tapi bagi sebagian lainnya pemasangan materi tertentu (misalnya pornografi) merupakan sesuatu yang tidak dapat diterima.

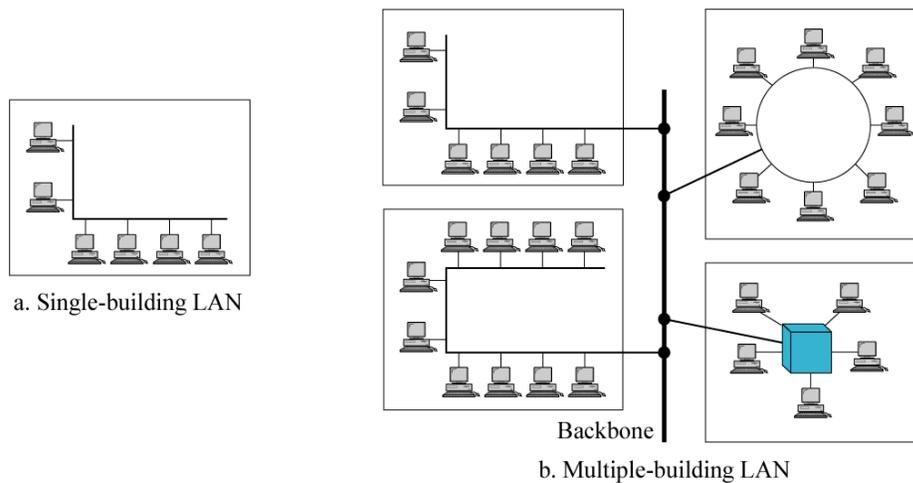
1.6 Jenis-Jenis jaringan

Secara umum jaringan komputer terbagi menjadi 3 jenis jaringan yaitu :

1.6.1 Local Area Network (LAN)

Sebuah LAN, adalah jaringan yang dibatasi oleh area yang relatif kecil, umumnya dibatasi oleh area lingkungan, seperti sebuah kantor pada sebuah gedung, atau tiap-tiap ruangan pada sebuah sekolah. Biasanya jarak antar node tidak lebih jauh dari sekitar 200 m.

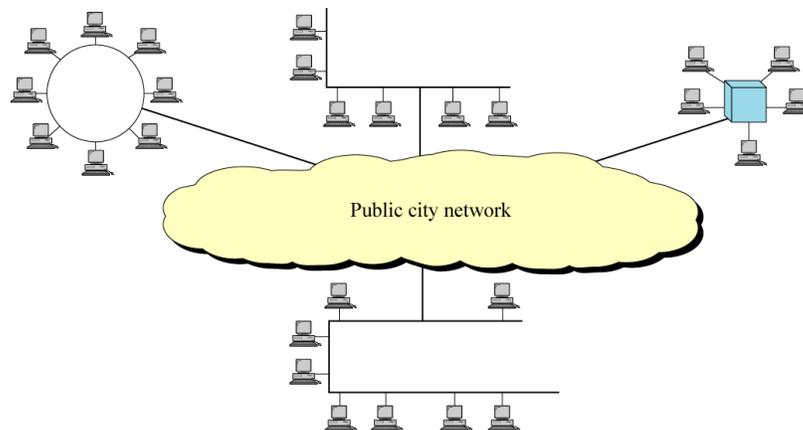




Gambar 1.6. Local Area Network (LAN)

1.6.2 Metropolitan Area Network (MAN)

Sebuah MAN, biasanya meliputi area yang lebih besar dari LAN, misalnya antar gedung dalam suatu daerah (wilayah seperti propinsi atau negara bagian). Dalam hal ini jaringan menghubungkan beberapa buah jaringan kecil ke dalam lingkungan area yang lebih besar, sebagai contoh yaitu: jaringan beberapa kantor cabang sebuah bank didalam sebuah kota besar yang dihubungkan antara satu dengan lainnya.



Gambar 1.7. Metropolitan Area Network

1.6.3 Wide Area Network (WAN)

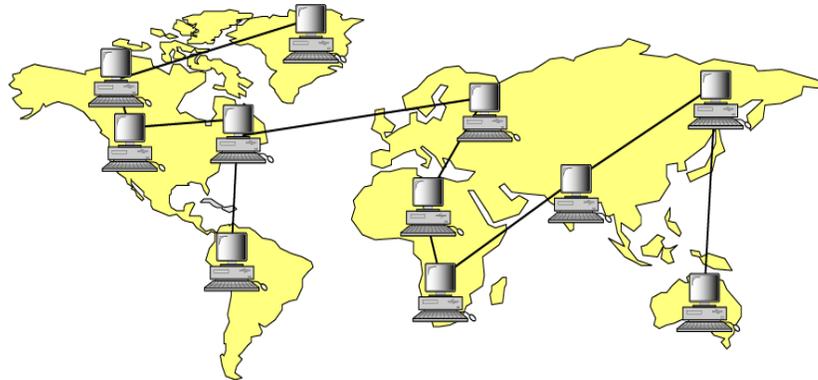
Wide Area Network (WAN) adalah jaringan yang biasanya sudah menggunakan media wireless, sarana satelit ataupun kabel serat optic, karena jangkauannya yang lebih luas, bukan hanya meliputi satu kota atau antar kota dalam suatu wilayah, tetapi mulai menjangkau area/wilayah otoritas negara lain.





Sebagai contoh jaringan komputer kantor City Bank yang ada di Indonesia ataupun yang ada di negara lain, yang saling berhubungan, jaringan ATM Master Card, Visa Card atau Cirrus yang tersebar diseluruh dunia dan lain-lain.

Biasanya WAN lebih rumit dan sangat kompleks bila dibandingkan LAN maupun MAN. Menggunakan banyak sarana untuk menghubungkan antara LAN dan WAN kedalam komunikasi global seperti internet, meski demikian antara LAN, MAN dan WAN tidak banyak berbeda dalam beberapa hal, hanya lingkup areanya saja yang berbeda satu diantara yang lainnya.



Gambar 1.8. Wide Area Network

Tabel 1.2. Interkoneksi berdasarkan jarak antar node

Distance Between CPUs	Location of CPUs	Name
0.1 m	Printed circuit board Personal data asst.	Motherboard Personal area network (PAN)
1.0 m	Millimeter Mainframe	Computer systems network
10 m	Room	Local area network (LAN) Your classroom
100 m	Building	Local area network (LAN) Your school
1000 m = 1 km	Campus	Local area network (LAN) Stanford University
100,000 m = 100 km	Country	Wide area network (WAN) Cisco Systems, Inc.
1,000,000 m = 1,000 km	Continent	Wide area network (WAN) Africa
10,000,000 m = 10,000 km	Planet	Wide area network (WAN) The Internet
100,000,000 m = 100,000 km	Earth-moon system	Wide area network (WAN) Earth and artificial satellites





Nilai-nilai yang terdapat pada tabel diatas, bukan merupakan nilai mutlak bagi jarak yang menghubungkan antar komputer, karena jarak tersebut bisa saja lebih pendek tergantung kondisi area suatu wilayah.

1.7 Rangkuman

Jaringan komputer (jarkom) adalah "interkoneksi" antara 2 komputer *autonomous* atau lebih, yang terhubung dengan media transmisi kabel atau tanpa kabel (wireless).

Dua unit komputer dikatakan terkoneksi apabila keduanya bisa saling bertukar data/informasi, berbagi resource yang dimiliki, seperti: file, printer, media penyimpanan (hardisk, floppy disk, cd-rom, flash disk, dll).

Tiap komputer, printer atau periferal yang terhubung dalam jaringan disebut dengan "node". Sebuah jaringan komputer sekurang-kurangnya terdiri dari dua unit komputer atau lebih.

Peer to peer adalah suatu model dimana tiap PC dapat memakai resource pada PC lain atau memberikan resourcenya untuk dipakai PC lain, Tidak ada yang bertindak sebagai server yang mengatur sistem komunikasi dan penggunaan resource komputer yang terdapat di jaringan, dengan kata lain setiap komputer dapat berfungsi sebagai client maupun server pada periode yang sama.

Client Server merupakan model jaringan yang menggunakan satu atau beberapa komputer sebagai server yang memberikan resource-nya kepada komputer lain (client) dalam jaringan.

1.8 Soal Latihan :

1. Jelaskan tentang pengertian jaringan komputer dan autonomous ?
2. Apa yang membedakan antara jaringan komputer dan sistem terdistribusi?
3. Apa manfaat jaringan komputer bagi sebuah perusahaan?
4. Masalah apa yang bisa ditimbulkan dari terbentuknya jaringan komputer global (internet)?
5. Jelaskan jenis-jenis jaringan komputer yang anda ketahui?

Multiple choise:

1. Ketika sebuah komputer dapat membuat komputer lain restart, shutdown, atau melakukan kontrol lainnya secara penuh, maka hal ini disebut dengan :
 - a. Jaringan komputer
 - b. Sistem Terdistribusi
 - c. Autonomous
 - d. Non-Autonomous
2. Komputer yang terhubung terdiri dari host (komputer utama) dan terminal-terminal (komputer yang terhubung dengan komputer host), merupakan ciri:
 - a. Jaringan komputer
 - b. Sistem Terdistribusi
 - c. Autonomous
 - d. Non-Autonomous
3. Metode komunikasi antar komputer dengan model Peer to Peer atau Client Server, terdapat pada:
 - a. Jaringan komputer
 - b. Sistem Terdistribusi
 - c. Autonomous
 - d. Non-Autonomous
4. Bila tiap PC yang terdapat pada jaringan dapat memakai resource PC lain atau memberikan resourcenya untuk dipakai PC lain, dengan kata lain dapat berfungsi sebagai client maupun server pada periode yang sama, maka hal ini disebut dengan:
 - a. Autonomous
 - b. Peer to peer
 - c. Client Server
 - d. Non-Sharing
5. Bila pada sebuah jaringan terdapat komputer yang hanya berfungsi sebagai server dan beberapa komputer lain hanya berfungsi sebagai client, maka hal ini merupakan metode:





- a. Remote Admin
- b. Peer to peer
- c. Client Server
- d. Sharing

DAFTAR PUSTAKA

Cisco, Materi CCNA 1, v.31

Introduction About Network, Mc Graw Hill Companies, Inc. 2003

Jaringan Komputer Edisi Bahasa Indonesia Jilid 1 Pearson Education Asia Pte. Ltd, Andrew S. Tanenbaum, Prentice-Hall Inc. 1996,

Jaringan Komputer, Lukas Tanutama, Elexmedia komputindo 2000

Pengantar Jaringan Komputer, Melwin Syafrizal, Andi Offset, Jogja, 2005

Pengantar Local Area Network, Robert M. Thomas, Elexmedia komputindo, 1999



MENGENAL HARDWARE DAN TOPOLOGI JARINGAN KOMPUTER

Kompetensi Dasar : Memahami topologi jaringan dan mengenal hardware jaringan LAN, Mampu memasang konektor RJ-45 pada kabel UTP dan menguji kualitas kabel UTP straight through dan crossover.

2.1 Hardware Jaringan





Membangun suatu jaringan, baik itu bersifat LAN (Local Area Network) maupun WAN (Wide Area Network), kita membutuhkan media baik hardware maupun software. Beberapa media hardware yang penting didalam membangun suatu jaringan, seperti: kabel atau perangkat Wi-Fi, ethernet card, hub atau switch, repeater, bridge atau router, dll.

2.1.1 Kabel

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

Perlu diingat bahwa hampir 85% kegagalan yang terjadi pada jaringan komputer disebabkan karena adanya kesalahan pada media komunikasi yang digunakan termasuk kabel dan konektor serta kualitas pemasangannya. Kegagalan lainnya bisa disebabkan faktor teknis dan kondisi sekitar.

Setiap jenis kabel mempunyai kemampuan dan spesifikasinya yang berbeda, oleh karena itu dibuatlah pengenalan tipe kabel. Ada dua jenis kabel yang dikenal secara umum dan sering dipakai untuk LAN, yaitu *coaxial* dan *twisted pair* (UTP *unshielded twisted pair* dan STP *shielded twisted pair*).

2.1.1.1 Coaxial Cable

Dikenal dua jenis tipe kabel koaksial yang dipergunakan buat jaringan komputer, yaitu:

- *thick coax* (mempunyai diameter lumayan besar) dan
- *thin coax* (mempunyai diameter lebih kecil).

2.1.1.1.1 Thick coaxial cable (kabel koaksial “gemuk”)

Kabel coaxial jenis ini dispesifikasikan berdasarkan standar IEEE 802.3 - 10BASE5, dimana kabel ini mempunyai diameter rata-rata 12mm. Kabel jenis ini biasa disebut sebagai *standard ethernet* atau *thick ethernet*, atau hanya disingkat *ThickNet*, atau bahkan cuma disebut sebagai *yellow cable* karena warnanya yang kuning.

Kabel Coaxial ini jika digunakan dalam jaringan mempunyai spesifikasi dan aturan sebagai berikut::

- Setiap ujung harus diterminasi dengan terminator 50-ohm (dianjurkan menggunakan terminator yang sudah dirakit, bukan menggunakan satu buah resistor 50 ohm 1 watt, sebab resistor mempunyai disipasi tegangan yang lumayan lebar).
- Maksimum 3 segment dengan tambahan peralatan (*attached devices, seperti repeater*) atau berupa *populated segments (seperti bridge)*.
- Setiap kartu jaringan mempunyai kemampuan penguat sinyal (*external transceiver*).
- Setiap segment maksimum berisi 100 perangkat jaringan, termasuk dalam hal ini *repeaters*.
- Maksimum panjang kabel per segment adalah 1.640 feet (sekitar 500m).
- Maksimum jarak antar segment adalah 4.920 feet (atau sekitar 1500 meter) dan setiap segment harus diberi ground.
- Jarak maksimum antara *tap* atau pencabang dari kabel utama ke perangkat (*device*) adalah 16 feet (sekitar 5 meter).
- Jarak minimum antar *tap* adalah 8 feet (sekitar 2,5 meter).





2.1.1.1.2 Thin coaxial cable (kabel koaksial “kurus”)

Kabel coaxial jenis ini banyak dipergunakan di kalangan radio amatir, terutama untuk transceiver yang tidak memerlukan output daya yang besar. Jenis yang banyak digunakan RG-8 atau RG-59 dengan impedansi 75 ohm. Jenis kabel untuk televisi juga termasuk jenis coaxial dengan impedansi 75 ohm.

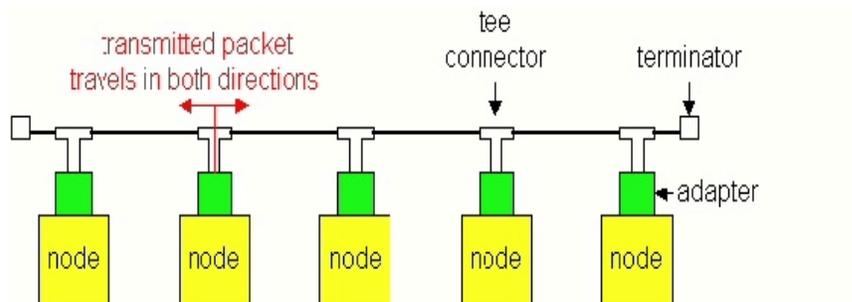
Namun untuk perangkat jaringan, kabel jenis coaxial yang dipergunakan adalah (**RG-58**) yang telah memenuhi standar IEEE 802.3 - 10BASE2, dimana diameter rata-rata berkisar 5 mm dan biasanya berwarna hitam. Setiap perangkat (*device*) dihubungkan dengan BNC T-*connector*. Kabel jenis ini juga dikenal sebagai *thin Ethernet* atau *ThinNet*.

Kabel coaxial jenis ini, misalnya jenis RG-58 A/U atau C/U, jika di-implementasikan dengan T-*connector* dan *terminator* dalam sebuah jaringan, harus mengikuti aturan sebagai berikut:

- Pada topologi bus, setiap ujung kabel diberi terminator 50-ohm.
- Panjang maksimal kabel adalah 606.8 feet (185 meter) per segment.
- Setiap segment maksimum terkoneksi sebanyak 30 perangkat jaringan (*devices*)
- Kartu jaringan sudah menggunakan *transceiver* yang *onboard*, tidak perlu tambahan *transceiver*, kecuali untuk *repeater*.
- Maksimum ada 3 segment terhubung satu sama lain (*populated segment*) dengan penghubung *repeater* $185 \times 3 = 555$ meter.
- Setiap segment sebaiknya dilengkapi 1 ground.
- Panjang minimum antar T-Connector adalah 1,5 feet (0.5 meter).



Gambar 2.1. Kabel koaksial yang telah dipasang konektor, terminator dan BNC T



Gambar 2.2. Model jaringan Ethernet BUS





2.1.1.2 Twisted Pair Cable

Selain kabel koaksial, Ethernet juga dapat menggunakan jenis kabel lain yakni UTP (Unshielded Twisted Pair) dan Shielded Twisted Pair (STP). Kabel UTP atau STP yang biasa digunakan adalah kabel yang terdiri dari 4 pasang kabel yang terpilin.

Dari 8 buah kabel yang ada pada kabel ini, hanya digunakan 4 buah saja yang digunakan untuk dapat mengirim dan menerima data (Ethernet).

Perangkat-perangkat lain yang berkenaan dengan penggunaan jenis kabel ini adalah konektor RJ-45 dan HUB.



Gambar 2.3. Kabel UTP (katagori 5) dan konektor RJ-45

Standar EIA/TIA 568 menjelaskan spesifikasi kabel UTP sebagai aturan dalam instalasi jaringan komputer. EIA/TIA menggunakan istilah kategori untuk membedakan beberapa tipe kabel UTP, Kategori untuk *twisted pair* (hingga saat ini, Mei 2005), yaitu:

Tabel 2.1. Tipe kabel UTP

Type Cable	Keterangan
UTP Catagory 1	Analog. Biasanya digunakan diperangkat telephone pada jalur ISDN (Integrated Service Digital Network), juga untuk menghubungkan modem dengan line telephone.
UTP Catagory 2	Bisa mencapai 4 Mbits (sering digunakan pada topologi token ring)
UTP / STP Catagory 3	10 Mbits data transfer (sering digunakan pada topologi token ring atau 10BaseT)
UTP / STP Catagory 4	16 Mbits data transfer (sering digunakan pada topologi token ring)
UTP / STP Catagory 5	Bisa mencapai 100 Mbits data transfer /22db (sering digunakan pada topologi star atau tree) ethernet 10Mbps, Fast ethernet 100Mbps, tokenring 16Mbps
UTP / STP Catagory 5e	1 Gigabit Ethernet (1000Mbps), jarak 100m
STP Catagory 6	2,5 Gigabit Ethernet, menjangkau jarak hingga 100m, atau 10Gbps (Gigabit Ethernet) 25 meters. 20,2 db Up to 155 MHz atau 250 MHz
STP Catagory 7	Gigabit Ethernet/20,8 db (Gigabit Ethernet). Up to 200 MHz atau 700 MHz

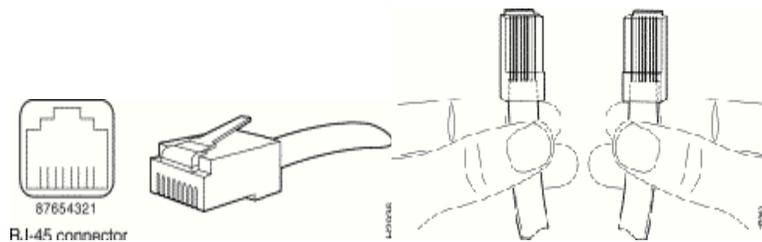
Sumber: <http://www.glossary-tech.com/cable.htm> dan
http://www.firewall.cx/cabling_utp.php





Pemberian kategori 1/2/3/4/5/6/7 merupakan kategori spesifikasi untuk masing-masing kabel tembaga dan juga untuk *jack*. Masing-masing merupakan seri revisi atas kualitas kabel, kualitas pembungkusan kabel (isolator) dan juga untuk kualitas “belitan” (*twist*) masing-masing pasang kabel. Selain itu juga untuk menentukan besaran frekuensi yang bisa lewat pada sarana kabel tersebut, dan juga kualitas *isolator* sehingga bisa mengurangi efek induksi antar kabel (*noise* bisa ditekan sedemikian rupa).

Perlu diperhatikan juga, spesifikasi antara CAT5 dan CAT5enhanced mempunyai standar industri yang sama, namun pada CAT5e sudah dilengkapi dengan insulator untuk mengurangi efek induksi atau electromagnetic interference. Kabel CAT5e bisa digunakan untuk menghubungkan network hingga kecepatan 1Gbps.



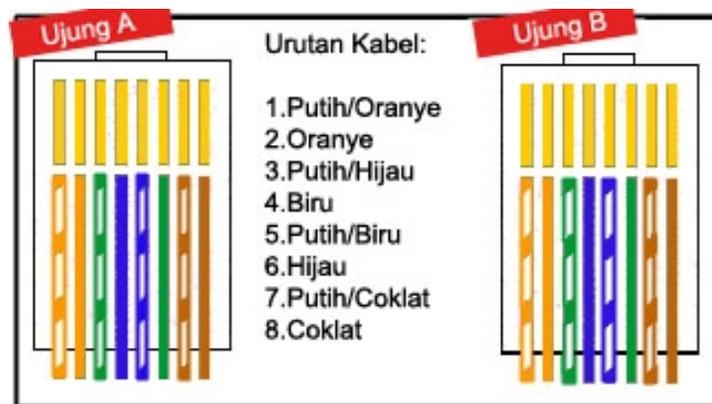
Gambar 2.4. Konektor RJ-45 dan cara membedakannya

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

- Straight Through Cable
- Cross Over Cable dan
- Roll Over Cable

2.1.1.2.1 Straight Through Cable

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



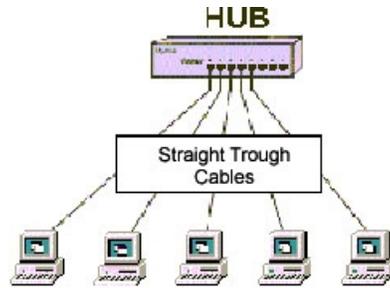
Gambar 2.5. Straight Through Cable T568B

Penggunaan kabel UTP model straight through pada jaringan lokal biasanya akan membentuk topologi star (bintang) atau tree (pohon) dengan HUB/switch sebagai pusatnya. Jika sebuah HUB/switch tidak berfungsi, maka seluruh komputer yang terhubung dengan HUB tersebut tidak dapat saling berhubungan.





Penggunaan HUB harus sesuai dengan kecepatan dari Ethernet card yang digunakan pada masing-masing komputer. Karena perbedaan kecepatan pada NIC dan HUB berarti kedua perangkat tersebut tidak dapat saling berkomunikasi secara maksimal.



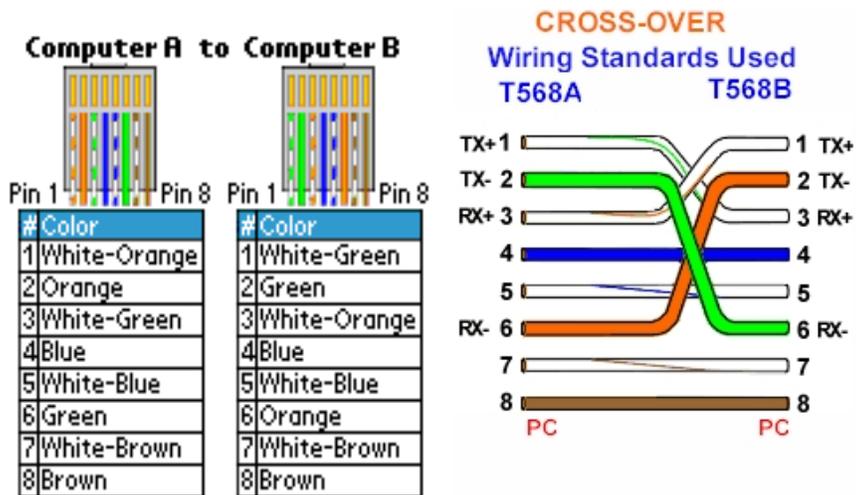
Gambar 2.6. Pemasangan Straight Through Cable dengan HUB

Penggunaan Straight Through Cable

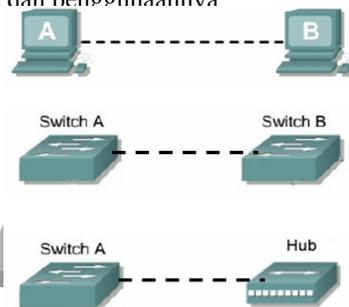
- o PC → Hub
- o PC → Switch
- o Hub → Hub
- o Switch → Router

2.1.1.2.2 Cross Over Cable

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



Gambar 2.7. Cross Over Cable dan penggunaannya





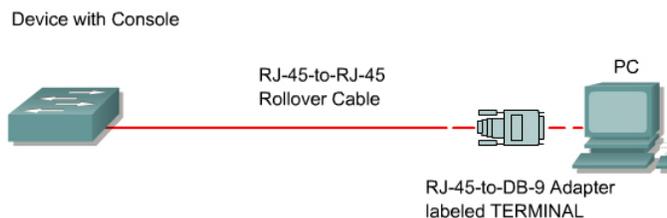
Penggunaan Cross Over Cable

- o PC → PC
- o Switch → Swiath
- o Switch → Hub

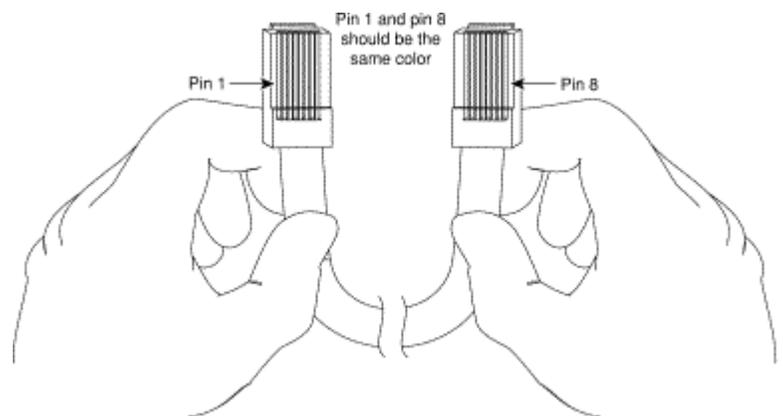
2.1.1.2.3 Roll-Over Cable

Pada sistem CISCO, ada satu cara lain pemasangan kabel UTP, yang digunakan untuk menghubungkan sebuah terminal (PC) dan modem ke console Cisco Router atau console switch managible, cara ini disebut dengan **Roll-Over**. Kabel Roll-Over tersebut sebelumnya terkoneksi dengan DB-25 atau DB-9 Adapter sebelum ke terminal (PC).

Anda dapat mengenali sebuah kabel roll-over dengan melihat ke dua ujung kabel. Dimana warna kabel dari sisi yang satu akan berbalik pada sisi kabel di ujung yang lain. Misalnya kabel putih orange yang berada pada pin 1 ujung kabel A, akan berada pada pin 8 ujung kabel B.

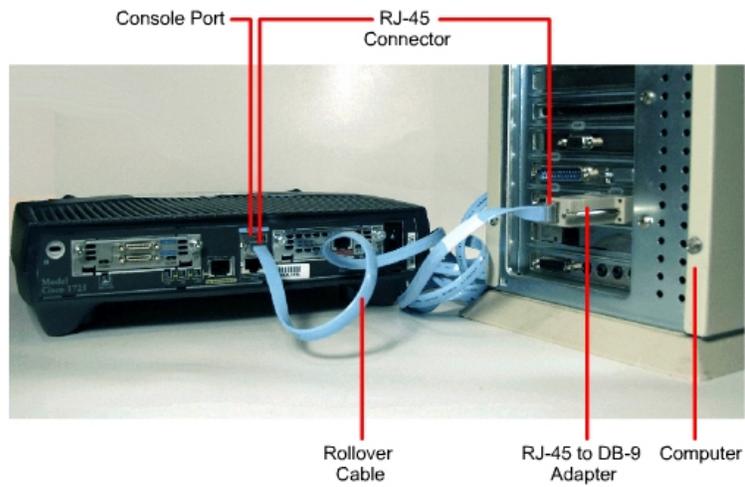


Gambar 2.8. RollOver Cable dari console switch ke PC

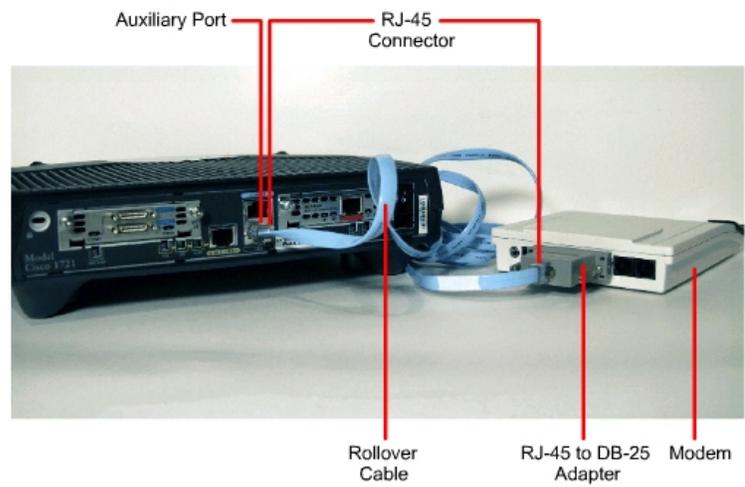


Gambar 2.9. Cara melihat Roll-Over Cable

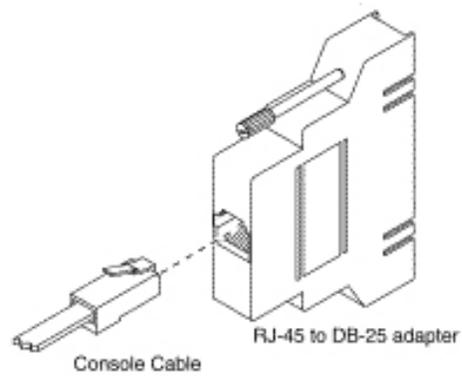




Gambar 2.10. Koneksi Console Terminal



Gambar 2.11. Koneksi Auxiliry port router cisco ke modem





Gambar 2.12. RJ-45 to DB-25 Adapter

Tabel 2.2. Hubungan antar pin RJ-45 untuk pemasangan kabel Roll-over

Router Pin name	Router Pin	Direction	Workstation Pin	Workstation Pin name
White-Orange	1	↔	8	Brown
Orange	2	↔	7	White-Brown
White-Green	3	↔	6	Green
Blue	4	↔	5	White-Blue
White-Blue	5	↔	4	Blue
Green	6	↔	3	White-Green
White-Brown	7	↔	2	Orange
Brown	8	↔	1	White-Orange

Penggunaan kabel rolover

- PC → console router
- PC → console switch managible
- Router → modem

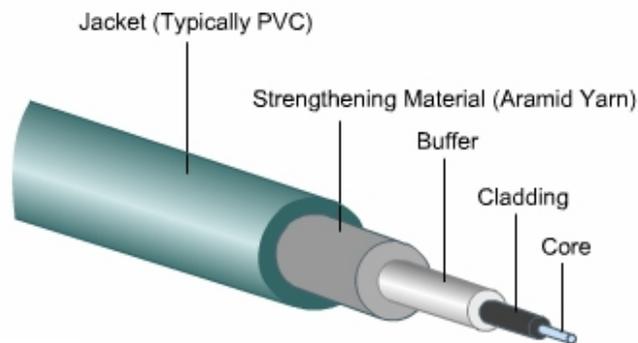
2.1.1.3 Fiber Optic Cable

Kabel yang memiliki inti serat kaca sebagai saluran untuk menyalurkan sinyal antar terminal, sering dipakai sebagai saluran BACKBONE karena keandalannya yang tinggi dibandingkan dengan coaxial cable atau kabel UTP. Karakteristik dari kabel ini tidak terpengaruh oleh adanya cuaca dan panas.



Gambar 2.13. Konektor dan kabel Fiber Optic





Gambar 2.14. Lapisan kabel fiber optic

2.1.1.3.1 Kemampuan Kabel Serat Optik (FO)

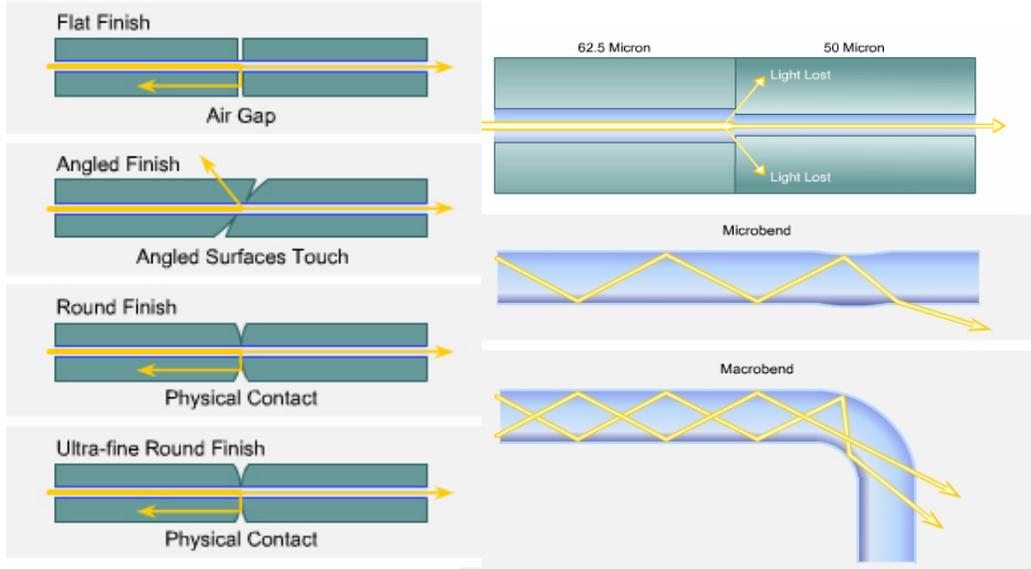
Fiber optik menunjukkan kualitas tinggi untuk berbagai macam aplikasi, hal ini di sebabkan:

- Dapat mentransmisi bit rate yg tinggi,
- Tidak sensitif pada gangguan elektromagnetik
- Memiliki Bit Error Rate (kesalahan) kecil
- Reliabilitas lebih baik dari kabel koaksial

2.1.1.3.2. Kondisi & tempat pemasangan kabel FO

- Di wilayah kota, terdapat banyak lekukan dan saluran yang biasanya dipenuhi oleh kabel lain, sehingga pemasangan infrastruktur baru selalu dibuat dalam jumlah kecil, sehingga radius belokan fiber dan kabel diusahakan tetap kecil.
- Kabel terpasang dalam bermacam-macam kondisi, seperti: di luar, dibawah tanah, di udara, dalam ruangan. Konsekuensinya banyak kondisi termal, mekanikal dan tekanan lain yang harus diterima.
- Hindari kondisi banyaknya penyambungan, sehingga tidak memerlukan teknisi yang terlatih dan persiapan yang mudah.
- Jangan sampai terjadi banyak tekukan & kebocoran jacket pelindung yang bisa menyebabkan kebocoran Cahaya
- Biaya jalur koneksi global harus menjadi lebih rendah.





Gambar 2.15. contoh kebocoran cahaya akibat kesalahan pemasangan dan penyambungan kabel FO

Berikut ini merupakan tabel standarisasi kabel dari IEEE untuk kabel jenis coaxial, UTP/STP maupun Fiber Optic

Tabel 2.3. Tipe Standarisasi Kabel 1

	10BASE2	10BASE5	10BASE-T	100BASE-TX	100BASE-FX
Media	50-ohm coaxial (Thinnet)	50-ohm coaxial (Thicknet)	EIA/TIA Category 3, 4, 5 UTP, two pair	EIA/TIA Category 5 UTP, two pair	62.5/125 multimode fiber
Maximum Segment Length	185 m (606.94 feet)	500 m (1640.4 feet)	100 m (328 feet)	100 m (328 feet)	400 m (1312.3 feet)
Topology	Bus	Bus	Star	Star	Star
Connector	BNC	Attachment unit interface (AUI)	ISO 8877 (RJ-45)	ISO 8877 (RJ-45)	





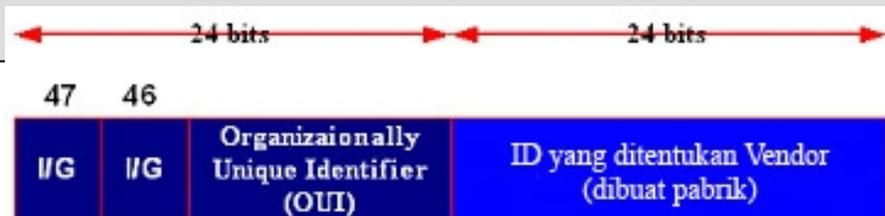
Tabel 2.4. Tipe Standarisasi Kabel 2

1000BASE-CX	1000BASE-T	1000BASE-SX	1000BASE-LX
STP	EIA/TIA Category 5 UTP, four pair	62.5/50 micro multimode fiber	62.5/50 micro multimode fiber; 9-micron single-mode fiber
25 m (82 feet)	100 m (328 feet)	275 m (853 feet) for 62.5 micro fiber; 550 m (1804.5 feet) for 50 micro fiber	440 m (1443.6 feet) for 62.5 micro fiber; 550 m (1804.5 feet) for 50 micro fiber; 3 to 10 km (1.86 to 6.2 miles) on single-mode fiber
Star	Star	Star	Star
ISO 8877 (RJ-45)	ISO 8877 (RJ-45)		

2.1.2 Ethernet Card /Network Interface Card (Network Adapter)

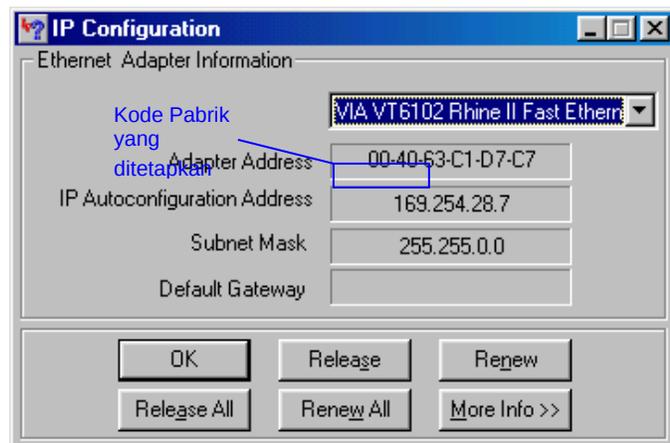
Cara kerja Ethernet Card berdasarkan **broadcast network** yaitu setiap node dalam suatu jaringan menerima setiap transmisi data yang dikirim oleh suatu node yang lain. Setiap Ethernet card mempunyai alamat sepanjang 48 bit yang dikenal sebagai Ethernet address (MAC Address).

Alamat tersebut telah ditanam ke dalam setiap rangkaian kartu jaringan (NIC) yang dikenali sebagai '*Media Access Control*' (MAC) atau lebih dikenali dengan istilah '*hardware address*'. 24 bit atau 3 byte awal merupakan kode yang telah ditentukan oleh IEEE.

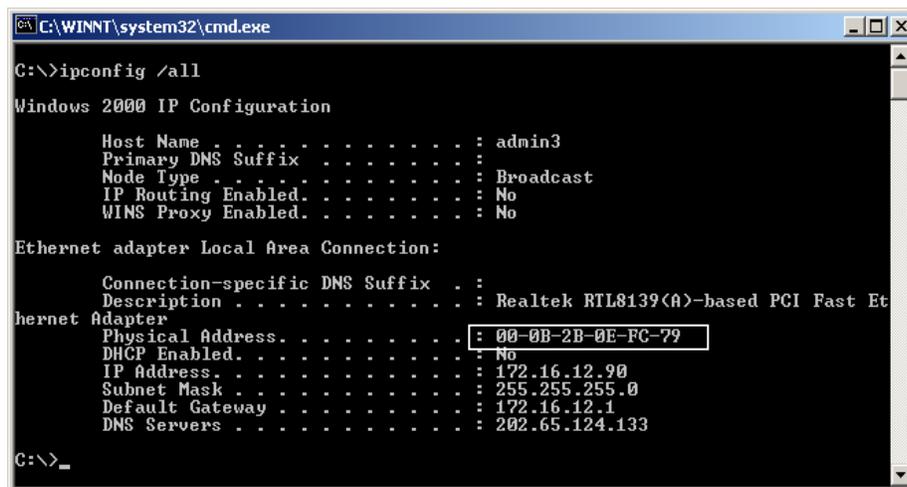


Gambar 2.16. Pembagian bit pada MAC Address.





Gambar 2.17. Cara melihat MAC Address, dengan mengetik **winipcfg** pada menu RUN di Windows 98.

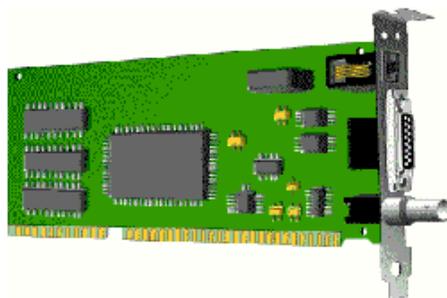


Gambar 2.18. Cara melihat MAC Address, dari shell DOS dengan mengetik **ipconfig /all** pada SO Windows.

Kartu jaringan Ethernet biasanya dibeli terpisah dengan komputer, kecuali network adapter yang sudah onboard. Komputer Macintosh juga sudah mengikutkan kartu jaringan ethernet didalamnya. Kartu Jaringan ethernet model 10Base umumnya telah menyediakan port koneksi untuk kabel coaxial ataupun kabel twisted pair, jika didesain untuk kabel coaxial konektornya adalah BNC, dan bila didesain untuk kabel twisted pair maka akan punya port konektor RJ-45.

Beberapa kartu jaringan ethernet kadang juga punya konektor AUI. Semua itu dikoneksikan dengan coaxial, twisted pair, ataupun dengan kabel fiber optik.



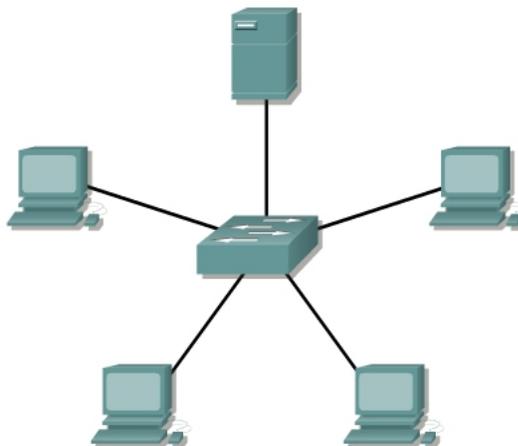


Gambar 2.19. Network Interface card (dari atas ke bawah konektor RJ-45, konektor AUI, dan konektor BNC)

2.1.3 Hub dan Switch (Konsentrator)

Sebuah konsentrator (Hub atau switch) adalah sebuah perangkat yang menyatukan kabel-kabel network dari tiap workstation, server atau perangkat lain. Dalam topologi bintang, kabel twisted pair datang dari sebuah workstation masuk kedalam hub atau switch.

Hub dan switch mempunyai banyak lubang port RJ-45 yang dapat dipasang konektor RJ-45 dan terhubung ke sejumlah komputer. Beberapa jenis hub dapat dipasang bertingkat (stackable) hingga 4 susun. Biasanya hub maupun switch memiliki jumlah lubang sebanyak 4 bh, 8 bh, 16 bh, hingga 24 bh.



Gambar 2.20. Beberapa komputer yang terhubung melalui sebuah hub

Switch merupakan konsentrator yang memiliki kemampuan manajemen traffic data lebih baik bila dibandingkan hub. Saat ini telah terdapat banyak tipe switch yang managible, selain dapat mengatur traffic data, juga dapat diberi IP Address.

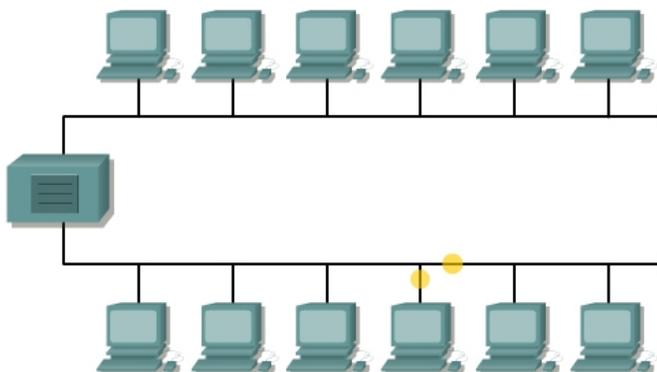
2.1.4 Repeater

Fungsi utama repeater yaitu untuk memperkuat sinyal dengan cara menerima sinyal dari suatu segmen kabel LAN lalu memancarkan kembali dengan kekuatan yang sama dengan sinyal asli pada segmen kabel yang lain. Dengan cara ini jarak antara kabel dapat diperjauh.





Penggunaan repeater antara dua segmen atau lebih segmen kabel LAN mengharuskan penggunaan protocol physical layer yang sama antara segmen-segmen kebel tersebut misalnya repeater dapat menghubungkan dua buah segmen kabel Ethernet 10BASE2.



Gambar 2.21. Penggunaan repeater antara dua segmen

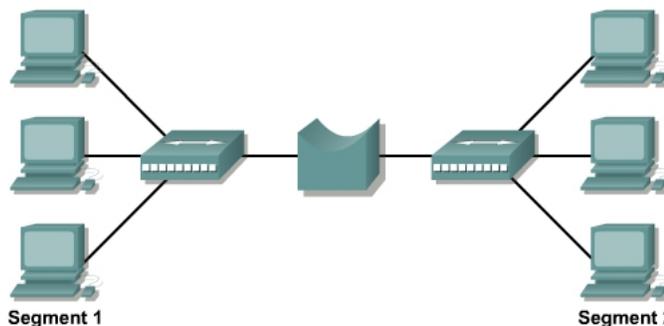
2.1.5 Bridge

Fungsi dari bridge itu sama dengan fungsi repeater tapi bridge lebih fleksibel dan lebih cerdas dari pada repeater. Bridge dapat menghubungkan jaringan yang menggunakan metode transmisi yang berbeda. Misalnya bridge dapat menghubungkan Ethernet baseband dengan Ethernet broadband.

Bridge mampu memisahkan sebagian dari trafik karena mengimplementasikan mekanisme frame filtering. Mekanisme yang digunakan di bridge ini umum disebut sebagai store and forward. Walaupun demikian broadcast traffic yang dibangkitkan dalam LAN tidak dapat difilter oleh bridge.

Terkadang pertumbuhan network sangat cepat makanya di perlukan jembatan untuk itu. Kebanyakan Bridges dapat mengetahui masing-masing alamat dari tiap-tiap segmen komputer pada jaringan sebelahnyanya dan juga pada jaringan yang lain di sebelahnyanya pula. Diibaratkan bahwa *Bridges ini seperti polisi lalu lintas yang mengatur dipersimpangan jalan pada saat jam-jam sibuk*. Dia mengatur agar informasi di antara kedua sisi network tetap jalan dengan baik dan teratur.

Bridges juga dapat digunakan untuk mengkoneksi network yang menggunakan tipe kabel yang berbeda ataupun topologi yang berbeda pula. Bridges dapat mengetahui alamat masing-masing komputer di masing-masing sisi jaringan.



Gambar 2.22. Bridges yang digunakan untuk mengkoneksi 2 segmen





2.1.6 Router

Sebuah Router mampu mengirimkan data/informasi dari satu jaringan ke jaringan lain yang berbeda, router hampir sama dengan bridge, meski tidak lebih pintar dibandingkan bridge, namun pengembangan perangkat router dewasa ini sudah mulai mencapai bahkan melampaui batas tuntutan teknologi yang diharapkan.

Router akan mencari jalur terbaik untuk mengirimkan sebuah pesan yang berdasarkan atas alamat tujuan dan alamat asal. Router mengetahui alamat masing-masing komputer dilingkungan jaringan lokalnya, mengetahui alamat bridges dan router lainnya.



Gambar 2.23. Cisco Router perspektif dari belakang

Router juga dapat mengetahui keseluruhan jaringan dengan melihat sisi mana yang paling sibuk dan bisa menarik data dari sisi yang sibuk tersebut sampai sisi tersebut bersih/clean.

Jika sebuah perusahaan mempunyai LAN dan menginginkan terkoneksi ke internet, maka mereka sebaiknya membeli dan menggunakan router, mengapa ?

Karena kemampuan yang dimiliki router, diantaranya:

1. router dapat menterjemahkan informasi diantara LAN anda dan internet
2. router akan mencari alternatif jalur yang terbaik untuk mengirimkan data melewati internet
3. mengatur jalur sinyal secara efisien dan dapat mengatur data yang mengalir diantara dua buah protocol
4. dapat mengatur aliran data diantara topologi jaringan linear Bus dan Star
5. dapat mengatur aliran data melewati kabel fiber optic, kabel koaksial atau kabel twisted pair.

Network Devices	
Repeater 	Bridge 
10BASE-T Hub 	Workgroup Switch 
100BASE-T Hub 	Router 
Hub 	Network Cloud 

Gambar 2.24. Simbol Network Device





2.2 Topologi Jaringan

Topologi jaringan atau arsitektur jaringan adalah gambaran perencanaan hubungan antar komputer dalam Local Area Network, yang umumnya menggunakan kabel (sebagai media transmisi), dengan konektor, ethernet card dan perangkat pendukung lainnya.

Ada beberapa jenis topologi yang sering terdapat pada hubungan komputer pada jaringan local area, seperti:

2.2.1 Topologi Bus

Topologi ini merupakan bentangan satu kabel yang kedua ujungnya ditutup, dimana sepanjang kabel terdapat node-node. Signal dalam kabel dengan topologi ini dilewati satu arah sehingga memungkinkan sebuah collision terjadi.

Keuntungan:

- murah, karena tidak memakai banyak media, kabel yang dipakai sudah umum (banyak tersedia dipasaran)
- setiap komputer dapat saling berhubungan langsung.

Kerugian:

- Sering terjadi hang / crass talk, yaitu bila lebih dari satu pasang memakai jalur diwaktu yang sama, harus bergantian atau ditambah relay.

2.2.2 Topologi Ring

Topologi jaringan yang berupa lingkaran tertutup yang berisi node-node. Signal mengalir dalam dua arah sehingga dapat menghindarkan terjadinya collision, sehingga memungkinkan terjadinya pergerakan data yang sangat cepat.

Semua komputer saling tersambung membentuk lingkaran (seperti bus tetapi ujung-ujung bus disambung). Data yang dikirim diberi address tujuan sehingga dapat menuju komputer yang dituju. Tiap stasiun (komputer) dapat diberi repeater (transceiver) yang berfungsi sebagai:

○ Listen State

Tiap bit dikirim kembali dengan mengalami delay waktu.

○ Transmit State

Bila bit yang berasal dari paket lebih besar dari ring maka repeater akan mengembalikan ke pengirim. Bila terdapat beberapa paket dalam ring, repeater yang tengah memancarkan, menerima bit dari paket yang tidak dikirimnya harus menampung dan memancarkan kembali.

○ Bypass State

Berfungsi untuk menghilangkan delay waktu dari stasiun yang tidak aktif.

Keuntungan:

- Kegagalan koneksi akibat gangguan media, dapat diatasi dengan jalur lain yang masih terhubung.
- Penggunaan sambungan point to point membuat transmission error dapat diperkecil





Kerugian:

- Data yang dikirim bila melalui banyak komputer, transfer data menjadi lambat.

2.2.3 Topologi Star

Karakteristik dari topologi jaringan ini adalah node (station) berkomunikasi langsung dengan station lain melalui central node (hub/switch), traffic data mengalir dari node ke central node dan diteruskan ke node (station) tujuan. Jika salah satu segmen kabel putus, jaringan lain tidak akan terputus.

Keuntungan:

- Akses ke station lain (client atau server) cepat
- Dapat menerima workstation baru selama port di centralnode (hub/switch) tersedia.
- Hub/switch bertindak sebagai konsentrator.
- Hub/switch dapat disusun seri (bertingkat) untuk menambah jumlah station yang terkoneksi di jaringan.
- User dapat lebih banyak dibanding topologi bus, maupun ring.

Kerugian:

Bila traffic data cukup tinggi dan terjadi collision, maka semua komunikasi akan ditunda, dan koneksi akan dilanjutkan/dipersilahkan dengan cara random, apabila hub/switch mendetect tidak ada jalur yang sedang dipergunakan oleh node lain.

2.2.4 Topologi Tree / Hierarchical (Hirarki)

Tidak semua stasiun mempunyai kedudukan yang sama. Stasiun yang kedudukannya lebih tinggi menguasai stasiun dibawahnya, sehingga jaringan sangat tergantung dengan stasiun yang kedudukannya lebih tinggi (hierachical topology) dan kedudukan stasiun yang sama disebut *peer topology*.

2.2.5 Topologi Mesh dan Full Connected

Topologi jaringan ini menerapkan hubungan antar sentral secara penuh. Jumlah saluran harus disediakan untuk membentuk jaringan Mesh adalah jumlah sentral dikurangi 1 ($n-1$, n = jumlah sentral). Tingkat kerumitan jaringan sebanding dengan meningkatnya jumlah sentral yang terpasang. Dengan demikian disamping kurang ekonomis juga relatif mahal dalam pengoperasiannya.

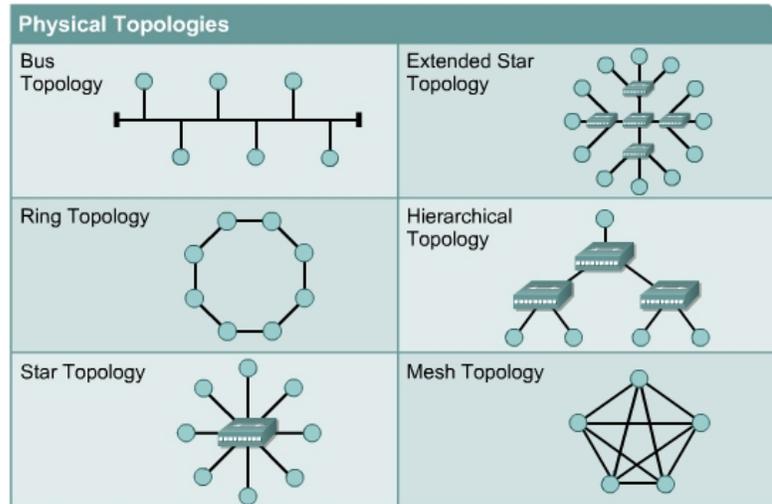
Topologi mesh ini merupakan teknologi khusus (ad hock) yang tidak dapat dibuat dengan pengkabelan, karena sistemnya yang rumit, namun dengan teknologi wireless topologi ini sangat memungkinkan untuk diwujudkan (karena dapat dipastikan tidak akan ada kabel yang berseliweran).

Biasanya untuk memperkuat sinyal transmisi data yang dikirimkan, ditengah-tengah (area) antar komputer yang kosong di tempatkan perangkat radio (air point) yang berfungsi seperti repeater untuk memperkuat sinyal sekaligus bisa mengatur arah komunikasi data yang terjadi.

2.2.6 Topologi Hybrid

Topologi ini merupakan topologi gabungan dari beberapa topologi yang ada, yang bisa memadukan kinerja dari beberapa topologi yang berbeda, baik berbeda sistem maupun berbeda media transmisinya.





Gambar 2.25. Beberapa jenis topologi

2.3 Teknik Penyaluran Sinyal

Komunikasi data antar komputer dalam topologi jaringan memerlukan teknik penyaluran sinyal agar data yang terkirim sesuai keadaan yang sebenarnya atau sesuai keinginan. Secara detail tentang bagaimana sinyal-sinyal tersebut terkirim, tidak kita bahas pada buku ini, karena memerlukan referensi tersendiri dan pengetahuan mendalam tentang teknologi analog maupun digital.

Namun secara singkat dapat diuraikan bahwa teknik penyaluran sinyal menunjukkan cara penyaluran sinyal dalam saluran media transmisi, dengan menggunakan teknik:

Baseband

Menggunakan sinyal digital. Transmisi yang digunakan bersifat *bidirectional* dan dipakai hanya untuk topologi bus yang jangkauannya pendek. Media yang digunakan kabel coaxial (50 ohm), dengan spesifikasi IEEE 802.3 (Ethernet), bila inti kabel coaxial berdiameter 0.4 inch dan data rate 10 Mbps, maka dengan perangkat ini kita dapat menjangkau jarak 500 m (dikenal dengan sebutan *10BASE5*). Untuk jarak yang lebih jauh dapat digunakan repeater.

Broadband

Menggunakan sinyal analog dengan Frequency Division Multiplexing (FDM). Spektrum media transmisi dapat dibagi sesuai keperluan, jarak yang dijangkau lebih jauh dibanding baseband dan mendukung topologi tree.

Broadband merupakan hubungan unidirectional yang penuh, yang mengharuskan ada dua saluran data. Semua stasiun mengirim sinyal melalui inbound dan menerima sinyal dari saluran outbound dengan cara :

- ❑ Memakai dua kabel terpisah (dual cable), atau
- ❑ Memakai satu kabel dengan frekuensi modulasi berbeda (split)
- ❑ Memakai media transmisi kabel coaxial 75 ohm dan data selalu dimodulasi terlebih dahulu, lebih baik dari baseband karena dapat mengirimkan voice dan video secara bersamaan.

2.4 Prinsip Penyaluran Sinyal

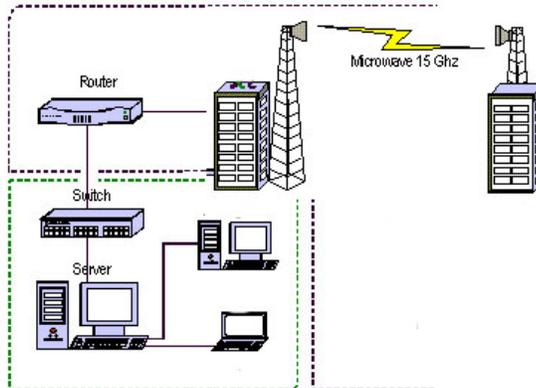




Transmisi pada Local Area Network hingga Wide Area network dapat dibagi ke dalam tiga kategori utama, yaitu : unicast, multicast dan broadcast yang masing-masing akan kita bahas berikut ini :

2.4.1 Unicast

Unicast merupakan transmisi **jaringan point to point** (one to one). Ketika digunakan, satu sistem tunggal hanya mencoba berkomunikasi dengan satu sistem lainnya. Jaringan point to point biasanya digunakan pada jaringan yang besar, dengan menghubungkan jaringan lokal ke jaringan lain melalui satu titik akses point.

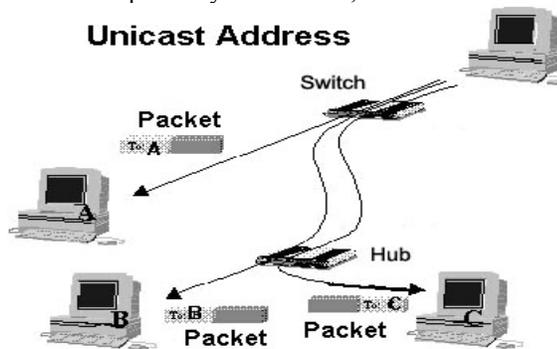


Gambar 2.26 Koneksi jaringan point to point menggunakan teknologi wireless (microwave 15 GHz)

Bila satu paket data akan dikirimkan ke mesin (node) lain di jaringan yang lain, maka paket tersebut harus melewati satu atau lebih node yang lain yang berfungsi sebagai perantara. Node perantara ini dapat juga merupakan komputer **gateway** yang berfungsi sebagai gerbang keluar masuknya paket data dari satu jaringan ke jaringan yang lain.

Pada jaringan Ethernet, penggunaan unicast dapat diketahui dengan melihat MAC Address asal dan tujuan yang merupakan alamat host yang unik. Pada jaringan yang menggunakan IP, alamat IP asal dan tujuan merupakan alamat yang unik (tidak akan sama satu dengan yang lain).

Ketika sistem berhubungan dengan frame jaringan, ia akan selalu memeriksa MAC Address miliknya untuk melihat apakah frame tersebut ditujukan untuk dirinya, Jika MAC Address-nya cocok dengan sistem tujuan, maka ia akan memprosesnya. Jika tidak, frame tersebut akan diabaikan.



Gambar 2.27. Pengiriman Packet data ke Unicast Address

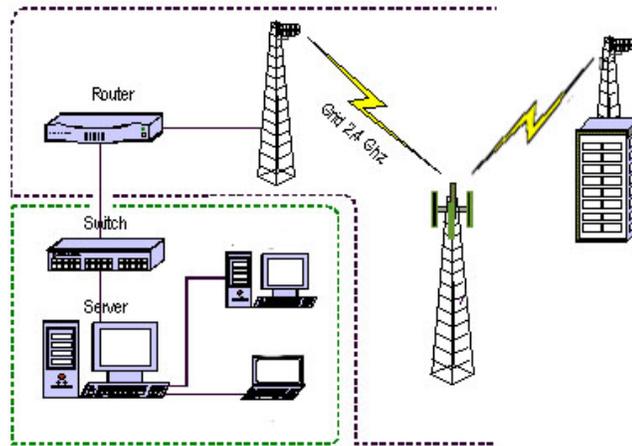




Ingat...!!!, ketika dihubungkan ke hub, semua sistem dapat melihat semua frame yang dikirimkan melalui jaringan, karena mereka semua bagian dari collision domain yang sama.

2.4.2 Multicast

Multicast merupakan transmisi yang dimaksudkan untuk banyak tujuan, tetapi tidak harus semua host. Oleh karena itu, multicast dikenal sebagai metode tranmisi one to many (satu ke banyak) atau **jaringan point to multipoint**.

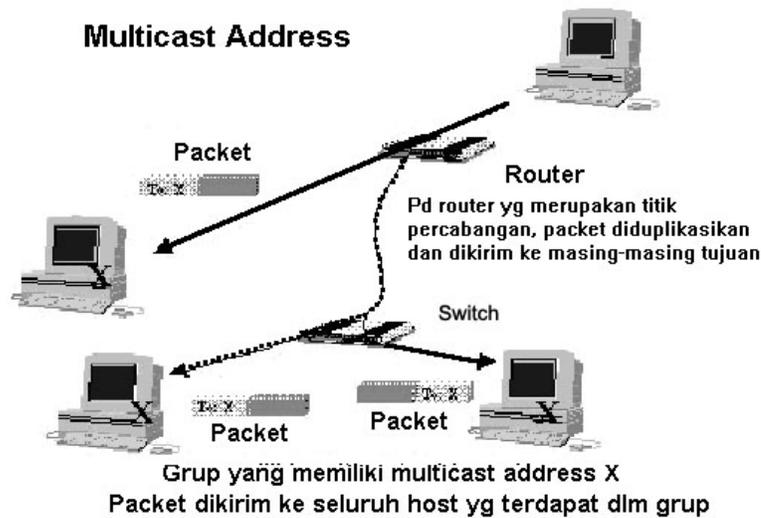


Gambar 2.28 Koneksi jaringan point to multipoint menggunakan teknologi wireless (wi-fi 2,4 GHz)

Multicast digunakan dalam kasus-kasus tertentu, misalnya ketika sekelompok komputer perlu menerima transmisi tertentu. Salah satu contohnya adalah streaming audio atau video. Misalkan banyak komputer ingin menerima transmisi video pada waktu yang bersamaan. Jika data tersebut dikirimkan ke setiap komputer secara individu, maka diperlukan beberapa aliran data. Jika data tersebut dikirimkan sebagai broadcast, maka tidak perlu lagi proses untuk semua system. Dengan multicast data tersebut hanya dikirim sekali, tetapi diterima oleh banyak system.

Protokol-protokol tertentu menggunakan range alamat khusus untuk multicast. Sebagai contoh, alamat IP dalam kelas D telah direservasi untuk keperluan multicast. Jika semua host perlu menerima data video, mereka akan menggunakan alamat IP multicast yang sama. Ketika mereka menerima paket yang ditujukan ke alamat tersebut, mereka akan memprosesnya.





Gambar 2.29 Pengiriman packet data ke alamat multicast

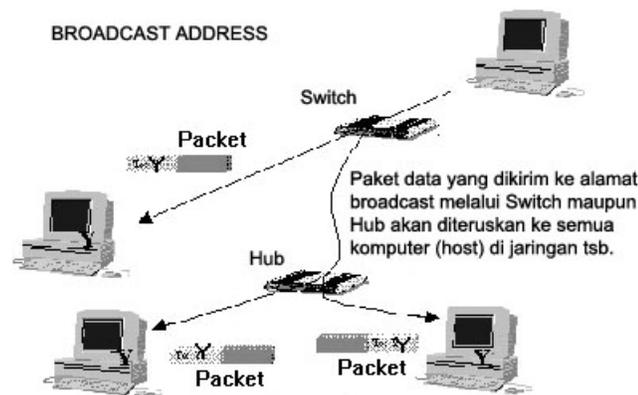
Ingat...!!!, bahwa setiap NIC selain memiliki MAC Address (dari vendor pembuat ethernet card atau network adapter), ia juga memiliki alamat IP sendiri-sendiri, selain itu mereka juga mendengarkan alamat multicast mereka.

Dalam teknologi pengiriman data SMS (Short Message Service) antar pengguna telephone selular, teknik multicast ini digunakan untuk menjelaskan bagaimana sebuah pesan yang dikirimkan dari satu ponsel dapat diterima oleh banyak ponsel lain (dari satu operator atau berbeda operator), atau juga sebuah pesan yang dikirimkan oleh operator selular yang biasanya berupa info layanan, berita, iklan dll, akan diterima oleh banyak ponsel lain dalam satu jaringan atau area layanan operator selular tersebut.

2.4.3 Broadcast

Jenis transmisi jaringan yang terakhir adalah broadcast, yang juga dikenal sebagai metode transmisi one to all (satu kesemua). **Sistem broadcast** juga dapat digunakan untuk menjelaskan bila ada paket-paket data yang dikirimkan dari satu mesin akan diterima oleh mesin-mesin lainnya dalam satu jaringan atau subnet jaringan lainnya. Pada jaringan Ethernet, broadcast dikirim ke alamat tujuan khusus, yaitu, FF-FF-FF-FF-FF-FF atau dengan oktet terakhir berisi bit 11111111. Broadcast ini harus diproses oleh semua host yang berada dalam broadcast domain yang ditentukan.



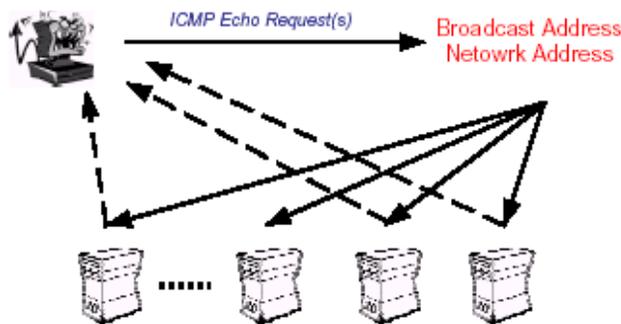


Gambar 2.30 Pengiriman packet data ke alamat broadcast

Field alamat pada sebuah paket berisi keterangan tentang kepada siapa paket itu dialamatkan. Saat menerima sebuah paket, mesin akan men-cek field alamat, bila alamat tersebut ditujukan untuk dirinya, maka paket tersebut akan diterima, namun bila alamat tersebut bukan ditujukan buat dirinya, maka paket tersebut akan diabaikan. Walaupun broadcast cenderung membuang resource, beberapa protokol seperti ARP, sangat bergantung kepadanya, dengan demikian, terjadinya beberapa traffic broadcast tidak dapat dihindari.

2.4.4 Broadcast ICMP

Cara termudah untuk mengetahui host yang hidup pada sebuah target jaringan adalah dengan mengirimkan ICMP echo request ke broadcast address pada target jaringan tersebut. Sebuah permintaan (request) akan dikirim secara broadcast ke semua host pada target network. Host yang hidup akan mengirimkan ICMP echo reply.



Gambar 2.31. Broadcast ICMP

2.5 Rangkuman

Tipe kabel yang sering digunakan untuk keperluan jaringan komputer adalah coaxial, UTP/STP dan Fiber Optic. Jaringan komputer tanpa kabel (wireless) menggunakan teknologi W-Fi, Microwave, dan WiMAX.

Tiga model pemasangan kabel UTP: Straight Through Cable, Cross Over Cable dan Roll Over Cable. Alat untuk menguji kualitas kabel dan hasil crimping konektor RJ-45 digunakan LAN cable tester atau Fluke.





Penggunaan kabel coaxial pada jaringan local biasanya akan membentuk topologi bus atau ring, sedangkan kabel UTP model straight through pada jaringan lokal biasanya akan membentuk topologi star (bintang) atau tree (pohon) dengan HUB/switch sebagai pusatnya. Jika sebuah HUB/switch tidak berfungsi, maka seluruh komputer yang terhubung dengan HUB tersebut tidak dapat saling berhubungan.

Kabel UTP model straight trough digunakan untuk menghubungkan PC dengan switch atau hub, hub ke hub atau switch ke router. Model crossover digunakan untuk menghubungkan PC ke PC, switch ke switch, switch ke hub. Model rollover digunakan untuk menghubungkan terminal (PC) dan modem ke console Cisco Router atau console switch managible.

Topologi jaringan : Bus, Ring, Star, Tree, Mesh, Hibryd.

Setiap NIC selain memiliki MAC Address (dari vendor pembuat ethernet card), ketika ia diberi alamat IP dan netmask, maka ia juga akan memiliki IP Broadcast dan mendengarkan alamat multicast mereka.

Kekurangan hub dibandingkan switch adalah penggunaan hub sebagai konsentrator membuat semua sistem dapat melihat semua frame yang dikirimkan melalui jaringan, karena mereka semua bagian dari collision domain yang sama.

Sistem broadcast digunakan untuk menjelaskan bila ada paket-paket data yang dikirimkan dari satu mesin akan diterima oleh mesin-mesin lainnya dalam satu jaringan atau subnet jaringan lainnya.

2.6 Soal Latihan :

1. Ada beberapa tipe kabel koaksial (coax). serta nilai impedansinya, sebutkan juga pada topologi apa kabel jenis ini digunakan.
2. Jelaskan beberapa cara pemasangan kabel UTP pada konektor RJ-45, pada topologi apa kabel jenis ini dipergunakan.
3. Apa yang dimaksud dengan MAC Address, dan jelaskan cara kerja Ethernet card secara singkat.
4. Gambarkan beberapa bentuk topologi yang kamu ketahui (minimal 5), jelaskan keuntungan dan kerugian masing-masing topologi tersebut (minimal 3)
5. Jelaskan pengertian dari baseband dan broadband

DAFTAR PUSTAKA

Cisco, Materi CCNA 1,2 v.31

http://www.firewall.cx/cabling_utp.php

<http://www.glossary-tech.com/cable.htm>

<http://www.ilmukomputer.com>

Pengantar Jaringan Komputer, Melwin Syafrizal, Andi Offset, Jogja, 2005





INTRANET, EXTRANET & INTERNET

Kopetensi Dasar: Mampu menjelaskan defenisi dan perbedaan internet, intranet dan extranet. Memahami teknologi dan cara untuk membangun koneksi internet (menghubungkan jaringan lokal ke internet), Mengenal teknologi wireless untuk membangun LAN dan koneksi internet

3.1 Intranet

Intranet merupakan sebuah jaringan internal perusahaan yang dibangun menggunakan teknologi internet (arsitektur berupa aplikasi web dan menggunakan protokol TCP/IP).





LAN tidak sama dengan intranet, karena dari segi penggunaan, luas area maupun implementasinya, intranet lebih luas dan bekerja lebih maksimal seperti halnya internet. Namun sangat terbatas dalam hal privilege dan hak akses para pemakainya. Sebuah LAN bisa saja disebut intranet, apabila LAN tersebut menerapkan aplikasi web dan menggunakan protokol TCP/IP didalamnya. Biasanya sebuah LAN dapat dihubungkan dengan jaringan internet, sedangkan intranet justru menghindari koneksi dengan jaringan luar.

Fakta bahwa perkembangan yang ada didunia internet dapat diimplementasikan secara langsung didalam *intranet*, menyebabkan *intranet* sangat populer dan berkembang pesat sejalan dengan perkembangan yang ada di internet.

3.1.1 Fungsi dan Implementasi Intranet

Informasi perusahaan (portal) yang mencakup berita, presensi kehadiran, prosedur kerja setiap divisi, kumpulan data penyimpanan, surat dan komunikasi antar divisi, dan lain-lain dapat diintegrasikan dalam satu sistem pusat informasi yang berbasis HTML (HyperText Markup Language) atau yang lebih dikenal dengan istilah World Wide Web (www).

Implementasi dan karakteristik *intranet* lainnya meliputi:

- ❖ Jadwal perorangan dan kelompok (personal and group scheduling),
- ❖ Pesan diterima ketika keluar (while were you out form),
- ❖ Manajemen informasi bagi perorangan dan kelompok (personal/group information management) dan
- ❖ transfer dokumen secara langsung (straight document transfer).

Hal yang mendorong penggunaan intranet adalah kebutuhan akan informasi. Berdasarkan survei yang dilakukan terhadap 103 executive sistem informasi yang memiliki 500 pegawai. Mereka memprioritaskan penggunaan intranet untuk menyebarkan manual, katalog, daftar barang, menyediakan human relation, dan informasi pekerjaan, menawarkan jasa email, dan mengadakan suatu revisi dokumen secara bersama-sama.

Alasan tersebut ditambah beberapa alasan antara lain :

- ❖ Komunikasi yang lebih baik antar pegawai
- ❖ Biaya pengembangan dan perawatan yang lebih murah dibanding teknologi client server biasa.
- ❖ Keinginan untuk menaikkan rasa kepemilikan data, dan tanggungjawab pengguna.
- ❖ Keinginan untuk menggunakan protokol yang terbuka.
- ❖ Mudah digunakan dan sederhana
- ❖ Mudah mendistribusikan program aplikasi ke user.
- ❖ Menaikkan akses dan distribusi informasi ke pengguna.

Awalnya teknologi intranet datang bersama dengan teknologi internet. Perbedaannya adalah pada penggunaan **firewall** bagi jaringan lokal intranet yang terkoneksi ke internet, agar dapat melindungi aset sistem informasi yang dimiliki perusahaan dari serangan pihak luar. Hal ini menjadikan intranet benar-benar dapat berfungsi secara independen dari internet, karena tidak terhubung dengan jaringan luar.





Hal lain yang membedakan intranet dan internet adalah dari sisi penggunanya. Aplikasi dan informasi intranet ditujukan bagi kalangan dalam organisasi itu sendiri. Sedangkan informasi di suatu situs internet ditujukan bagi kalangan luas (umum).

Pada saat ini teknologi intranet, telah mengalahkan popularitas *teknologi client-server tradisional*. Setiap orang dan perusahaan berlomba-lomba memanfaatkan teknologi ini. Hingga sebagian besar melupakan *salah satu hal yang paling penting dalam model client-server*, yaitu: ***pengembangan sistem tanpa disain yang baik akan mengakibatkan suatu sistem menjadi kurang bermanfaat***.

3.1.2 Jenis pemanfaatan Intranet

Penggunaan intranet tergantung dari bentuk organisasi penggunanya. Apakah suatu toko, perusahaan multi nasional, suatu instansi atau departemen lainnya. Dengan memahami kerja organisasi tersebut terlebih dahulu, maka akan sangat membantu model desain intranet yang akan digunakan.

Pemanfaatan Intranet dalam suatu organisasi, banyak digunakan untuk:

- ❖ Human resource personal services
- ❖ Material and logistic services, seperti penyediaan ruangan, barang dan sebagainya.
- ❖ Information system services, dll.

Human Resource Services

Pada model organisasi ini Intranet dapat digunakan untuk menyajikan informasi-informasi, seperti:

- ❖ Manual pekerja, misal tata-tertib, petunjuk kerja, informasi liburan, asuransi, prosedur pembelian dan pengeluaran barang.
- ❖ Bulletin board perusahaan, misal pengumuman kebijaksanaan, pengumuman pekerjaan, jadwal kerja, pelatihan, menu kafeteria, jadwal kegiatan extra.
- ❖ Record pekerja, misal waktu kerja dan kehadiran, data kepegawaian, seperti alamat rumah hingga prestasi kerja.
- ❖ Newsletter (berita-berita penting) untuk pekerja.
- ❖ Informasi-informasi yang berkaitan dengan human resource department, misal informasi yang digunakan untuk menyewa property, memecat, memindahkan, mempromosikan, melatih karyawan dan lain lain.

Materiel and Logistic Services

Organisasi kerja seperti ini dapat berupa toko, cleaning services, dan lain lain. Informasi yang dapat diletakkan di intranet misalnya :

- ❖ Listing peralatan atau services yang disediakan
- ❖ Image yang dapat di-click, yang menerangkan gambaran suatu fasilitas ruangan pada suatu kantor.
- ❖ Image map yang dapat menerangkan buku telephone suatu perusahaan.
- ❖ Suatu form yang dapat diisi dan digunakan untuk mencari informasi mengenai, order, katalog dan lain sebagainya.

Information System Services

Pada model ini Intranet dapat digunakan untuk menyediakan informasi seperti:

- ❖ Informasi mengenai komputer-komputer para staff.



- ❖ Informasi yang dibutuhkan para user, berkaitan dengan pengetahuan umum, manual operasi program untuk suatu pekerjaan, dapat dikumpulkan pada suatu database, sehingga dapat berupa suatu perpustakaan elektronis.
- ❖ Semua data atau dokumen yang berbentuk file word processing, spreadsheet, graphic dll, dapat digunakan bersama-sama dengan memanfaatkan aplikasi berbasis web dengan pusat data di web server.

3.1.3 Komponen Pembentuk Intranet

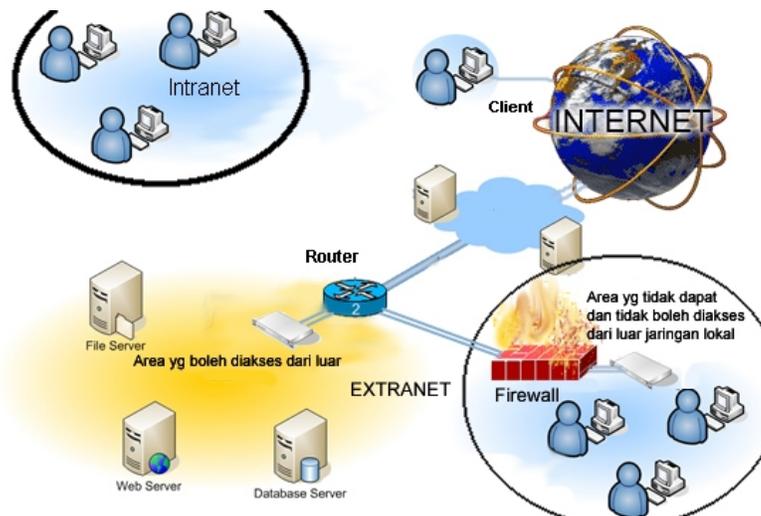
Komponen pembentuk intranet pada dasarnya sama dengan komponen pembentuk Internet, seperti :

1. Aplikasi browser
2. Komputer server
3. Perangkat jaringan dan
4. Protokol TCP/IP
5. Bahasa pemrograman
6. Komputer client
7. Perangkat bantu (development tool) untuk manajemen jaringan lokal.

3.2 Extranet

Extranet merupakan jaringan intranet perusahaan yang ingin mengekspose sebagian informasi yang mereka miliki ke jaringan luar. Informasi yang diekspose bisa berupa info produk/layanan, file-file yang diperlukan konsumen, klien atau karyawan yang mobile, atau juga database yang diperkenankan diakses dari jaringan lain atau jaringan internet.

Firewall akan memproteksi sebagian jaringan internal perusahaan sehingga tidak dapat diakses dari jaringan luar, sekaligus membatasi akses jaringan internal agar tidak dapat mengakses semua layanan/service dari internet.



Gambar 3.1. Intranet, Extranet dan Internet

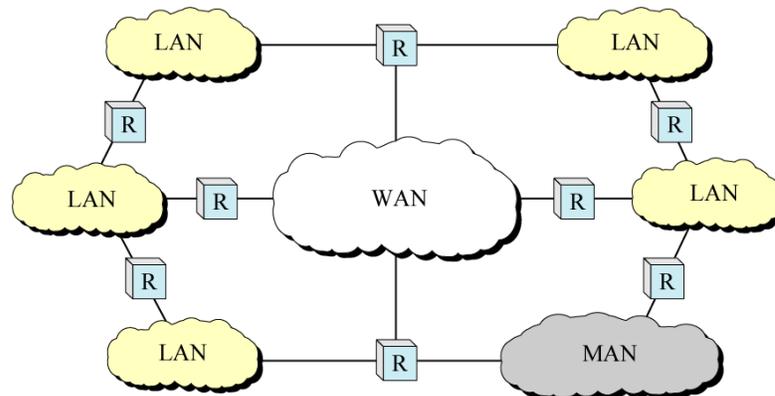


3.3 Internet

Interconnected Network atau yang lebih populer dengan sebutan **internet** adalah sebuah sistem komunikasi global yang menghubungkan komputer-komputer dan jaringan-jaringan komputer di seluruh dunia.

Setiap komputer dan jaringan, terhubung secara langsung maupun tidak langsung ke beberapa jalur utama yang disebut **internet backbone** dan dibedakan satu dengan yang lainnya menggunakan *unique name* yang biasa disebut dengan *alamat IP* 32 bit. Contoh: 202.65.124.130.

Secara harafiah, internet ('inter-network') adalah rangkaian komputer yang terhubung ke beberapa jaringan lain. Ketika komputer terhubung secara global dengan menggunakan TCP/IP sebagai protokol pertukaran paket data (*packet switching communication protocol*), maka rangkaian jaringan komputer yang besar ini dapat dinamakan **internet**. Cara menghubungkan rangkaian komputer dengan kaedah ini dinamakan internetworking.



Gambar 3.2. Internetworking

Internetworking merupakan kumpulan jaringan lokal area, juga metropolitan area yang umumnya terhubung melalui router-router sehingga membentuk jaringan wide area yang begitu besar. Terkoneksi ke internet berarti menghubungkan perangkat komputer atau perangkat lain yang digunakan, kedalam jaringan komputer global di dunia.

Tidak hanya perangkat komputer seperti Router, PC, Laptop atau server yang bisa terkoneksi ke internet, beberapa perangkat lain seperti mobile device (ponsel/PDA), web camera, security camera, alarm, refrigerator (lemari es), TV, remote control home/office device (seperti: instalasi lampu ruangan/taman) dan perangkat pribadi lainnya, juga dapat terkoneksi ke internet.

3.3.1 Kemunculan Internet

Rangkaian pusat yang membentuk internet diawali pada tahun 1969 sebagai ARPANET, yang dibangun oleh ARPA (United States Department of Defense Advanced Research Projects Agency). Beberapa penyelidikan awal yang disumbang oleh ARPANET termasuk kaedah rangkaian tanpa pusat (decentralised network), teori queueing, dan kaedah pertukaran paket (packet switching).

Pada 01 Januari 1983, ARPANET menukar protokol rangkaian pusatnya, dari NCP ke TCP/IP. Ini merupakan awal dari internet yang kita kenal hari ini. Pada sekitar 1990-an, internet telah berkembang dan menyambungkan banyak pengguna jaringan-jaringan komputer yang ada.





3.3.2 Internet pada saat ini

Intenet diatur oleh perjanjian bilateral atau multilateral dan spesifikasi teknis (*protokol yang ditetapkan dan disepakati untuk digunakan bersama, menerangkan tentang perpindahan data antar jaringan*). Protokol-protokol ini umumnya dibentuk berdasarkan kesepakatan (ketetapan).

Badan yang mengatur registrasi internet adalah IETF (Internet Engineering Task Force), yang terbuka kepada umum. Badan ini mengeluarkan dokumen yang dikenali sebagai RFC (Request for Comments). Sebagian dari RFC dijadikan sebagai standar internet, oleh Badan Arsitektur Internet (Internet Architecture Board).

Protokol-protokol internet yang sering digunakan adalah seperti, IP, TCP, UDP, DNS, PPP, SLIP, ICMP, POP3, IMAP, SMTP, HTTP, HTTPS, SSH, Telnet, FTP, LDAP, dan SSL.

Beberapa layanan populer di internet yang menggunakan protokol di atas, seperti email (surat elektronik), Usenet, Newsgroup, File Sharing, WWW (World Wide Web), Gopher, Session Access, WAIS, Finger, IRC, MUD, MUSH dll.

Di antara semua ini, email (surat elektronik) dan World Wide Web (www) lebih kerap digunakan, dan lebih banyak servis yang dibangun berdasarkannya, seperti milis (Mailing List) dan Weblog. Internet memungkinkan adanya servis terkini (Real-time service), seperti radio streaming, dan webcast, yang dapat diakses di seluruh dunia. Beberapa servis internet yang populer berdasarkan sistem tertutup (Proprietary System), seperti IRC, ICQ, AIM, CDDDB, dan Gnutella.

3.3.3 Budaya Internet

Jumlah pengguna internet yang besar dan semakin berkembang, telah mewujudkan budaya internet. Internet juga mempunyai pengaruh yang besar atas ilmu, dan pandangan dunia. Dengan hanya berpandukan mesin pencari seperti Google, pengguna di seluruh dunia mempunyai akses yang mudah atas bermacam-macam informasi. Dibanding dengan buku dan perpustakaan, internet melambangkan penyebaran (decentralization) informasi dan data secara ekstrim.

Perkembangan internet juga telah mempengaruhi perkembangan ekonomi. Berbagai transaksi jual beli yang sebelumnya hanya bisa dilakukan dengan cara tatap muka (dan sebagian sangat kecil melalui pos atau telepon), kini sangat mudah dan sering dilakukan melalui internet. Transaksi melalui internet ini dikenal dengan nama e-commerce. Terkait dengan pemerintahan, Internet juga memicu tumbuhnya transparansi pelaksanaan pemerintahan melalui e-government.

Internet membentuk budaya baru dikalangan pengguna. Kebiasaan baru mencari informasi, cara memandang sebuah masalah/kejadian, cara baru mencari/menyebarkan berita/isu, cara baru berbelanja atau memesan barang, dll.

3.3.4 Akses Internet

Negara dengan akses internet terbaik, termasuk USA, Germany, UK, Japan dan South Korea, umumnya memiliki penetrasi penggunaan internet yang cukup baik. Berbeda dengan Indonesia atau negara berkembang lain, yang penetrasi internetnya baru 7.0 % dari sekitar 219.307.147 populasi penduduk Indonesia berdasarkan survey **C.I.Almanac Feb./05** yang dipaparkan Internet World Statistic Last update March 23, 2005 (<http://www.internetworldstats.com/top20.htm>).



Tabel 3.1. TOP 20 COUNTRIES WITH HIGHEST NUMBER OF INTERNET USERS

No	Country or Region	Internet Users, Latest Data	Population (2005 Est.)	Internet Penetration	Source and Date of Latest Data	% Users of World
1	United States	200,933,147	296,208,476	67.8 %	Nielsen//NR Feb./05	22.6 %
2	China	94,000,000	1,282,198,289	7.3 %	CNNIC Dec./04	10.6 %
3	Japan	67,677,947	128,137,485	52.8 %	Nielsen//NR Nov./04	7.6 %
4	Germany	46,312,662	82,726,188	56.0 %	Nielsen//NR Feb./05	5.2 %
5	India	39,200,000	1,094,870,677	3.6 %	C.I.Almanac Feb./05	4.4 %
6	United Kingdom	35,179,141	59,889,407	58.7 %	Nielsen//NR Feb./05	4.0 %
7	Korea (South)	31,600,000	49,929,293	63.3 %	KRNIC Dec./04	3.6 %
8	Italy	28,610,000	58,608,565	48.8 %	C.I.Almanac Dec./03	3.2 %
9	France	24,848,009	60,293,927	41.2 %	Nielsen//NR Feb./05	2.8 %
10	Russia	22,300,000	144,003,901	15.5 %	C.I.Almanac Feb./05	2.5 %
11	Canada	20,450,000	32,050,369	63.8 %	C.I.Almanac Dec./03	2.3 %
12	Brazil	17,945,437	181,823,645	9.9 %	Nielsen//NR Feb./05	2.0 %
13	Indonesia	15,300,000	219,307,147	7.0 %	C.I.Almanac Feb./05	1.7 %
14	Spain	14,590,180	43,435,136	33.6 %	Nielsen//NR Feb./05	1.6 %
15	Australia	13,611,680	20,507,264	66.4 %	Nielsen//NR Feb./05	1.5 %
16	Mexico	12,250,000	103,872,328	11.8 %	ITU Sept./04	1.4 %
17	Taiwan	12,200,000	22,794,795	53.5 %	FIND Dec./04	1.4 %
18	Netherlands	10,806,328	16,316,019	66.2 %	Nielsen//NR June/04	1.2 %
19	Poland	10,600,000	38,133,891	27.8 %	C-I-A Feb./05	1.2 %
20	Malaysia	9,513,100	26,500,699	35.9 %	MCMC Sep./04	1.1 %
TOP 20 Countries		727,927,531	3,961,607,501	18.4 %	IWS - Mar./05	81.9 %
Rest of the World		160,753,600	2,450,459,684	6.6 %	IWS - Mar./05	18.1 %
TotalWorld - Users		888,681,131	6,412,067,185	13.9 %	IWS - Mar./05	100 %

3.3.5 Teknologi Koneksi Internet

Satu unit komputer atau komputer di jaringan dapat terkoneksi keinternet menggunakan jalur:

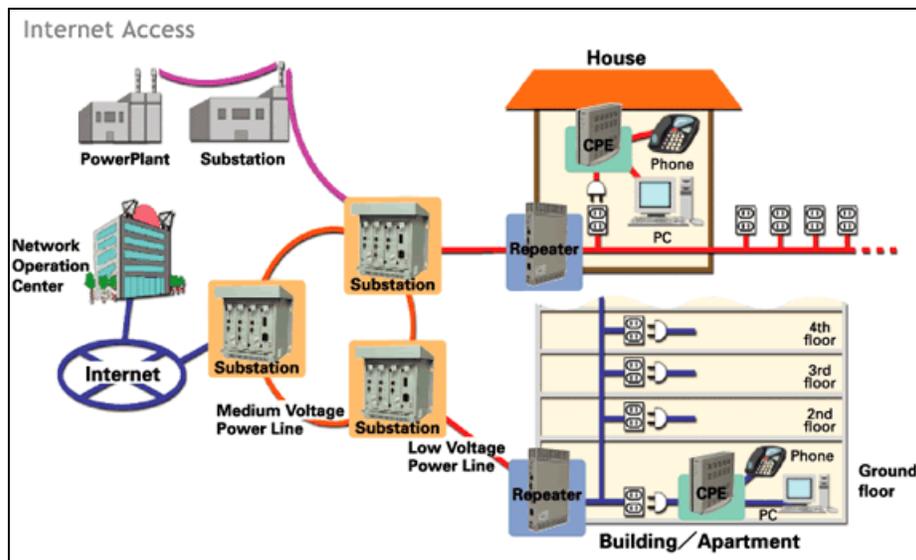
- a. **Public Line (jalur umum)**, seperti:



1. **Dial-up melalui jalur PSTN** (Public Switched Telephone Network) - Client (komputer user) terhubung ke ISP (Internet Service Provider) melalui jaringan telephone reguler (PSTN).
2. **Dial-up dengan teknologi GPRS** (General Packet Radio Service) dan **CDMA** (Code Division Multiple Access) - Perangkat ponsel berfungsi sebagai modem yang terhubung ke komputer melalui kabel data ponsel (port comm atau USB), IRDA juga Bluetooth. Koneksi internet melalui operator selular yang bertindak sebagai ISP, dengan mengatur konfigurasi pada komputer maupun ponsel.
3. **DSL (Digital Subscriber Line)** - Sebuah metode transfer data melalui saluran telepon reguler. Sirkuit DSL dikonfigurasi untuk menghubungkan dua lokasi yang spesifik, seperti halnya pada sambungan Leased Line. DSL berbeda dengan Leased Line. Koneksi melalui DSL jauh lebih cepat dibandingkan dengan koneksi melalui saluran telepon reguler walaupun keduanya sama-sama menggunakan kabel tembaga (jalur PSTN).

4. **PLC (PowerLine Communication)**

Koneksi PC dengan internet menggunakan jalur listrik PLN yang bertindak sebagai ISP, dengan bantuan modem yang langsung dapat ditancapkan ke stop kontak yang telah beraliran listrik.



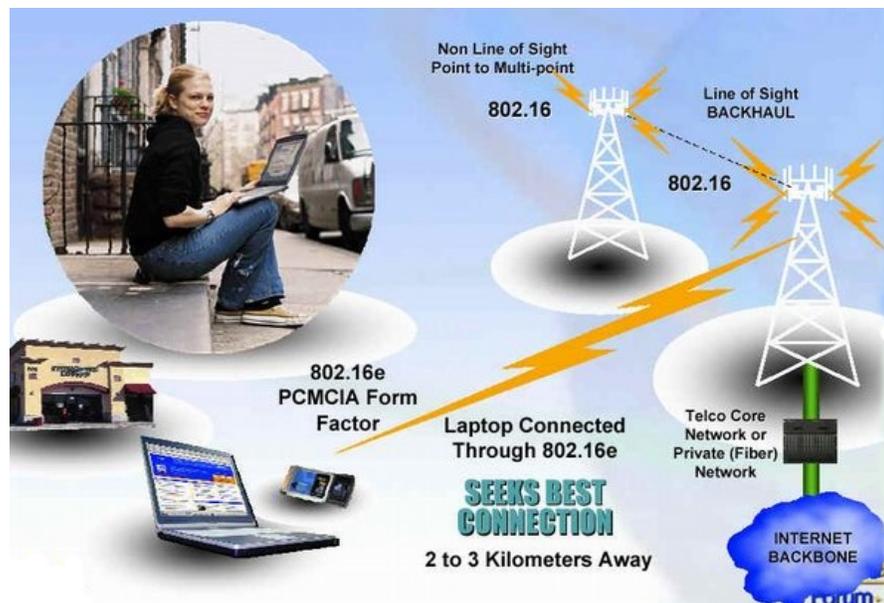
Gambar 3.3. PowerLine communication

5. **ADSL (Asynchronous Digital Subscriber Line)** dengan modem dan router merupakan sebuah tipe DSL dimana upstream dan downstream berjalan pada kecepatan yang berbeda. Dalam hal ini, downstream biasanya lebih tinggi. Teknologi ADSL memungkinkan user dapat memisahkan pemanfaatan jalur telephone reguler untuk keperluan komunikasi reguler dan koneksi internet.
6. **ISDN (Integrated Services Digital Network)** Pada dasarnya, ISDN merupakan jalan untuk melayani transfer data dengan kecepatan lebih tinggi melalui saluran telepon reguler. ISDN memungkinkan kecepatan transfer data hingga 128.000 bps (bit per detik). Tidak seperti DSL, ISDN dapat dikoneksikan dengan lokasi lain seperti halnya saluran telepon.



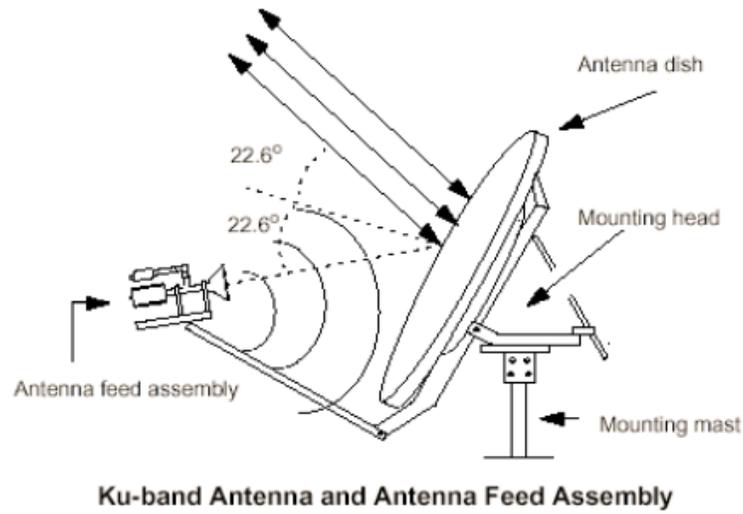
b. **Dedicated Line (jalur khusus internet)**, seperti:

1. **Leased line** adalah saluran koneksi telepon permanen antara dua titik yang disediakan oleh perusahaan telekomunikasi publik. Umumnya, *leased line* digunakan ketika terdapat kebutuhan komunikasi data jarak jauh yang harus dilakukan secara terus-menerus. *Leased line* memiliki beberapa tingkatan tarif yang bergantung kepada lebar jalur data (*Bandwidth*) yang mampu dikirimkan melalui *leased line* tersebut.
2. **Terrestrial** – menggunakan media kabel atau nirkabel sebagai aksesnya, dapat menggunakan kabel coaxial atau fiber optik yang disewa khusus untuk penggunaan koneksi internet selama 24 jam sehari atau untuk menghubungkan beberapa komputer dari satu lokasi ke lokasi lain (Frame Relay dan MPLS termasuk jenis layanan ini).
3. **Frame Relay** - layanan data paket yang memungkinkan beberapa user menggunakan satu jalur transmisi pada waktu yang bersamaan. Untuk lalu lintas komunikasi yang padat, Frame Relay jauh lebih efisien dari pada sirkuit sewa (leased line) yang disediakan khusus untuk satu pelanggan (dedicated), yang umumnya hanya terpakai 10% sampai 20% dari kapasitas bandwidth-nya.
4. **Fixed Wireless** – Koneksi perangkat mobile ke accesspoint atau Koneksi jaringan lokal ke ISP dengan perangkat radio/antenna dengan gelombang micro Wi-Fi 2.4 GHz (free-license), Microwave 3.3 GHz, 5.8 GHz, 10.5 GHz, 15 GHz (license) dan WiMAX 3,5 GHz.



Gambar 3.4. Teknologi WiMAX

5. **VSAT (Very Small Aperture Terminal)** - pilihan bagi mereka yang berada di tempat terpencil dan membutuhkan koneksi internet dimana tidak ada infrastruktur lain seperti leased line, ADSL, ISDN, bahkan tidak juga telepon. Antena VSAT berbentuk seperti piringan yang berukuran besar dan menghadap ke langit (satelit). Dengan peralatan ini maka sinyal digital diterima dan dikirimkan ke satelit. Satelit berfungsi sebagai penerus sinyal untuk dikirimkan ke titik lainnya di atas bumi.



Gambar 3.5. Antena VSAT (Ku-band Antenna)

6. **MPLS (Multiprotocol Label Switching)** - adalah jaringan pita lebar yang berbasis IP, MPLS memiliki jangkauan wilayah yang luas. Layanan ini memberikan layanan *end to end* dengan pilihan *bandwidth* kecil hingga kapasitas yang tak terhingga.

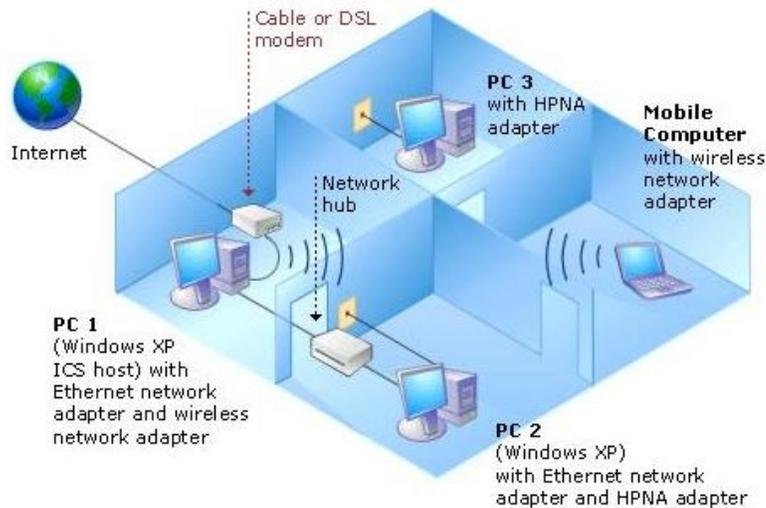
3.3.6 Penggunaan Internet di tempat umum

Internet juga semakin banyak digunakan di tempat umum. Beberapa tempat umum yang menyediakan layanan internet seperti toko-toko atau kampus-kampus juga hotel-hotel yang menyediakan akses **wi-fi (hotspot)**. Pengguna hanya perlu menyewa penggunaan komputer, atau membawa laptop (notebook) dan PDA, yang mempunyai teknologi wi-fi untuk mendapatkan akses internet (melalui access point - hotspot area), koneksi diberikan secara free atau dengan membeli voucher.

Terdapat juga tempat awam yang menyediakan pusat akses internet, seperti Warung Internet (warnet), Internet Café, Kios Internet, Public Access Terminal, dan Telepon Web, dimana pengguna hanya perlu menyewa penggunaan komputer untuk beberapa waktu.

Berikut ini adalah diagram sederhana yang menjelaskan bagaimana sambungan internet dihadirkan ke dalam kantor atau rumah anda, menggunakan jaringan yang mendukung kabel UTP dan wireless (hybrid) dengan sharing gateway menggunakan sebuah PC server.





Gambar 3.6. Membangun koneksi internet di rumah/kantor

3.4 Rangkuman

Intranet merupakan sebuah jaringan internal perusahaan yang dibangun menggunakan teknologi internet (arsitektur berupa aplikasi web dan menggunakan protokol TCP/IP). Extranet merupakan jaringan intranet perusahaan yang ingin mengekspose sebagian informasi yang mereka miliki ke jaringan luar. Internet adalah sebuah sistem komunikasi global yang menghubungkan komputer-komputer dan jaringan-jaringan komputer di seluruh dunia.

Awalnya teknologi intranet datang bersama dengan teknologi internet. Perbedaannya adalah pada penggunaan **firewall** bagi jaringan lokal intranet yang terkoneksi ke internet, agar dapat melindungi aset sistem informasi yang dimiliki perusahaan dari serangan pihak luar. Hal ini menjadikan intranet benar-benar dapat berfungsi secara independen dari internet, karena tidak terhubung dengan jaringan luar.

Hal lain yang membedakan intranet dan internet adalah dari sisi penggunaannya. Aplikasi dan informasi intranet ditujukan bagi kalangan dalam organisasi itu. Sedangkan informasi di suatu situs internet ditujukan bagi kalangan umum.

Teknologi yang digunakan untuk menghubungkan PC atau komputer di jaringan ke internet, antara lain melalui: Publik Line dan Dedicare Line.

Public Line menggunakan teknik dial-up melalui jalur PSTN, teknologi GPRS, CDMA, DSL, ADSL, ISDN hingga PLC. Teknologi ini menggunakan perangkat yang disebut modem yang berfungsi sebagai penghubung/koneksi ke penyedia jasa internet (ISP).

Dedicare Line merupakan jalur khusus yang hanya digunakan untuk keperluan koneksi internet. Koneksi dapat menggunakan media kabel (leased line maupun teresterial), wireless (Wi-Fi, Microwave, WiMAX), Frame Relay, VSAT maupun MPLS.

3.5 Soal Latihan :

1. Jelaskan perbedaan antara Intranet – Extranet dan Internet.
2. Apa persamaan yang dimiliki antara intranet dan internet
3. Apakah jaringan lokal (LAN) dapat disebut dengan intranet?



4. Jelaskan komponen-komponen pembentuk intranet
5. Apa yang membedakan pengembangan suatu intranet dibandingkan sistem client server biasa ?
6. Ada berapa cara / teknologi yang dapat kita gunakan untuk melakukan koneksi ke internet.
7. Apa jenis-jenis pelanggaran yang paling banyak terjadi di internet.
8. Apakah Indonesia sudah memiliki aturan-aturan (hukum) yang mengatur tentang pelanggaran hak cipta, pornografi, pelecehan dan lain-lain yang terkait dengan kegiatan di internet (Cyberlaw).
9. Apa yang anda ketahui tentang kegiatan Hacking dan Carding.
10. Apa yang anda ketahui tentang hotspot (untuk koneksi internet) dan apa hubungannya dengan laptop.

DAFTAR PUSTAKA

<http://www.internetworldstats.com/top20.htm>

Pengantar Jaringan Komputer, Melwin Syafrizal, Andi Offset, Jogja, 2005





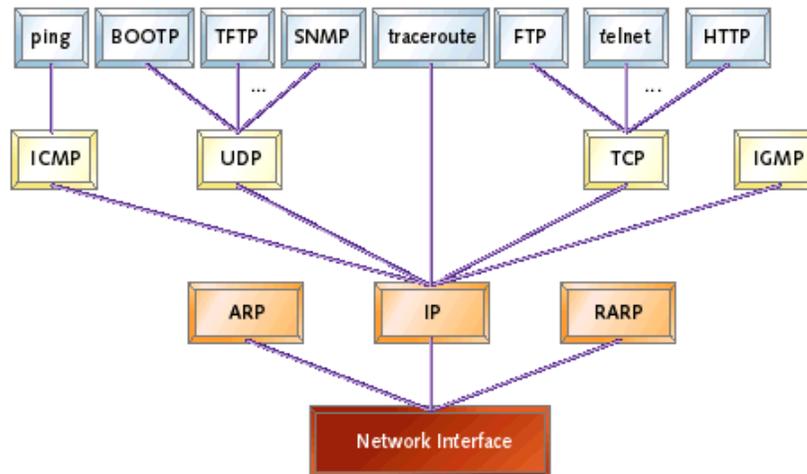
TCP/IP & IP ADDRESS

Kopetensi Dasar: Memahami konsep dasar TCP/IP dan protokol-protokol di lingkungan TCP/IP, dan konsep pengalaman menggunakan IP Address.

4.1 Konsep Dasar TCP/IP

4.1.1 Apa itu TCP/IP ?

TCP/IP adalah sekumpulan protokol yang terdapat di dalam jaringan komputer (network) yang digunakan untuk berkomunikasi atau bertukar data antar komputer. TCP/IP merupakan standar protokol pada jaringan internet yang menghubungkan banyak komputer yang berbeda jenis mesin maupun sistem operasinya agar dapat berinteraksi satu sama lain.



Gambar 4.1. Beberapa protokol yang terdapat pada TCP/IP

4.1.2 Apa yang membuat TCP/IP menjadi penting ?

Karena TCP/IP merupakan protokol yang telah diterapkan pada hampir semua perangkat keras dan sistem operasi, maka rasanya tidak ada rangkaian protokol lain yang begitu powerful kemampuannya untuk dapat bekerja pada semua lapisan perangkat keras dan sistem operasi seperti berikut ini

- Novell Netware.
- Mainframe IBM.
- Sistem Digital VMS.
- Microsoft Windows Server.
- Server & workstation UNIX, LinuX, FreeBSD, Open BSD.
- Macintosh.



g. PC DOS dan lain-lain.

4.1.3 Bagaimana awalnya keberadaan TCP/IP ?

Konsep TCP/IP berawal dari kebutuhan DoD (Departement of Defense) USA akan suatu komunikasi di antara berbagai variasi komputer yang telah ada. Komputer-komputer DoD ini seringkali harus menghubungkan antara satu organisasi peneliti dengan organisasi peneliti lainnya. Komputer tersebut harus tetap berhubungan karena terkait dengan pertahanan negara dan sumber informasi harus tetap berjalan meskipun terjadi bencana alam besar, seperti ledakan nuklir, dll sbg. Oleh karenanya pada tahun 1969 dimulailah penelitian terhadap serangkaian protokol TCP/IP.

Adapun tujuan-tujuan penelitian tersebut adalah sebagai berikut :

1. Terciptanya protokol-protokol umum, (DoD memerlukan suatu protokol yang dapat dipergunakan untuk semua jenis jaringan).
2. Meningkatkan efisiensi komunikasi data.
3. Dapat dipadukan dengan teknologi WAN (Wide Area Network) yang telah ada
4. Mudah dikonfigurasi.

Tahun 1968 DoD ARPAnet (Advanced Reseach Project Agency) memulai penelitian yang kemudian menjadi cikal bakal packet switching. Packet switching inilah yang memungkinkan komunikasi antara lapisan network, dimana data dijalankan dan disalurkan melalui jaringan dalam bentuk unit-unit kecil yang disebut packet. Tiap-tiap packet ini membawa informasi alamatnya masing-masing yang ditangani dengan khusus oleh jaringan tersebut dan tidak tergantung dengan paket-paket lain. Jaringan yang dikembangkan ini, yang menggunakan ARPAnet sebagai tulang punggungnya, menjadi terkenal sebagai **internet**.

Protokol-protokol TCP/IP dikembangkan lebih lanjut pada awal 1980 dan menjadi protokol standard untuk ARPAnet pada tahun 1983. Protokol-protokol ini mengalami peningkatan popularitas di komunitas pemakai ketika TCP/IP dapat di implementasikan dengan sangat baik pada versi 4.2 BSD (Berkeley Standard Distribution) UNIX. Versi ini digunakan secara luas pada institusi penelitian dan pendidikan serta digunakan sebagai dasar dari beberapa penerapan UNIX komersial, termasuk SunOS dari Sun dan Ultrix dari Digital.

4.1.4 Layanan apa saja yang diberikan oleh TCP/IP ?

Beberapa layanan "tradisional" yang dilakukan TCP/IP, diantaranya :

- a. Pengiriman File – File Transfer Protocol (FTP)
- b. Remote Login – Network Terminal Protocol (Telnet)
- c. E-mail – SMTP (Simple Mail Transfer Protocol)
- d. Network File System (NFS)
- e. Remote Execution

4.1.5 Bagaimana TCP dan IP bekerja ?

Seperti yang telah dikemukakan diatas, TCP dan IP hanyalah merupakan protokol yang bekerja pada suatu layer dan menjadi penghubung antara satu komputer dengan komputer lainnya dalam network, meskipun ke dua komputer tersebut memiliki OS yang berbeda. Untuk mengerti lebih jauh mari kita tinjau proses pengiriman sebuah email.

Dalam pengiriman email ada beberapa prinsip dasar yang harus dilakukan:





- ❖ Pertama, mencakup hal-hal umum seperti siapa yang mengirim email, siapa yang menerima email tersebut serta isi dari email tersebut.
- ❖ Kedua, bagaimana cara agar email tersebut sampai ketujuannya yang benar.

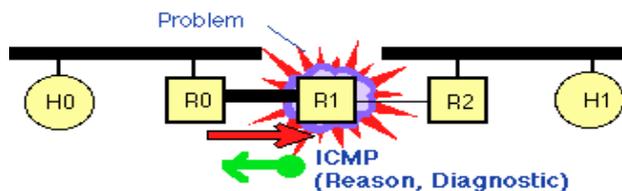
Dari konsep ini kita dapat mengetahui bahwa pengirim email memerlukan "perantara" yang memungkinkan emailnya sampai ketujuan (seperti layaknya pak pos), dan ini adalah tugas dari protokol TCP dan IP.

Antara TCP dan IP ada pembagian tugas masing-masing:

- ❖ **TCP** merupakan connection-oriented, yang berarti bahwa kedua komputer yang ikut serta dalam pertukaran data harus melakukan hubungan terlebih dulu sebelum pertukaran data berlangsung (dalam hal ini email). Selain itu TCP juga bertanggungjawab untuk menyakinkan bahwa email tersebut akan sampai ke tujuan, memeriksa kesalahan dan mengirimkan error ke lapisan atas hanya bila TCP tidak berhasil melakukan hubungan (hal inilah yang membuat TCP sukar untuk dikelabui). Jika isi email tersebut terlalu besar untuk satu datagram, TCP akan membaginya kedalam beberapa datagram.
- ❖ **IP** bertanggung jawab setelah hubungan berlangsung, tugasnya adalah untuk me-rute-kan paket data, didalam network. IP hanya bertugas sebagai kurir dari TCP dan mencari jalur yang terbaik dalam penyampaian datagram, IP "tidak bertanggung jawab" jika data tersebut tidak sampai dengan utuh (hal ini disebabkan IP tidak memiliki informasi mengenai isi data yang dikirimkan), namun IP akan mengirimkan pesan kesalahan (error message) melalui **ICMP**, jika hal ini terjadi dan kemudian kembali ke sumber data.

Karena IP "hanya" mengirimkan data "tanpa" mengetahui urutan data mana yang akan disusun berikutnya, maka hal ini menyebabkan IP mudah untuk dimodifikasi di daerah "sumber dan tujuan" datagram. Hal inilah yang menjadi penyebab banyaknya paket data yang hilang sebelum sampai ke tujuan.

Datagram dan paket sering dipertukarkan penggunaannya. Secara teknis, datagram merupakan unit dari data, yang tercakup dalam protokol. ICMP adalah kependekan dari Internet Control Message Protocol yang bertugas memberikan pesan-pesan kesalahan dan kondisi lain yang memerlukan perhatian khusus. Pesan/paket ICMP dikirim jika terjadi masalah pada layer IP dan layer di atasnya (TCP dan UDP)



Gambar 4.2. Akibat kegagalan mengirim pesan, Pesan kesalahan ICMP disampaikan kesumber alamat pengirim

Berikut adalah beberapa pesan potensial yang sering timbul:

- Destination unreachable**, terjadi jika host, jaringan, port atau protokol tertentu tidak dapat dijangkau.
- Time exceeded**, dimana datagram tidak bisa dikirim karena time to live habis.





- c. **Parameter problem**, terjadi kesalahan parameter dan letak oktet dimana kesalahan terdeteksi.
- d. **Source quench**, terjadi karena router/host tujuan membuang datagram karena batasan ruang buffer atau karena datagram tidak dapat diproses.
- e. **Redirect**, pesan ini memberi saran kepada host asal datagram mengenai router yang lebih tepat untuk menerima datagram tsb.
- f. **Echo request** dan **echo reply message**, pesan ini saling mempertukarkan data antara host.

4.2 IP ADDRESS Versi 4

IP Address merupakan pengenalan yang digunakan untuk memberi alamat pada tiap-tiap komputer dalam jaringan. Format IP address adalah bilangan 32 bit yang tiap 8 bit-nya dipisahkan oleh tanda titik. Adapun format IP Address dapat berupa bentuk '*biner*' (xxxxxxxx.xxxxxxxxx.xxxxxxxxx.xxxxxxxxx dengan x merupakan bilangan biner 0 atau 1). Atau dengan bentuk empat bilangan desimal yang masing-masing dipisahkan oleh titik, bentuk ini dikenal dengan '*dotted decimal*' (xxx.xxx.xxx.xxx adapun xxx merupakan nilai dari 1 oktet yang berasal dari 8 bit).

Dikenal dua cara pembagian IP Address, yakni: *classfull* dan *classless addressing*.

4.2.1 Classfull Addressing

Classfull merupakan metode pembagian IP address berdasarkan kelas, dimana IP address (yang berjumlah sekitar 4 milyar) dibagi kedalam lima kelas yakni:

Kelas A

Format : 0nnnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh
Bit pertama : 0
Panjang NetID : 8 bit
Panjang HostID: 24 bit
Byte pertama : 0-127
Jumlah : 126 Kelas A (0 dan 127 dicadangkan)
Range IP : 1.xxx.xxx.xxx sampai 126.xxx.xxx.xxx
Jumlah IP : 16.777.214 IP Address disetiap Kelas A
Deskripsi : Diberikan untuk jaringan dengan jumlah host yang besar

Kelas B

Format : 10nnnnnnn.nnnnnnnn.hhhhhhhh.hhhhhhhh
Bit pertama : 10
Panjang NetID : 16 bit
Panjang HostID: 16 bit
Byte pertama : 128-191
Jumlah : 16.384 Kelas B
Range IP : 128.0.xxx.xxx sampai 191.255.xxx.xxx
Jumlah IP : 65.532 IP Address pada setiap Kelas B
Deskripsi : Dialokasikan untuk jaringan besar dan sedang





Kelas C

Format : 110nnnnn.nnnnnnnn.nnnnnnnn.hhhhhhhh
Bit pertama : 110
Panjang NetID : 24 bit
Panjang HostID : 8 bit
Byte pertama : 192-223
Jumlah : 2.097.152 Kelas C
Range IP : 192.xxx.xxx.xxx s/d 223.255.255.xxx
Jumlah IP : 254 IP Address pada setiap Kelas C
Deskripsi : Digunakan untuk jaringan berukuran kecil

Kelas D

Format : 1110mmmm.mmmmmmm.mmmmmmm.mmmmmmm
Bit pertama : 1110
Bit multicast : 28 bit
Byte inisial : 224-247
Deskripsi : Kelas D digunakan untuk keperluan IPmulticasting

Kelas E

Format : 1111rrrrr.rrrrrrrrr.rrrrrrrrr.rrrrrrrrr
Bit pertama : 1111
Bit cadangan : 28 bit
Byte inisial : 248-255
Deskripsi : Kelas E dicadangkan untuk keperluan eksperimen.

4.2.2 Classless Addressing

Metode **classless addressing** (pengalamatan tanpa kelas) saat ini mulai banyak diterapkan, yakni dengan pengalokasian IP Address dalam notasi Classless Inter Domain Routing (**CIDR**). Istilah lain yang digunakan untuk menyebut bagian IP address yang menunjuk suatu jaringan secara lebih spesifik, disebut juga dengan **Network Prefix**.

Biasanya dalam menuliskan network prefix suatu kelas IP Address digunakan tanda garis miring (*Slash*) “/”, diikuti dengan angka yang menunjukkan panjang network prefix ini dalam bit.

Misalnya, ketika menuliskan network kelas A dengan alokasi IP 12.xxx.xxx.xxx, network prefixnya dituliskan sebagai 12/8. Angka /8 menunjukkan notasi CIDR yang merupakan jumlah bit yang digunakan oleh network prefix, yang berarti netmask-nya 255.0.0.0 dengan jumlah maksimum host pada jaringan sebanyak 16.777.214 node.

Contoh lain untuk menunjukan suatu network kelas B 167.205.xxx.xxx digunakan: 167.205/18. Angka /18 merupakan notasi CIDR, yang berarti netmask yang digunakan pada jaringan ini adalah 255.255.192.0 dengan jumlah maksimum host pada jaringan sebanyak 16.382 node.

4.2.3 Pengalokasian IP address

IP Address terdiri atas dua bagian yaitu *network ID* dan *host ID*. Network ID menunjukkan nomor network, sedangkan hostID meng-identifikasi-host dalam satu network. Pengalokasian IP address pada dasarnya ialah proses memilih network ID dan host ID yang tepat untuk suatu jaringan. Tepat





atau tidaknya konfigurasi ini tergantung dari tujuan yang hendak dicapai, yaitu mengalokasikan IP address se-efisien mungkin.

Terdapat beberapa aturan dasar dalam menentukan network ID dan host ID yang hendak digunakan. Aturan tersebut adalah :

- ❖ Network ID 127.0.0.1 tidak dapat digunakan karena ia secara default digunakan dalam keperluan 'loop-back'. ('Loop-Back' adalah IP address yang digunakan komputer untuk menunjuk dirinya sendiri).
- ❖ Host ID tidak boleh semua bitnya diset 1 (contoh klas A: 126.255.255.255), karena akan diartikan sebagai alamat broadcast. ID broadcast merupakan alamat yang mewakili seluruh anggota jaringan. Pengiriman paket ke alamat ini akan menyebabkan paket ini didengarkan oleh seluruh anggota network tersebut.
- ❖ Network ID dan host ID tidak boleh sama dengan 0 (seluruh bit diset 0 seperti 0.0.0.0), Karena IP address dengan host ID 0 diartikan sebagai alamat network. Alamat network adalah alamat yang digunakan untuk menunjuk suatu jaringan, dan tidak menunjukan suatu host.
- ❖ Host ID harus unik dalam suatu network (dalam satu network, tidak boleh ada dua host dengan host ID yang sama).

Aturan lain yang menjadi panduan network engineer dalam menetapkan IP Address yang dipergunakan dalam jaringan lokal adalah sebagai berikut:

0/8 → 0.0.0.1 s.d. 0.255.255.254 Hosts/Net: 16.777.214
 10/8 → 10.0.0.1 s.d. 10.255.255.254 Hosts/Net: 16.777.214
 127/8 → 127.0.0.1 s.d. 127.255.255.254 Hosts/Net: 16.777.214
 169.254/16 → 169.254.0.1 s.d. 169.254.255.254 Hosts/Net: 65.534
 172.16/12 → 172.16.0.1 s.d. 172.31.255.254 Hosts/Net: 1.048.574
 192.0.2/24 → 192.0.2.1 s.d. 192.0.2.254 Hosts/Net: 254
 192.168/16 → 192.168.0.1 s.d. 192.168.255.254 Hosts/Net: 65.534

dan semua space dari klas D dan E dapat digunakan untuk IP Address local area network, karena IP ini tidak digunakan (di publish) di internet.

Filtered source addresses

0/8 ! broadcast
 10/8 ! RFC 1918 private
 127/8 ! loopback
 169.254.0/16 ! link local
 172.16.0.0/12 ! RFC 1918 private
 192.0.2.0/24 ! TEST-NET
 192.168.0/16 ! RFC 1918 private
 224.0.0.0/4 ! class D multicast
 240.0.0.0/5 ! class E reserved
 248.0.0.0/5 ! reserved
 255.255.255.255/32 ! broadcast





IP address, subnet mask, broadcast address merupakan dasar dari teknik routing di Internet. Untuk memahami ini, semua kemampuan matematika khususnya matematika boolean, atau matematika binary akan sangat membantu memahami konsep routing Internet dan pengalaman IP.

4.2.4 Alokasi IP Address di Jaringan

Teknik subnet merupakan cara yang biasa digunakan untuk mengalokasikan sejumlah alamat IP di sebuah jaringan (LAN atau WAN). Teknik subnet menjadi penting bila kita mempunyai alokasi IP yang terbatas misalnya hanya ada 200 IP untuk 200 komputer yang akan di distribusikan ke beberapa LAN.

Untuk memberikan gambaran, misalkan kita mempunyai alokasi alamat IP dari 192.168.1/24 untuk 254 host, maka parameter yang digunakan untuk alokasi tersebut adalah:

- 255.255.255.0 - subnet mask LAN
- 192.168.1.0 - network address LAN.
- 192.168.1.1 s/d 192.168.1.254 – IP yang digunakan host LAN
- 192.168.1.255 - broadcast address LAN
- 192.168.1.25 - contoh IP salah satu workstation di LAN.

Perhatikan bahwa,

- ❖ Alamat IP pertama 192.168.1.0 tidak digunakan untuk *workstation*, tapi untuk menginformasikan bahwa LAN tersebut menggunakan alamat 192.168.1.0. Istilah keren-nya alamat IP 192.168.1.0 di sebut *network address*.
- ❖ Alamat IP terakhir 192.168.1.255 juga tidak digunakan untuk workstation, karena digunakan untuk alamat *broadcast*. Alamat broadcast digunakan untuk memberikan informasi ke seluruh workstation yang berada di network 192.168.1.0 tersebut. Contoh informasi broadcast adalah informasi routing menggunakan Routing Information Protocol (RIP).
- ❖ Subnetmask LAN 255.255.255.0, dalam bahasa yang sederhana dapat diterjemahkan bahwa setiap bit “1” menunjukkan posisi network address, sedang setiap bit “0” menunjukkan posisi *host address*.

Konsep network address dan host address menjadi penting sekali berkaitan erat dengan subnet mask. Perhatikan dari contoh di atas maka alamat yang digunakan adalah :

192.168.1.0	network address	11000000.10101000.00000000.00000000
192.168.1.1	host ke 1	11000000.10101000.00000000.00000001
192.168.1.2	host ke 2	11000000.10101000.00000000.00000010
192.168.1.3	host ke 3	11000000.10101000.00000000.00000011
.....		
192.168.1.254	host ke 254	11000000.10101000.00000000.11111110
192.168.1.255	broadcast address	11000000.10101000.00000000.11111111

Perhatikan bahwa angka 192.168.1 tidak pernah berubah sama sekali. Hal ini menyebabkan network address yang digunakan 192.168.1.0. Jika diperhatikan maka 192.168.1 terdiri dari 24 bit yang konstan tidak berubah, dan hanya 8 bit terakhir (bit hostID) yang berubah. Tidak heran kalau *netmask* yang digunakan adalah binary 11111111.11111111.11111111.00000000 (desimal = 255.255.255.0).

Walaupun alamat IP workstation tetap, tetapi netmask yang digunakan dimasing-masing router akan berubah-ubah bergantung pada posisi router dalam jaringan.





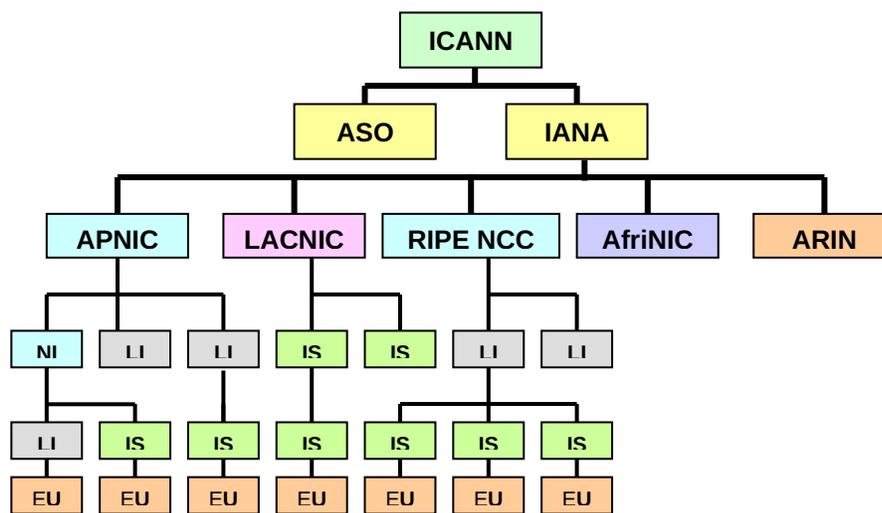
4.2.5 Alokasi Alamat IP

APJII mendapatkan pendelegasian wewenang dari APNIC untuk membagikan IP Address di Indonesia. PJI (ISP) di Indonesia akan memperoleh manfaat karena tidak perlu lagi menjadi anggota langsung dari APNIC (dengan biaya keanggotaan berkisar 2,500 – 10,000 USD per tahun) untuk mendapatkan alokasi IP address. Hal ini dapat juga dilihat sebagai upaya penghematan devisa.

Perusahaan yang membutuhkan alamat IP yang independen terhadap ISP juga dapat dilayani oleh APJII, dengan biaya alokasi yang akan ditetapkan kemudian.

4.2.6 Hirarki Pendistribusian IP Address v4

- *Address IPv4* didistribusikan sesuai dengan struktur hirarki yang dijabarkan secara sederhana, seperti struktur berikut:



Gambar 4.3. Hirarki distribusi *address space* IPv4

- Sejarahnya pengaturan nomor IP dan nama host diatur secara tersentral oleh IANA (Internet Assigned Numbers Authority), dimotori oleh Jon Postel (August 6, 1943 - October 16, 1998)
- *Daftar tabel di-download secara berkala*

Keterangan :

1. **ICANN** : Internet Corporation For Assigned Names and Numbers
2. **ASO** : The Address Supporting Organization
3. **IANA** : Internet Assigned Numbers Authority
4. **APNIC** : Asia Pasific Network Information Center
5. **ARIN** : American Registry for Internet Numbers
6. **LACNIC** : Latin American and Caribbean Internet Addresses Registry NIC
7. **RIPENCC** : RIPE Network Coordination Centre (**RIPE**: Réseaux IP Européens)
8. **AfriNIC** : African Network Information Center
9. **NIR** : National Internet Registry
10. **LIR** : Local Internet Registry
11. **ISP** : Internet Service Provider





12. EU : End user

ICANN mendelegasikan pendistribusian resource yang terkait dengan Address Space kepada ASO, IANA, dan DNSO. IANA mengalokasikan *address space* pada APNIC, untuk didistribusikan kembali ke seluruh kawasan Asia Pasifik.

APNIC mengalokasikan *address space* kepada *Internet Registries* (IRs) dan juga mendelegasikan wewenang kepada mereka untuk melakukan pendelegasian dan pengalokasian. Dalam beberapa kasus APNIC mendelegasikan *address space* kepada *end-user*/pengguna akhir. IR nasional dan lokal mengalokasikan dan mendelegasikan *address space* kepada anggota mereka dan para konsumen dibawah pengawasan APNIC sesuai dengan kebijakan dan prosedur yang ditetapkan

Bila ingin menggunakan IP Address Public yang dapat dikenali di internet, maka kita harus berhubungan dengan ISP tempat kita berlangganan koneksi internet, ISP nantinya yang akan mengalokasikan IP yang mereka punya ke anda.

Berikutnya untuk nama domain, anda harus memeriksakan apakah domain yang anda inginkan sudah didaftarkan fihak lain atau belum (cek di <http://www.domainregistry.com/>), kemudian mendaftarkan atau membeli domain name yang akan digunakan, Anda bisa minta bantuan ISP terdekat untuk hal ini, atau kontak langsung ke NSI atau reseller lain. (<http://www.networksolutions.com/>).



Gambar 4.4. Internet Map Region

4.3 Rangkuman

TCP/IP merupakan sekumpulan protokol yang terdapat di dalam jaringan komputer (network) yang digunakan untuk berkomunikasi atau bertukar data antar komputer. Protokol-protokol tersebut antara lain: TCP, IP, ICMP, UDP, SNMP, TFTP, FTP, HTTP, BOOTP, ARP, RARP, dll.

Konsep TCP/IP berawal dari kebutuhan DoD (Departement of Defense) USA akan suatu komunikasi di antara berbagai variasi komputer yang telah ada, DoD memerlukan suatu protokol yang dapat dipergunakan untuk semua jenis jaringan dan semua jenis platform.





TCP dan IP merupakan protokol yang berbeda, bekerja pada suatu layer yang menjadi penghubung antara satu komputer dengan komputer lainnya dalam jaringan, meskipun ke dua komputer tersebut memiliki OS yang berbeda.

IP Address merupakan pengenalan yang digunakan untuk memberi alamat pada tiap-tiap komputer dalam jaringan. Format IP address versi 4 adalah bilangan 32 bit yang tiap 8 bit-nya dipisahkan oleh tanda titik, contoh: 202.91.9.254.

IP Address terdiri atas dua bagian yaitu *network ID* dan *host ID*. Network ID menunjukkan nomor network, sedangkan hostID meng-identifikasi-kan host dalam satu network.

Pengalokasian IP Address dibagi dalam dua teknik pengalamatan: class addressing dan classless addressing. Class addressing menggunakan teknik pembagian IP berdasarkan kelas-kelas IP, sedangkan classless addressing menggunakan teknik CIDR maupun VLSM. CIDR merupakan teknik pendistribusian IP Address dari IANA (IP Public), sedangkan VLSM akan menerapkan teknik pengalokasian IP Private kedalam jaringan local.

Teknik subnet merupakan cara yang biasa digunakan untuk mengalokasikan sejumlah alamat IP di sebuah jaringan (LAN atau WAN). Penggunaan netmask non-default class (seperti: 255.255.255.248, 255.255.255.240, dll) akan membentuk jaringan dengan jumlah komputer terbatas (seperti 2, 6, 14, 30, 62 atau hanya 126 komputer dalam satu jaringan).

4.4 Soal Latihan:

Pilih satu atau beberapa jawaban yang anda anggap benar

1. Yang merupakan sekumpulan protokol dan terdapat di dalam jaringan komputer (network) yang digunakan untuk berkomunikasi atau bertukar data antar komputer, adalah protocol:
 - a. TCP/IP
 - b. IPX/SPX
 - c. PPP
 - d. AppleTalk
2. Apa yang membuat protocol TCP/IP menjadi penting, adalah karena:
 - a. Dapat dipakai oleh semua jenis mesin komputer
 - b. Kemampuannya untuk menjamin paket sampai ketujuan
 - c. Dapat diterapkan pada semua sistem operasi
 - d. Kemampuannya untuk mengatasi serangan dari luar
3. Tujuan awal penelitian terhadap serangkaian protokol TCP/IP yang dilakukan DoD (Departemen of Defence) USA adalah:
 - a. Terciptanya protokol-protokol umum
 - b. Meningkatkan efisiensi komunikasi data.
 - c. Dapat dipadukan dengan teknologi WAN yang ada
 - d. Mudah dikonfigurasi.
4. Jenis Layanan yang dilakukan oleh TCP/IP:
 - a. Pengiriman/pengambilan file (FTP) dari komputer lain
 - b. Remote login (telnet)
 - c. Memberikan inisial nama pada sebuah perangkat
 - d. Mengatur antrian data





5. Apabila IP gagal dalam melakukan pengiriman data, maka yang memberikan laporan kesalahan (error) yang terjadi adalah protocol:
 - a. TCP
 - b. IP
 - c. ICMP
 - d. Semua benar
6. User Datagram Protocol (UDP) adalah sebuah protokol yang bekerja pada transport layer, Protocol UDP ini tidak handal, karena:
 - a. Bekerja terlalu lama
 - b. Tidak ada duplikasi paket
 - c. Semua benar
 - d. Tidak menjamin paket akan sampai ketujuan
7. Nilai decimal dari 11001010.10011111.00010111.00101101 adalah:
 - a. 202.59.230.145
 - b. 202.159.23.45
 - c. 202.59.23.145
 - d. 202.159.23.145
8. Bila 11001010.10011111.00010111.00101101 di AND dengan 11111111.11111111.11111111.00000000, maka hasilnya adalah :
 - a. 11001010.10011111.00010111.00000000
 - b. 11001010.10011111.00010111.11111111
 - c. 00110101.01100000.11101000.00101001
 - d. 11111111.11111111.11111111.00101101
9. Bila seseorang membutuhkan sebuah IP Public untuk digunakan pada sebuah server yang akan ditempatkan on-line 24 jam di internet, maka dari mana orang tersebut dapat memperoleh IP Public yang diinginkan?
 - a. ISP
 - b. APJII
 - c. APNIC
 - d. IANA
10. Dari mana sebuah ISP di Indonesia memperoleh IP Address?
 - a. ISP lain.
 - b. APJII
 - c. APNIC
 - d. IANA

DAFTAR PUSTAKA

<http://www.apjii.or.id/>

Pengantar Jaringan Komputer, Melwin Syafrizal, Andi Offset, Jogja, 2005

TCP/IP dan Implementasinya, Onno W Purbo, Adnan Basalamah, Ismail Fahmi, Achmad Husni T, Elexmedia Komputindo 1999.





SUBNET & KONSEP ROUTING

Kopetensi Dasar: Mampu melakukan konfigurasi IP Address dikomputer jaringan, memahami konsep alokasi IP Public dengan metode Classless Addressing (CIDR), memahami konsep subnetting, memahami teknik penggunaan subnet mask dan dapat melakukan teknik subnetting menggunakan metode VLSM. Memahami konsep routing dan protokol routing.

5.1 Subnet

Jumlah IP Address Versi 4 sangat terbatas, apalagi jika harus memberikan alamat semua host di Internet. Oleh karena itu, perlu dilakukan efisiensi dalam penggunaan IP Address tersebut supaya dapat mengalami semaksimal mungkin host yang ada dalam satu jaringan.

Konsep subnetting dari IP Address merupakan teknik yang umum digunakan di Internet untuk mengefisienkan alokasi IP Address dalam sebuah jaringan supaya bisa memaksimalkan penggunaan IP Address.

Subnetting merupakan proses memecah satu kelas IP Address menjadi beberapa subnet dengan jumlah host yang lebih sedikit, dan untuk menentukan batas network ID dalam suatu subnet, digunakan subnet mask.

Seperti yang telah dijelaskan pada bab sebelumnya, bahwa selain menggunakan metode classfull untuk pembagian IP address, kita juga dapat menggunakan metode *classless addressing* (pengalamatan tanpa kelas), menggunakan notasi penulisan singkat dengan prefix.

Metode ini merupakan metode pengalamatan IPv4 tingkat lanjut, muncul karena ada ke-khawatiran persediaan IPv4 berkelas tidak akan mencukupi kebutuhan, sehingga diciptakan metode lain untuk memperbanyak persediaan IP address.

5.1.1 Classless Inter-Domain Routing (CIDR)

Diperkenalkan oleh lembaga IETF pada tahun 1992, merupakan konsep baru untuk mengembangkan Supernetting dengan Classless Inter-Domain Routing. CIDR menghindari cara pemberian IP Address tradisional menggunakan kelas A, B dan C. CIDR menggunakan “network prefix” dengan panjang tertentu. *Prefix-length* menentukan jumlah “bit sebelah kiri” yang akan dipergunakan sebagai network ID.

Jika suatu IP Address memiliki 16 bit sebagai network ID, maka IP address tersebut akan diberikan *prefix-length* 16 bit yang umumnya ditulis sebagai /16 dibelakang IP Address, contoh: 202.152.0.1/18. Oleh karena tidak mengenal kelas, CIDR dapat mengalokasikan kelompok IP address dengan lebih efektif.

Seperti contoh, jika satu blok IP address (202.91.8/26) dialokasikan untuk sejumlah host (komputer) yang akan dibagi dalam beberapa jaringan (subnet), maka setiap bagian (segmen/subnet) akan menerima porsi IP address yang sama satu sama lain.

Subnet 1 = 62 host – network address = 202.91.8.0/26



Subnet 2 = 62 host – network address = 202.91.8.64/26

Subnet 3 = 62 host – network address = 202.91.8.128/26

Subnet 4 = 62 host – network address = 202.91.8.192/26

Subnet Mask = 255.255.255.192

Bila salah satu subnet masih ingin memecah jaringannya menjadi beberapa bagian, misal subnet 4 masih akan dibagi menjadi 2 jaringan (subnet), maka 62 IP yang sebelumnya akan dialokasikan buat host subnet 4 akan dipecah menjadi 2 subnet lagi dengan jumlah host yang sama.

Subnet 4 = 30 host – network address = 202.91.8.192/27

Subnet 5 = 30 host – network address = 202.91.8.224/27

Subnet Mask = 255.255.255.224

Sisa host masing-masing subnet yang baru hanya 30 host, dikarenakan 1 IP sebagai identitas alamat Network dan 1 IP lainnya (yang terakhir) digunakan sebagai IP broadcast subnet tersebut.

5.1.2 Variable Length Subnet Mask (VLSM)

Jika pada pengalokasian IP address classfull, suatu network ID hanya memiliki satu subnetmask, maka VLSM menggunakan metode yang berbeda, yakni dengan memberikan suatu network address lebih dari satu subnetmask.

Perhatikan contoh berikut:

Satu blok IP address (169.254.0.0/20) dibagi menjadi 16.

Subnet 1 = 4094 host – Net address = 169.254.0.0/20

Subnet 2 = 4094 host – Net address = 169.254.16.0/20

Subnet 3 = 4094 host – Net address = 169.254.32.0/20

Subnet 4 = 4094 host – Net address = 169.254.64.0/20

...

Subnet 16 = 4094 host – Net address = 169.254.240.0/20

Subnet Mask = 255.255.240.0

Berikutnya Subnet 2 akan dipecah menjadi 16 subnet lagi yang lebih kecil.

Subnet 2.1 = 254 host – Net address = 169.254.16.0/24

Subnet 2.2 = 254 host – Net address = 169.254.17.0/24

Subnet 2.3 = 254 host – Net address = 169.254.18.0/24

...

Subnet 2.16 = 254 host – Net address = 169.254.31.0/24

Subnet Mask = 255.255.255.0

Bila subnet 2.1 akan dipecah lagi menjadi beberapa subnet, misal 4 subnet, maka:

Subnet 2.1.1 = 62 host – Net address = 169.254.16.0/26

Subnet 2.1.2 = 62 host – Net address = 169.254.16.64/26

Subnet 2.1.3 = 62 host – Net address = 169.254.16.128/26





Subnet2.1.4= 62 host – Net address = 169.254.16.192/26

Subnet Mask = 255.255.255.192

Nah...terlihatkan kalau pada Subnet 2 (Net address 169.254.16.0) dapat memecah jaringannya menjadi beberapa subnet lagi dengan mengganti Subnetmask-nya menjadi: 255.255.240.0, 255.255.255.0 dan 255.255.255.192.

Jika anda perhatikan, CIDR dan metode VLSM mirip satu sama lain, yaitu blok network address dapat dibagi lebih lanjut menjadi sejumlah blok IP address yang lebih kecil.

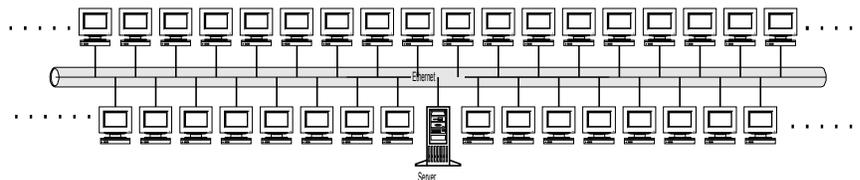
Perbedaannya adalah CIDR merupakan sebuah konsep untuk pembagian blok IP Public yang telah didistribusikan dari IANA, sedangkan VLSM merupakan implementasi pengalokasian blok IP yang dilakukan oleh pemilik network (network administrator) dari blok IP yang telah diberikan padanya (sifatnya local dan tidak dikenal di internet).

Esensi dari subnetting adalah “memindahkan” garis pemisah antara bagian network dan bagian host dari suatu IP Address. Beberapa bit dari bagian hostID dialokasikan menjadi bit tambahan pada bagian networkID. Address satu network menurut struktur baku dipecah menjadi beberapa subnetwork. Cara ini menciptakan sejumlah network tambahan dengan mengurangi jumlah maksimum host yang ada dalam tiap network tersebut.

Tujuan lain dari subnetting yang tidak kalah pentingnya adalah untuk mengurangi tingkat kongesti (gangguan/ tabrakan) lalulintas data dalam suatu network.

Perhatikan...!!! pengertian satu network secara logika adalah host-host yang tersambung pada suatu jaringan fisik. Misalkan pada suatu LAN dengan topologi bus, maka anggota suatu network secara logika haruslah host yang tersambung pada bentangan kabel tersebut. Jika menggunakan hub untuk topologi star, maka keseluruhan network adalah semua host yang terhubung dalam hub yang sama. Bayangkan jika network kelas B hanya dijadikan satu network secara logika, maka seluruh host yang jumlahnya dapat mencapai puluhan ribu itu akan “berbicara” pada media yang sama.

Jika kita perhatikan ilustrasi pada gambar berikut, hal ini sama dengan ratusan orang berada pada suatu ruangan. Jika ada banyak orang yang berbicara pada saat bersamaan, maka pendengaran kita terhadap seorang pembicara akan terganggu oleh pembicara lainnya. Akibatnya, kita bisa salah menangkap isi pembicaraan, atau bahkan sama sekali tidak bisa mendengarnya. Artinya tingkat kongesti dalam jaringan yang besar akan sangat tinggi, karena probabilitas “tabrakan” pembicaraan bertambah tinggi jika jumlah yang berbicara bertambah banyak.

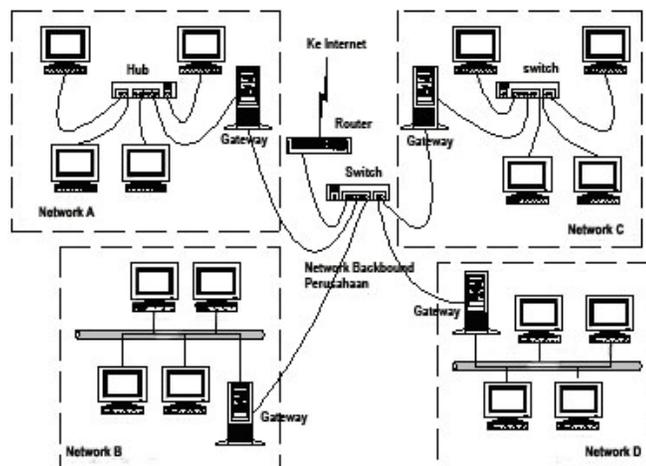


Gambar 5.1. Satu Physical Network dengan host yang banyak

Untuk menghindari terjadinya kongesti akibat terlalu banyak host dalam suatu physical network, dilakukan segmentasi jaringan.

Misalkan suatu perusahaan yang terdiri dari 4 departemen ingin memiliki LAN yang dapat mengintegrasikan seluruh departemen. Masing-masing departemen memiliki server sendiri-sendiri (bisa Novell Server, Windows Server, Linux atau UNIX). Cara yang sederhana adalah membuat topologi network perusahaan tersebut seperti ditampilkan pada gambar berikut.





Gambar 5.2. Subnetting secara fisik

Kita membuat 5 buah physical network (sekaligus logical network), yakni 4 buah pada masing-masing departemen, dan satu buah lagi sebagai jaringan backbone antar departemen. Dengan kata lain, kita membuat beberapa subnetwork (melakukan subnetting). Keseluruhan komputer tetap dapat saling berhubungan karena server juga berfungsi sebagai router. Pada server terdapat dua network interface, masing-masing tersambung ke jaringan backbone dan jaringan departemennya sendiri.

Setelah membuat subnet secara fisik, kita juga harus membuat *subnet logic*. Masing-masing subnet fisik setiap departemen harus mendapat *subnet logic* (IP Address) yang berbeda, yang merupakan bagian dari network address perusahaan. Dengan mengetahui dan menetapkan subnetmask, kita dapat memperkirakan jumlah host maksimal masing-masing subnet pada jaringan tersebut.

Berikut ini daftar subnetting yang bisa dihapal dan diterapkan untuk membuat subnet.

Tabel 5.1. Subnetting

Bit Host Masked	CIDR	Subnet	Net Mask	Host per Network
0	/8	1 network	255.0.0.0	16777214
1	/9	2	255.128.0.0	8388606
2	/10	4	255.192.0.0	4194302
3	/11	8	255.224.0.0	2097150
4	/12	16	255.240.0.0	1048574
5	/13	32	255.248.0.0	524286
6	/14	64	255.252.0.0	262142
7	/15	128	255.254.0.0	131070
8	/16	256	255.255.0.0	65534
9	/17	512	255.255.128.0	32766
10	/18	1024	255.255.192.0	16382
11	/19	2048	255.255.224.0	8910
12	/20	4096	255.255.240.0	4094
13	/21	8912	255.255.248.0	2046
14	/22	16384	255.255.252.0	1022



15	/23	32768	255.255.254.0	510
16	/24	65536	255.255.255.0	254
17	/25	131072	255.255.255.128	126
18	/26	262144	255.255.255.192	62
19	/27	524288	255.255.255.224	30
20	/28	1048576	225.255.255.240	14
21	/29	2097152	255.255.255.248	6
22	/30	4194304	255.255.255.252	2 host
23	/31	invalid	255.255.255.254	invalid

Disamping menghafal tabel-tabel diatas, dapat juga mempelajari cara menghitung dengan menggunakan rumus

Jumlah Host per Network = $2^n - 2$

Dimana n adalah jumlah bit tersisa yang belum diselubungi, misal Network Prefix /10, maka bit tersisa (n) adalah $32 - 10 = 22$

$2^{22} - 2 = 4194302$

Sedangkan untuk mencari : Jumlah Subnet = 2^N

Dimana N adalah jumlah bit yang dipergunakan (diselubungi) atau $N = \text{Network Prefix} - 8$

Seperti contoh, bila network prefix /10, maka $N = 10 - 8 = 2 \rightarrow 2^2 = 4$

Untuk menyusun tabel diatas, sebenarnya tidak terlalu sulit, anda bisa lebih detail memperhatikan bahwa, nilai jumlah host per network ternyata tersusun terbalik dengan jumlah subnet, Host/network dapat dengan gampang anda susun dengan rumus lain, seperti: $X \times 2 + 2 = X_n$

X = jumlah host sebelumnya, dan
 X_n = jumlah host

Perhatikan: $2 \times 2 + 2 = 6$, $6 \times 2 + 2 = 14$, $14 \times 2 + 2 = 30$ dst.

Subnet: $1 \times 2 = 2$, $2 \times 2 = 4$, $4 \times 2 = 8$, $8 \times 2 = 16$, dst.

~~“Cinana, sudah mulai faham? kelas belum mungkin contoh kasus berikut bisa lebih membantu pemahaman anda ☺.~~

Contoh Kasus:

Bila anda memiliki IP address dari klas C seperti 192.168.0.1, Tentukan berapa jumlah host maksimal yang anda bisa susun dalam satu network dan berapa jumlah network (subnet) yang bisa anda bentuk (1 network atau lebih)

Penyelesaian:

```

Net Address : 192.168.0.0/24 11000000.10101000.00000000.00000000
Netmask     : 255.255.255.0 11111111.11111111.11111111.00000000
Wildcard    : 0.0.0.255      00000000.00000000.00000000.11111111

IP Host Awal: 192.168.0.1   11000000.10101000.00000000.00000001
IP Host Akhir: 192.168.0.254 11000000.10101000.00000000.11111110

```





```

Broadcast      : 192.168.0.255  11000000.10101000.00000000.11111111
Hosts/Net      : 254 (1 Network)

```

```

Network        : 192.168.0.0/25  11000000.10101000.00000000.00000000
Netmask        : 255.255.255.128  11111111.11111111.11111111.10000000
Wildcard       : 0 .0 .0 .127    00000000.00000000.00000000.01111111

IP Host Awal  : 192.168.0.1     11000000.10101000.00000000.00000001
IP Host Akhir  : 192.168.0.126  11000000.10101000.00000000.01111110
Broadcast      : 192.168.0.127  11000000.10101000.00000000.01111111
Hosts/Net      : 126 (1 Network)

Network        : 192.168.0.128  11000000.10101000.00000000.10000000
IP Host Awal  : 192.168.0.129  11000000.10101000.00000000.10000001
IP Host Akhir  : 192.168.0.254  11000000.10101000.00000000.11111110
Broadcast      : 192.168.0.255  11000000.10101000.00000000.11111111
Hosts/Net      : 126 (1 Network)

Subnets       : 2 Network
Hosts Max      : 252

```

```

Net Add        : 192.168.0.0/26  11000000.10101000.00000000.00000001
Netmask        : 255.255.255.192  11111111.11111111.11111111.11000000
Wildcard       : 0.0.0.63        00000000.00000000.00000000.00111111

Network        : 192.168.0.0/26  11000000.10101000.00000000.00000000
HostMin        : 192.168.0.1     11000000.10101000.00000000.00000001
HostMax        : 192.168.0.62    11000000.10101000.00000000.00111110
Broadcast      : 192.168.0.63    11000000.10101000.00000000.00111111
Hosts/Net      : 62

Network        : 192.168.0.64/26  11000000.10101000.00000000.01 000000
HostMin        : 192.168.0.65    11000000.10101000.00000000.01 000001
HostMax        : 192.168.0.126   11000000.10101000.00000000.01 111110
Broadcast      : 192.168.0.127   11000000.10101000.00000000.01 111111
Hosts/Net      : 62

Network        : 192.168.0.128/26 11000000.10101000.00000000.10 000000
HostMin        : 192.168.0.129   11000000.10101000.00000000.10 000001
HostMax        : 192.168.0.190   11000000.10101000.00000000.10 111110
Broadcast      : 192.168.0.191   11000000.10101000.00000000.10 111111
Hosts/Net      : 62

Network        : 192.168.0.192/26 11000000.10101000.00000000.11 000000
HostMin        : 192.168.0.193   11000000.10101000.00000000.11 000001
HostMax        : 192.168.0.254   11000000.10101000.00000000.11 111110
Broadcast      : 192.168.0.255   11000000.10101000.00000000.11 111111
Hosts/Net      : 62

Subnets       : 4
Hosts          : 248

```





Masih banyak lagi network yang kita bisa bentuk dengan 192.168.0.0/27,
 192.168.0.0/28,
 192.168.0.0/29, dan
 192.168.0.0/30.

Singkatnya anda bisa lihat ditabel berikut:

Tabel 5.2. Subnetmask dari IP Address klas C

Bit Maske d	Bit Host ID	CID R	Subne t	Net Mask	Host Max	Host per Networ k
0	8	/24	1	255.255.255.0	254	254
1	7	/25	2	255.255.255.128	252	126
2	6	/26	4	255.255.255.192	248	62
3	5	/27	8	255.255.255.224	240	30
4	4	/28	16	255.255.255.240	224	14
5	3	/29	32	255.255.255.248	192	6
6	2	/30	64	255.255.255.252	128	2

Contoh lain, bila sebuah kampus memiliki IP Address 167.205.7.xxx diperkirakan jumlah komputer maksimum yang tersambung di dalam setiap LAN tidak akan melebihi 30 buah. Oleh karena itu, pemilihan subnetmask yang tepat untuk ini adalah 27 bit (255.255.255.224), ini berarti jumlah bit host adalah 5, maka, subnet 167.205.7.xxx tadi dipecah menjadi 8 buah subnet baru yang lebih kecil. Setiap subnet baru terdiri dari 32 IP Address (1 IP untuk Net Address, 30 IP untuk host dan 1 IP untuk broadcast).

Ingat bahwa address paling awal dalam setiap subnet (seluruh bit host bernilai 0) diambil sebagai network address dan address paling akhir (seluruh bit host bernilai 1) sebagai broadcast.

Tabel 5.3. Pembagian Net 167.205.7.xxx menjadi 8 buah Subnet

Subnet	Struktur IP Address	Network Address	Broadcast Address
Subnet 1	167.205.7 .000 hhhhh	167.205.7.0	167.205.7.31
Subnet 2	167.205.7 .001 hhhhh	167.205.7.32	167.205.7.63
Subnet 3	167.205.7 .010 hhhhh	167.205.7.64	167.205.7.95
Subnet 4	167.205.7 .011 hhhhh	167.205.7.96	167.205.7.127
Subnet 5	167.205.7 .100 hhhhh	167.205.7.128	167.205.7.159





Subnet 6	167.205.7. hhhhh	101	167.205.7.160	167.205.7.191
Subnet 7	167.205.7. hhhhh	110	167.205.7.192	167.205.7.223
Subnet 8	167.205.7. hhhhh	111	167.205.7.224	167.205.7.255

Setelah mendapatkan angka-angka di atas, pendelegasian IP address dapat dilakukan. Contoh pembagiannya adalah sbb :

subnet 1 (167.205.7.0) untuk LAN pada Akademik

subnet 2 (167.205.7.32) untuk LAN pada Laboratorium 1

subnet 3 (167.205.7.64) untuk LAN pada Laboratorium 2, dst.

Perhatikan bahwa jika kita hanya memiliki 10 buah komputer pada LAN yang berkapasitas 30 host (penerapan masking 27 bit), maka 20 IP address lainnya yang belum/tidak terpakai tidak dapat dipakai pada LAN lain, karena akan mengacaukan jalannya routing.

Dalam melakukan subnetting, kita harus terlebih dahulu menentukan seberapa besar jaringan kita saat ini, serta kemungkinannya dimasa mendatang. Untuk hal tersebut kita dapat mengikuti beberapa petunjuk umum berikut:

- ❖ Tentukan dulu jumlah jaringan fisik yang ada
- ❖ Tentukan jumlah IP address yang dibutuhkan oleh masing-masing jaringan.

Berdasarkan requirement ini, definisikan:

- ❖ Satu subnet mask untuk seluruh network
- ❖ Subnet ID yang unik untuk setiap segmen jaringan
- ❖ Range host ID untuk setiap subjek

Cara paling sederhana dalam membentuk subnet ialah mengalokasikan IP Address sama rata untuk setiap subnet. Namun hal ini hanya cocok jika alokasi IP yang kita miliki besar sekali atau kita menggunakan IP private, dan jaringan menjalankan protokol routing RIP versi 1.

Jika kita ingin membuat jaringan dengan subnet berukuran berbeda, RIP versi 1 tidak dapat digunakan. **Alokasi IP dengan subnet yang besarnya berbeda-beda sesuai kebutuhan ini disebut sebagai VLSM (Variable Length Subnet Mask).** VLSM dapat menghasilkan alokasi IP yang lebih efisien.

5.2 Konsep Routing

5.2.1 Mengapa perlu router ?

Sebelum kita pelajari lebih jauh mengenai bagaimana konsep routing, kita perlu memahami lebih baik lagi mengenai beberapa aturan dasar routing. Juga tentunya kita harus memahami sistem penomoran IP, subnetting, netmasking dan saudara-saudaranya yang lain.

Contoh kasus:





Host X → 128.1.1.1 (IP Kelas B network id 128.1.x.x)

Host Y → 128.1.1.7 (IP kelas B network id 128.1.x.x)

Host Z → 128.2.2.1 (IP kelas B network id 128.2.x.x)

Pada kasus di atas, host X dan host Y dapat berkomunikasi langsung tetapi baik host X maupun Y tidak dapat berkomunikasi dengan host Z, karena mereka memiliki Network Id yang berbeda. Bagaimana supaya Z dapat berkomunikasi dengan X dan Y ? **gunakan router !**

Contoh lain:

Host A → 192.168.0.1 subnet mask 255.255.255.240

Host B → 192.168.0.2 subnet mask 255.255.255.240

Host C → 192.168.0.17 subnet mask 255.255.255.240

Nah, ketika subnetting dipergunakan, maka dua host yang terhubung ke segmen jaringan yang sama dapat berkomunikasi hanya jika baik Network ID maupun subnetID-nya sesuai. Pada kasus di atas, A dan B dapat berkomunikasi dengan langsung, C memiliki Network ID yang sama dengan A dan B tetapi memiliki subnetmask yang berbeda. Dengan demikian C tidak dapat berkomunikasi secara langsung dengan A dan B. Bagaimana supaya C dapat berkomunikasi dengan A dan B ? **gunakan router !**

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

Dalam implementasinya, router sering dipakai untuk menghubungkan jaringan antar lembaga atau perusahaan yang masing-masing telah memiliki jaringan dengan Network ID yang berbeda.

Contoh lainnya yang saat ini populer adalah ketika sebuah perusahaan akan terhubung ke internet. Maka router akan berfungsi mengalirkan paket data dari perusahaan tersebut ke lembaga lain melalui internet, sudah barang tentu nomor jaringan perusahaan itu akan berbeda dengan perusahaan yang dituju.

Jika sekedar menghubungkan 2 buah jaringan, sebenarnya anda juga dapat menggunakan PC berbasis windows NT atau Linux, dengan memberikan 2 buah network card dan sedikit setting, maka anda telah membuat router praktis. Namun tentunya dengan segala keterbatasannya. Di pasaran sangat beragam merek router, antara lain baynetworks, 3com, Cisco, dll.

5.2.2 Routing Statik dan Dinamik

Secara umum mekanisme koordinasi routing dapat dibagi menjadi dua, yaitu: *routing statik* dan *routing dinamik*.

Pada *routing statik*, entri-entri dalam forwarding table router diisi dan dihapus secara manual, sedangkan pada *routing dinamik* perubahan dilakukan otomatis melalui protokol routing.

Routing statik adalah pengaturan routing paling sederhana yang dapat dilakukan pada jaringan komputer. Menggunakan routing statik murni dalam sebuah jaringan berarti mengisi setiap entri dalam forwarding table di setiap router yang berada di jaringan tersebut.





Penggunaan routing statik dalam sebuah jaringan yang kecil tentu bukanlah suatu masalah, hanya beberapa entri yang perlu diisikan pada forwarding table di setiap router. Namun Anda tentu dapat membayangkan bagaimana jika harus melengkapi forwarding table di setiap router yang jumlahnya tidak sedikit dalam jaringan yang besar. Apalagi jika Anda ditugaskan untuk mengisi entri-entri di seluruh router di Internet yang jumlahnya banyak sekali dan terus bertambah setiap hari. Tentu repot sekali!

Routing dinamik adalah cara yang digunakan untuk melepaskan kewajiban mengisi entri-entri forwarding table secara manual. Protokol routing mengatur router-router sehingga dapat berkomunikasi satu dengan yang lain dan saling memberikan informasi routing yang dapat mengubah isi forwarding table, tergantung keadaan jaringannya. Dengan cara ini, router-router mengetahui keadaan jaringan yang terakhir dan mampu meneruskan datagram ke arah yang benar. Dengan kata lain, routing dinamik adalah proses pengisian data routing di table routing secara otomatis.

Berikut ini tabel perbedaan yang spesifik untuk kedua jenis routing.

Tabel 5.4. Perbedaan routing statik dan routing dinamik

Routing Statik	Routing Dinamik
Berfungsi pada protokol IP	Berfungsi pada inter-routing protocol
Router tidak dapat membagi informasi routing	Router membagi informasi routing secara otomatis
Routing tabel dibuat dan dihapus secara manual	Routing tabel dibuat dan dihapus secara dinamis oleh router
Tidak menggunakan routing protocol	Terdapat routing protocol, seperti RIP atau OSPF
Microsoft mendukung multihomed system seperti router	Microsoft mendukung RIP untuk IP dan IPX/SPX

5.3 Rangkuman

Konsep subnetting dari IP Address versi 4 merupakan teknik yang umum digunakan di Internet untuk mengefisienkan alokasi IP Address dalam sebuah jaringan supaya bisa memaksimalkan penggunaan IP Address.

Subnetting merupakan proses memecah satu kelas IP Address menjadi beberapa subnet dengan jumlah host yang lebih sedikit, dan untuk menentukan batas network ID dalam suatu subnet, digunakan subnet mask.

Fungsi router secara sederhana adalah menghubungkan dua buah jaringan yang berbeda; tepatnya mengarahkan rute yang terbaik untuk mencapai network yang diharapkan.

CIDR merupakan konsep baru untuk mengembangkan Supernetting dengan metode Classless Inter-Domain Routing. CIDR menghindari cara pemberian IP Address tradisional menggunakan klas A, B dan C. CIDR menggunakan “network prefix” dengan panjang tertentu. *Prefix-length* menentukan jumlah “bit sebelah kiri” yang akan dipergunakan sebagai network ID.

Jika suatu IP Address memiliki 16 bit sebagai network ID, maka IP address tersebut akan diberikan *prefix-length (network prefix)* 16 bit yang umumnya ditulis sebagai /16 dibelakang IP Address, contoh: 202.152.0.1/18.

Jika diperhatikan, CIDR dan metode VLSM mirip satu sama lain, yaitu blok network address dapat dibagi lebih lanjut menjadi sejumlah blok IP address yang lebih kecil. Perbedaannya adalah CIDR merupakan sebuah konsep untuk pembagian blok IP Public yang telah didistribusikan dari IANA,





sedangkan VLSM merupakan implementasi pengalokasian blok IP yang dilakukan oleh pemilik network (network administrator) dari blok IP yang telah diberikan padanya (sifatnya local dan tidak dikenal di internet).

Jika pada pengalokasian IP address classfull, suatu network ID hanya memiliki satu subnetmask, maka VLSM menggunakan metode yang berbeda, yakni dengan memberikan suatu network address lebih dari satu subnetmask.

Sebelum melakukan subnetting, hal yang kita harus kita tentukan terlebih dahulu adalah seberapa besar jaringan kita saat ini, serta kemungkinannya dimasa mendatang.

Routing statik menggunakan routing statik murni dalam sebuah jaringan, hal ini berarti mengisi setiap entri dalam forwarding table di setiap router yang berada di jaringan tersebut.

Routing dinamik merupakan cara yang digunakan untuk melepaskan kewajiban mengisi entri-entri forwarding table secara manual. Protokol routing mengatur router-router sehingga dapat berkomunikasi satu dengan yang lain dan saling memberikan informasi routing yang dapat mengubah isi forwarding table, tergantung keadaan jaringannya. Dengan cara ini, router-router mengetahui keadaan jaringan yang terakhir dan mampu meneruskan datagram ke arah yang benar. Dengan kata lain, routing dinamik adalah proses pengisian data routing di table routing secara otomatis.

5.4 Soal latihan :

1. Bila anda memiliki 1 blok alamat IP dari klas C seperti 192.168.0/25. Anda diminta untuk membagi blok IP tersebut menjadi 2 subnet (untuk 2 bh network yang tidak saling berhubungan antara host dinetwork yang satu dengan host di network yang lain). Tentukanlah Subnetmask, Wildcard dan IP address untuk masing-masing network (termasuk Net Address, IP Broadcast, IP yang digunakan untuk host (awal dan akhir) serta jumlah host maksimal dimasing-masing network yang anda bisa susun.
2. Bila seorang administrator jaringan sebuah kantor akan mengalokasikan IP Address 172.16.12.xxx kedalam 8 bh subnet (untuk 8 bh departemen/bagian yang terdapat dalam kantor tersebut), maka coba anda perkirakan jumlah komputer maksimum yang tersambung dalam setiap LAN pada masing-masing departemen tersebut. Pilih subnetmask yang tepat untuk ini serta tetapkan IP Net Address untuk tiap LAN dan Broadcast untuk tiap subnet tersebut.
3. Sebuah host dengan IP 202.152.204.65 dengan subnet mask 255.255.255.224, berapa alamat subnet dan IP Broadcast?
4. Jika diberikan Net Address 192.168.10.0 dan Subnet Mask 255.255.255.192, maka berapa banyak subnet (LAN) yang bisa dihasilkan dan berapa jumlah host maksimal tiap LAN?
5. Isilah daftar di table berikut hingga bernilai benar

Bit Maske d	Bit Host ID	CID R	Jml Subne t	Net Mask	Host Max	Host per Networ k
		/24				
		/25				
		/26				





		/27				
		/28				
		/29				
		/30				

6. Jelaskan dengan singkat tentang:
 - a. Subnetting
 - b. Konsep subnetting dari IP Address
 - c. Esensi dari Subnetting, serta
 - d. Tujuan dari subnetting
7. Identifikasi alamat IP 169.254.0.0 berikut adalah:
 - a. *Host IP Address*
 - b. *Network Address*
 - c. *Broadcast Address*
 - d. *Network Prefix*
8. Identifikasi alamat IP 172.31.255.255 berikut ini merupakan:
 - a. *Alamat Loopback*
 - b. *Network Address*
 - c. *Broadcast Address*
 - d. *Network Prefix*
9. Penggunaan alamat *loopback* digunakan untuk mengirim sebuah paket dari _____ ke _____:
 - a. *Host; host lainnya*
 - b. *Host; gateway*
 - c. *Host; router*
 - d. *Host; host itu sendiri*
10. Berikut ini yang merupakan alamat loopback adalah:
 - a. *127.0.0.1*
 - b. *127.0.0.0*
 - c. *192.168.0.0*
 - d. *192.168.0.1*
11. Nilai **192.0.2/24** berikut merupakan (pilih 2 jawaban)
 - a. *Network Prefix dengan netmask 255.255.255.0*
 - b. *Network Prefix dengan netmask 255.255.255.128*
 - c. *Blok IP Address dengan host maksimal 254*
 - d. *Blok IP Address dengan host maksimal 63*
12. Protocol routing seperti RIP, OSPF, IGRP dapat digolongkan sebagai:
 - a. *Interior Gateway Protocol*
 - b. *Exterior Gateway Protocol*
 - c. *Routing balanced hybrid type*
 - d. *Routing Tidak langsung*





13. Suatu kondisi ketika dua router atau beberapa router bertetangga/terdekat saling mengira bahwa untuk mencapai suatu alamat, maka datagram harus dilewatkan melalui router terdekat, sehingga datagram berputar dari satu router ke router tetangga dan kembali ke router itu lagi, disebut
- a. *Routing Langsung*
 - b. *Routing Loop*
 - c. *Routing Statik*
 - d. *Routing Dinamik*
14. Apa yang terjadi jika pada protokol routing RIP hop ke-16 telah tercapai? (pilih dua jawaban)
- a. *Paket yang dikirim diterima oleh komputer tujuan*
 - b. *Paket yang dikirim tidak mencapai tujuan*
 - c. *Paket yang dikirim akan dibuang*
 - d. *Paket yang dikirim akan diseleksi di komputer tujuan*
15. Pilih 2 jenis routing yang menggunakan metode distance vector (pilih 2 jawaban)
- a. *RIP*
 - b. *EIGRP*
 - c. *OSPF*
 - d. *IGRP*
16. Protokol routing yang menggunakan Autonomous System adalah (pilih beberapa jawaban yang anda anggap benar):
- a. *IGRP*
 - b. *EIGRP*
 - c. *OSPF*
 - d. *NLSP*
17. Metode apakah yang dapat dipergunakan untuk mencegah agar informasi yang dikirim oleh router dikirim kembali ketempat dimana informasi berasal
- a. *Routing loop*
 - b. *Efek bouncing*
 - c. *Counting to Infinity*
 - d. *Split Horizon*
18. Metode dan routing metric yang dipergunakan oleh RIP adalah (pilih 2 jawaban):
- a. *Link State*
 - b. *Distance vector*
 - c. *Balanced hybrid*
 - d. *Hop Count*
19. Tiga cara router untuk mempelajari jalur tujuannya adalah dengan:
- a. *Satic Routing*
 - b. *Default Routing*
 - c. *Dynamic Routing*
 - d. *Standart Routing*
20. Metode yang dapat dipergunakan untuk mengirimkan routing update, agar dapat memberitahu bahwa suatu paket tidak mencapai tujuannya adalah dengan:
- a. *Route Poisoning*
 - b. *Slow converge*
 - c. *Priodic Update*
 - d. *Load balancing*

DAFTAR PUSTAKA





<http://www.apjii.or.id/>

<http://distancelearning.ksi.edu/demo/520/cis520.htm>

http://www.pemula.com/materi/cisco01_konsep_pemula.htm, yerianto@yahoo.com

Implementing IP Routing By Todd Lammler, with Monica Lammler and James Chellis.
<http://www.microsoft.com/technet/archive/winntas/deploy/implip.mspx>

Konsep Subnetting IP Address Untuk Efisiensi Internet, Aulia K. Arif & Onno W. Purbo, Computer Network Research Group ITB, 2000 - <http://bebas.vlsm.org/v09/onno-ind-1/network/konsep-subnetting-ip-address-untuk-efisiensi-internet-11-199.zip>,

Pengantar Jaringan Komputer, Melwin Syafrizal, Andi Offset, Jogja, 2005

Routing Protocols and the Configuration of RIP and IGRP (Cisco CCNA Exam #640-607 Certification Guide", by Wendell Odom, Cisco Press)

TCP/IP dan Implementasinya, Onno W Purbo, Adnan Basalamah, Ismail Fahmi, Achmad Husni T, Elexmedia Komputindo 1999.



NAT

(Network Address Translation)

Cara lain menghemat IP Address

Kopetensi Dasar: Memahami konsep NAT dan mampu melakukan konfigurasi Network Address Translation (NAT)

Misi awal Internet adalah sebagai jaringan komunikasi non-profit. Pada awalnya, Internet didesain tanpa memperhatikan dunia bisnis. Kemudian hal ini menjadi masalah sekarang dan di masa depan. Dengan semakin banyaknya penghuni Internet, baik pencari informasi maupun penyedia informasi, maka kebutuhan akan pengalamatan di Internet makin membengkak. Kebutuhan besar akan IP *address* biasanya terjadi di jaringan komputer perusahaan dan LAN-LAN di lembaga pendidikan.

IP *address* sebagai sarana pengalamatan di Internet semakin menjadi barang mewah dan eksklusif. Tidak sembarang orang sekarang ini bisa mendapatkan IP *address* yang valid dengan mudah. Oleh karena itulah dibutuhkan suatu mekanisme yang dapat menghemat IP *address*. Logika sederhana untuk penghematan IP *address* ialah dengan meng-*share* suatu nomor IP *address* valid ke beberapa *client* IP lainnya. Atau dengan kata lain beberapa komputer bisa mengakses Internet walau kita hanya memiliki satu IP *address* yang valid. Salah satu Mekanisme itu disediakan oleh *Network Address Translation* (NAT)

Sebelum kita membahas lebih lanjut ada baiknya kita urai kembali konsep-konsep dasar yang harus dipahami sebelum masuk ke NAT. Diantaranya adalah TCP/IP, *Gateway*, *Router*, *Proxy*, dan *Firewall*.





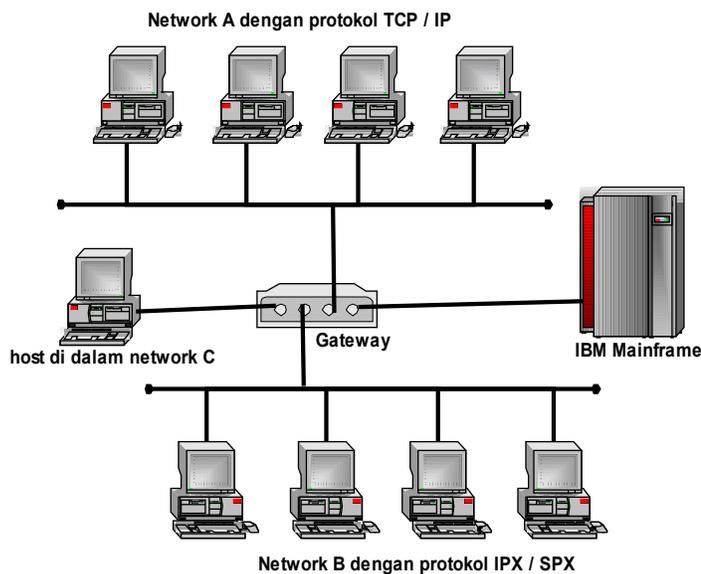
TCP/IP – karena merupakan Protokol yang menjadi standar dan dipakai hampir oleh seluruh komunitas Internet adalah TCP/IP (*Transmission Control Protocol/Internet Protocol*). Agar komputer bisa berkomunikasi dengan komputer lainnya, maka menurut aturan TCP/IP, komputer tersebut harus memiliki suatu *address* yang unik. Alamat tersebut dinamakan *IP address*.

6.1 Gateway /Router

Untuk menghubungkan dua network yang berbeda dibutuhkan *gateway*. *Gateway* bisa berupa komputer yang memiliki minimal 2 buah *network interface* untuk menghubungkan 2 buah jaringan atau lebih atau berupa perangkat router atau juga berupa software. 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*). *Gateway* yang berupa komputer menjalankan *Network Operating System* plus *routing daemon*. Misalkan PC yang dipasang **Unix FreeBSD** atau **Linux** 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 dipasang mekanisme pembatasan atau pengamanan (*filtering*) paket-paket data. Mekanisme ini disebut *Firewall*.

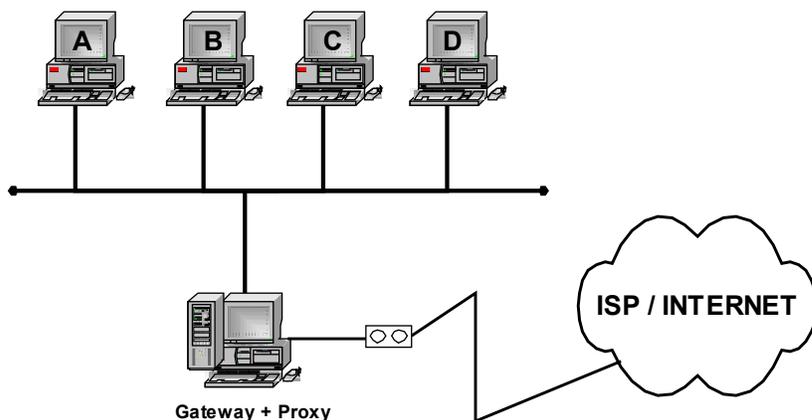


Gambar 6.1. Contoh jaringan menggunakan gateway

6.2 Proxy Server

Konsep proxy sebagai berikut :





Gambar 6.2. Proxy Server

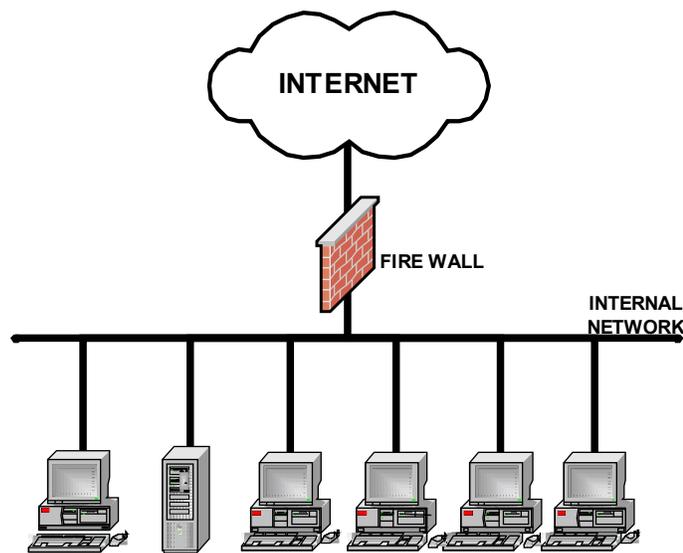
Jika komputer A me-*request* suatu halaman web dan komputer A sebagai proxy client maka *request* tersebut akan diterima oleh proxy server, selanjutnya proxy server yang akan mencoba mengambil halaman web tersebut dari web server, setelah itu akan diberikan kepada komputer A. Komputer proxy server juga akan menyimpan halaman web tersebut di dalam cache memori-nya dalam jangka waktu tertentu tergantung *setting*-nya, untuk sewaktu-waktu bila ada *request* halaman web yang sama, tidak perlu lagi mengambil dari web server, sehingga akan menjadi lebih cepat.

6.3 Firewall

Sebenarnya *Firewall* adalah suatu program yang dijalankan di *gateway/router* yang bertugas memeriksa setiap paket data yang lewat kemudian membandingkannya dengan *rule* yang diterapkan dan akhirnya memutuskan apakah paket data tersebut boleh diteruskan atau ditolak. Tujuan dasarnya adalah sebagai *security* yang melindungi jaringan internal dari ancaman dari luar. Namun dalam tulisan ini *Firewall* digunakan sebagai basis untuk menjalankan *Network Address Translation* (NAT).

Dalam FreeBSD, program yang dijalankan sebagai *Firewall* adalah ipfw. Sebelum dapat menjalankan ipfw, *kernel* GENERIC harus dimodifikasi supaya mendukung fungsi *firewall*. Ipfw mengatur lalu lintas paket data berdasarkan IP asal, IP tujuan, nomor *port*, dan jenis *protocol*. Untuk menjalankan NAT, option IPDIVERT harus diaktifkan dalam *kernel*. Di linux ada banyak firewall yang dapat digunakan, Kernel sebelum 2.4 menggunakan ipchains untuk mem-filter paket. Kernel 2.4 keatas menggunakan iptables (disebut juga netfilter), yang sama dengan ipchains tetapi mempunyai ruang lingkup dan kontrol yang lebih luas sebagai firewall. Ada juga TCP Wrappers, SQUID, dll.





Gambar 6.3. Firewall

6.4 DIVERT (mekanisme diversifikasi paket kernel)

Socket divert sebenarnya sama saja dengan *socket* IP biasa, kecuali bahwa *socket divert* bisa di *bind* ke *port divert* khusus lewat *bind system call*. IP *address* dalam *bind* tidak diperhatikan, hanya nomor *port*-nya yang diperhatikan. Sebuah *socket divert* yang di *bind* ke *port divert* akan menerima semua paket yang di *diversifikasi* pada *port* tersebut oleh mekanisme di *kernel* yang dijalankan oleh implementasi *filtering* dan program *ipfw*. Mekanisme ini yang dimanfaatkan nantinya oleh *Network Address Translator*.

6.5 Network Address Translation (NAT)

Dalam FreeBSD, mekanisme *Network Address Translation* (NAT) dijalankan oleh program *Natd* yang bekerja sebagai *daemon*. *Network Address Translation Daemon* (*Natd*) menyediakan solusi untuk permasalahan penghematan ini dengan cara menyembunyikan IP *address* jaringan internal, dengan membuat paket yang di-*generate* di dalam terlihat seolah-olah dihasilkan dari mesin yang memiliki IP *address* legal. *Natd* memberikan konektivitas ke dunia luar tanpa harus menggunakan IP *address* legal dalam jaringan internal.

Dengan NAT, aturan bahwa untuk berkomunikasi harus menggunakan IP *address* legal, dilanggar. NAT bekerja dengan jalan mengkonversikan IP *address* ke satu atau lebih IP *address* lain. IP *address* yang di konversi adalah IP *address* yang diberikan untuk tiap mesin dalam jaringan internal (bisa sembarang IP). IP *address* yang menjadi hasil konversi terletak di luar jaringan internal tersebut dan merupakan IP *address* legal yang *valid/routable*.

6.5.1 Mekanisme NAT

Sebuah paket TCP terdiri dari *header* dan data. *Header* memiliki sejumlah *field* di dalamnya, salah satu *field* yang penting di sini adalah MAC (*Media Access Control*) *address* asal dan tujuan, IP *address* asal dan tujuan, dan nomor *port* asal dan tujuan. Saat mesin A menghubungi mesin B, *header* paket berisi IP A sebagai IP *address* asal dan IP B sebagai IP *address* tujuan. *Header* ini juga berisi





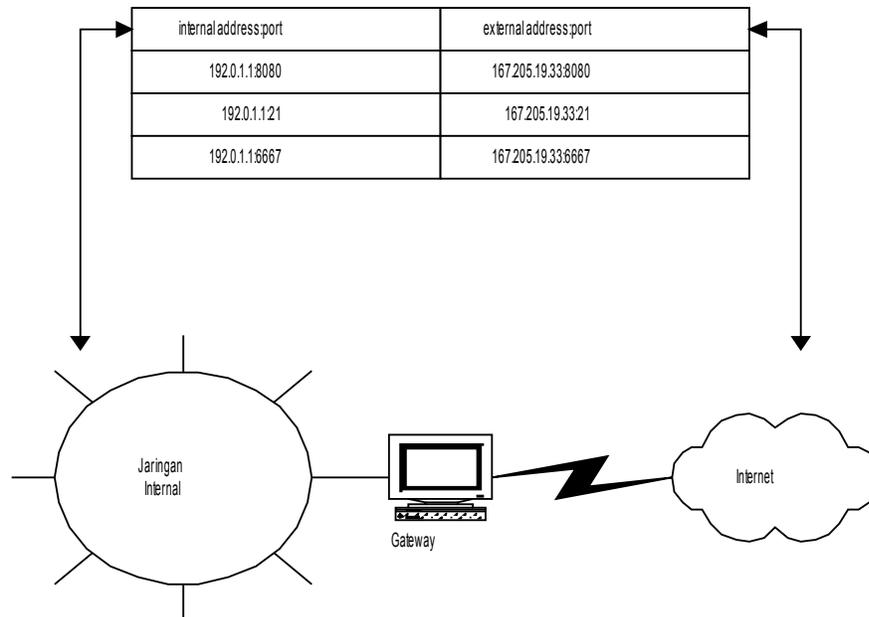
nomor *port* asal (biasanya dipilih oleh mesin pengirim dari sekumpulan nomor *port*) dan nomor *port* tujuan yang spesifik, misalnya *port* 80 (untuk *web*).

Kemudian B menerima paket pada *port* 80 dan memilih nomor *port* balasan untuk digunakan sebagai nomor *port* asal menggantikan *port* 80 tadi. Mesin B lalu membalik IP *address* asal & tujuan dan nomor *port* asal & tujuan dalam *header* paket. Sehingga keadaan sekarang IP B adalah IP *address* asal dan IP A adalah IP *address* tujuan. Kemudian B mengirim paket itu kembali ke A. Selama *session* terbuka, paket data hilir mudik menggunakan nomor *port* yang dipilih.

Router (yang biasa – tanpa Natd) memodifikasi *field* MAC *address* asal & tujuan dalam *header* ketika me-*route* paket yang melewatinya. IP *address*, nomor *port*, dan nomor *sequence* asal & tujuan tidak disentuh sama sekali. NAT juga bekerja atas dasar ini. Dimulai dengan membuat tabel translasi internal untuk semua IP *address* jaringan internal yang mengirim paket melewatinya. Lalu men-*set* tabel nomor *port* yang akan digunakan oleh IP *address* yang valid. Ketika paket dari jaringan internal dikirim ke Natd untuk disampaikan keluar, Natd melakukan hal-hal sebagai berikut:

1. Mencatat IP *address* dan *port* asal dalam tabel translasi
2. Menggantikan nomor IP asal paket dengan nomor IP dirinya yang valid
3. Menetapkan nomor *port* khusus untuk paket yang dikirim keluar, memasukkannya dalam tabel translasi dan menggantikan nomor *port* asal tersebut dengan nomor *port* khusus ini.

Ketika paket balasan datang kembali, Natd mengecek nomor *port* tujuannya. Jika ini cocok dengan nomor *port* yang khusus telah ditetapkan sebelumnya, maka dia akan melihat tabel translasi dan mencari mesin mana di jaringan internal yang sesuai. Setelah ditemukan, ia akan menulis kembali nomor *port* dan IP *address* tujuan dengan IP *address* dan nomor *port* asal yang asli yang digunakan dulu untuk memulai koneksi. Lalu mengirim paket ini ke mesin di jaringan internal yang dituju. Natd memelihara isi tabel translasi selama koneksi masih terbuka.



Gambar 6.4. Contoh Mekanisme Natd

6.5.2 Perbedaan dengan sistem *Proxy*

Hampir mirip dengan NAT, suatu jaringan kecil dengan *proxy* bisa menempatkan beberapa mesin untuk mengakses *web* dibelakang sebuah mesin yang memiliki IP *address* valid. Ini juga merupakan





langkah penghematan biaya dibanding harus menyewa beberapa account dari ISP dan memasang modem & sambungan telepon pada tiap mesin.

Namun demikian, *proxy* server ini tidak sesuai untuk jaringan yang lebih besar. Bagaimanapun, menambah *hard disk* dan RAM pada server *proxy* supaya *proxy* berjalan efisien tidak selalu dapat dilakukan (karena *constraint* biaya). Lagi pula, persentase *web page* yang bisa dilayani oleh *cache proxy* akan makin menurun sejalan dengan semakin menipisnya ruang kosong di *hard disk*, sehingga penggunaan *cache proxy* menjadi tidak lebih baik dari pada sambungan langsung. Tambahan lagi, tiap koneksi bersamaan akan meng-*generate* proses tambahan dalam *proxy*. Tiap proses ini harus menggunakan *disk I/O channel* yang sama, dan saat *disk I/O channel* jenuh, maka terjadilah *bottle neck*.

NAT menawarkan solusi yang lebih fleksibel dan *scalable*. NAT menghilangkan keharusan mengkonfigurasi *proxy/sock* dalam tiap *client*. NAT lebih cepat dan mampu menangani trafik *network* untuk beribu-ribu *user* secara simultan.

Selain itu, translasi alamat yang diterapkan dalam NAT, membuat para *cracker* di Internet tidak mungkin menyerang langsung sistem-sistem di dalam jaringan internal. *Intruder* harus menyerang dan memperoleh akses ke mesin NAT dulu sebelum menyiapkan serangan ke mesin-mesin di jaringan internal. Penting di ketahui bahwa, sementara dengan NAT jaringan internal terproteksi, namun untuk masalah *security*, tetap saja diperlukan paket *filtering* dan metoda pengamanan lainnya dalam mesin NAT.

Contoh Kasus Instalasi Natd

Sebuah perusahaan kecil memiliki sejumlah komputer dan sambungan ke Internet. Komputer-komputer itu saat ini telah membentuk suatu LAN. Sambungan Internet-nya diasumsikan berupa *dedicated T1 link*

Langkah-langkah yang harus dilakukan

1. Instalasi FreeBSD

Sediakan satu komputer untuk dijadikan *Gateway*. Penulis menyarankan penggunaan **FreeBSD RELEASE 2.2.6** (Natd hanya jalan di FreeBSD 2.2.1 ke atas), karena selain gratis juga *requirement hardware*-nya tidak terlalu boros. PC 486 dengan 16 MB *memory* dan HD 850 MB juga sudah cukup mewah.

Untuk mengetahui proses instalasi FreeBSD, silahkan baca kembali tulisan-tulisan di Infokomputer sebelumnya dan manual FreeBSD sendiri.

2. Instalasi Gateway

Pasang 2 *network interface* agar mesin ini menjadi *gateway*. *Network Card* (misal NE2000 atau 3COM) satu dihubungkan ke jaringan internal dan satu lagi untuk koneksi ke ISP. Misalnya keduanya NE2000 *Compatible*. maka *nick* untuk *card* yang menghadap ke dalam adalah ed0 dan untuk *card* yang menghadap keluar adalah ed1.

Pastikan juga option *gateway* = "YES" tertulis dengan benar dalam *file rc.conf*. Atau bisa juga dengan mengetik perintah: `sysctl -w net.inet.ip.forwarding=1`

3. Instalasi Firewall

Pasang IP *firewall* di mesin FreeBSD ini. Caranya adalah :

- a. Edit *kernel source* di `/usr/src/sys/i386/conf`





Tambahkan *option-option* berikut ini pada file *kernel*.

```
options    IPFIREWALL
options    IPFIREWALL_VERBOSE
options    "IPFIREWALL_VERBOSE_LIMIT=100"
options    IPDIVERT
```

- b. Compile *kernel* tersebut
- c. Aktifkan *firewall* di *rc.conf* dengan menambahkan
firewall="YES"
firewall_type="OPEN"

4. Instalasi Natd

Langkah-langkahnya adalah sbb:

- a. *Download source* nya di `ftp://ftp.suutari.iki.fi/pub/natd`
- b. *Unzip* dan *untar archive* tersebut dengan perintah
`gzip -dc natd_1.12.tar.gz | tar -xvf -`
- c. Lakukan *make* dan *make install* di direktori yang dihasilkan. Ketikkan perintah berikut:
`cd natd_1.12`
`make`
`make install`
- d. Edit *startup file* supaya Natd berjalan secara otomatis
Buat file `natd.sh` di `/usr/local/etc/rc.d`. Isi file tersebut adalah

```
#!/bin/sh
/sbin/ipfw -f flush
/sbin/ipfw add divert 13494 ip from any to any via ed0
/sbin/ipfw add pass all from 127.0.0.1 to 127.0.0.1
/sbin/ipfw add pass ip from any to any
/usr/local/sbin/natd -port 13494 -interface ed0
```

Arti dari file ini adalah:

- ❖ Hapuskan semua rule *firewall*
- ❖ Tambahkan feature *divert* di *port* 13494 (Anda bisa mengganti ini dengan *port* yang Anda inginkan) untuk mendiversi paket dari dan ke *gateway* lewat *interface* `ed0`
- ❖ Bolehkan semua paket lewat di atas local host





- ❖ Bolehkan semua paket IP lewat semua *interface*
 - ❖ Jalankan Natd dengan menjadi *daemon* yang menunggu di *port* 13494 via *interface* ed0.
- e. Reboot mesin FreeBSD-nya supaya setting bisa diaktifkan.

6.5.3 Konfigurasi TCP/IP Client.

Jadikan nomor IP *card* ed0 di FreeBSD sebagai *gateway* dari tiap *workstation*, IP tiap-tiap *work station* harus berada dalam *network* yang sama dengan *card* ed0 yang ada di mesin *gateway*. Misal ed0 di-beri nomor IP 192.168.1.1 dan ed1 167.205.19.5, maka *workstation* diberi nomor IP 192.168.1.2 s/d 192.168.1.14 jika digunakan *mask* 16 atau 255.255.255.240. ed1 adalah *interface* yang memiliki IP *address* valid

Setelah semuanya langkah-langkah di atas dijalankan dengan baik maka, aplikasi Internet di *client* siap dijalankan via NAT.

Untuk kasus lain misalnya sambungan ke Internet-nya menggunakan modem, maka mekanismenya sama saja, tinggal diganti *interface* di *gateway* yang menghadap keluar dengan *interface* modem (tun0) dan jalankan program ppp untuk men-*dial* ISP-nya. Khusus untuk *dial-out*, ppp sebenarnya memiliki mekanisme sendiri untuk kasus ini yaitu dengan option *-alias*. Jadi jika kita menjalankan ppp dengan option *-alias* maka kita tidak perlu menjalankan Natd, karena option ini menyediakan fasilitas yang sama dengan Natd khusus untuk *dial-out*.

Natd hanyalah salah satu cara untuk menghemat persediaan IP *address* yang semakin menipis. Dengan adanya fakta bahwa untuk bergabung ke Internet, *host* pencari informasi (*Client*) sebenarnya tidak perlu memiliki IP *address* legal, maka IP *address* legal tersebut bisa dicadangkan untuk *host-host* penyedia informasi (*Server*). Penelitian untuk terus memperbaiki performansi Internet ini masih terus dikembangkan. Sekarang ini juga sedang dikembangkan model IP versi baru yaitu IP versi 6 (IPv6), yang bisa menampung lebih banyak lagi komputer-komputer di Internet. Namun demikian untuk kondisi sekarang, Natd masih merupakan solusi ampuh sebelum IPv6 diterapkan.

6.6 Rangkuman

Teknologi NAT memungkinkan alamat IP lokal/'private' terhubung ke jaringan publik, seperti Internet. Sebuah router NAT ditempatkan antara jaringan lokal (inside network) dan jaringan publik (outside network), dan mentranslasikan alamat lokal/internal menjadi alamat IP global yang unik sebelum mengirimkan paket ke jaringan luar seperti Internet.

Dengan NAT, jaringan internal/lokal, tidak akan terlihat oleh dunia luar/internet. IP lokal yang cukup banyak dapat dilewatkan ke Internet hanya dengan melalui translasi ke satu IP publik/global.

Dua tipe NAT adalah Static dan Dinamik yang keduanya dapat digunakan secara terpisah maupun bersamaan.

NAT Statik : Translasi Static terjadi ketika sebuah alamat lokal (inside) di petakan ke sebuah alamat global/internet (outside). Alamat lokal dan global dipetakan satu lawan satu secara Statik.

NAT Dinamik : NAT dengan Pool (kelompok), Translasi Dinamik terjadi ketika router NAT diset untuk memahami alamat lokal yang harus ditranslasikan, dan kelompok (pool) alamat global yang akan digunakan untuk terhubung ke internet. Proses NAT Dinamik ini dapat memetakan beberapa kelompok alamat lokal ke beberapa kelompok alamat global.





NAT Overload merupakan sejumlah IP lokal/internal dapat ditranslasikan ke satu alamat IP global/outside. Hal ini sangat menghemat penggunaan alokasi IP dari ISP. Sharing/pemakaian bersama satu alamat IP ini menggunakan metoda port multiplexing, atau perubahan port ke packet outbound.

6.7 Soal Latihan :

1. Jelaskan fungsi gateway dan bagaimana bentuk gateway tersebut
2. Jelaskan tentang Proxy Server
3. Apa yang membedakan NAT dengan system proxy
4. Mengapa sebuah jaringan memerlukan NAT dan kapan sebaiknya NAT digunakan
5. Bagaimana cara kerja NAT, jelaskan secara singkat

DAFTAR PUSTAKA

FreeBSD Handbook. FreeBSD Inc.2002

NAT, Mudji Basuki, mudji@infoteknologi.com, <http://www.ilmukomputer.com>

Network Address Translation (NAT): Cara lain menghemat IP Address, Tito Sugiharta, Laboratorium Sistem Informasi & Keputusan (LSIK), Teknik Industri ITB, 2002.

Networking UNIX, The Complete Reference for UNIX networks, Douba, Salim, SAMS Publishing. 1995

Unix Integration to WAN: Applied Computer Internetworking. CNRG ITB, 2000.





KUNCI JAWABAN SOAL

BAB 1. JARINGAN KOMPUTER

1. Jaringan komputer adalah "interkoneksi" antara 2 komputer *autonomous* atau lebih, yang terhubung dengan media transmisi kabel atau tanpa kabel (wireless).

Autonomous adalah apabila sebuah komputer tidak melakukan kontrol terhadap komputer lain dengan akses penuh, sehingga dapat membuat komputer lain, restart, shutdowns, kehilangan file atau merusakkan sistem

2. Perbedaan utama antara jaringan komputer dan sistem terdistribusi lebih terletak pada perangkat lunaknya (khususnya sistem operasi) bukan pada perangkat kerasnya, karena perangkat lunaklah yang menentukan tingkat keterpaduan dan transparansi jaringan yang bersangkutan.

3. Tujuan utama dari terbangunnya sebuah jaringan pada suatu perusahaan adalah:

Resource sharing yang bertujuan agar seluruh program, peralatan, khususnya data dapat digunakan oleh setiap orang yang ada pada jaringan.

Saving Money (Penghematan uang/anggaran): Perangkat dan data yang dapat dishare akan membuat penghematan anggaran yang cukup besar, karena tidak perlu membeli perangkat baru untuk dipasang ditiap-tiap unit komputer

High reliability (kehandalan tinggi): Sistem Informasi Manajemen Kantor Terpadu atau Sistem Pelayanan Satu Atap dengan teknologi client-server, internet maupun intranet dapat diterapkan pada jaringan komputer, sehingga dapat memberikan pelayanan yang handal, cepat dan akurat sesuai kebutuhan dan harapan.

4. Penggunaan jaringan oleh masyarakat luas akan menyebabkan timbulnya masalah-masalah sosial, etika, politik, ekonomi, budaya, hukum yang tak terelakkan.
5. Jenis-jenis jaringan komputer: LAN, MAN dan WAN

Multiple Choice

1. d. Non-Autonomous





2. b. Sistem Terdistribusi
3. a. Jaringan Komputer
4. b. Peer to peer
5. c. Client - Server

BAB 2. MENGENAL HARDWARE DAN TOPOLOGI JARINGAN KOMPUTER

1. Tipe kabel koaksial :
 - Thin Ethernet (**ThinNet**)
 - Thick Ethernet (**ThickNet**)

Kabel jenis ini dipergunakan pada topologi **ring** atau **bus**

2. Cara pemasangan kabel UTP pada konektor RJ-45 :

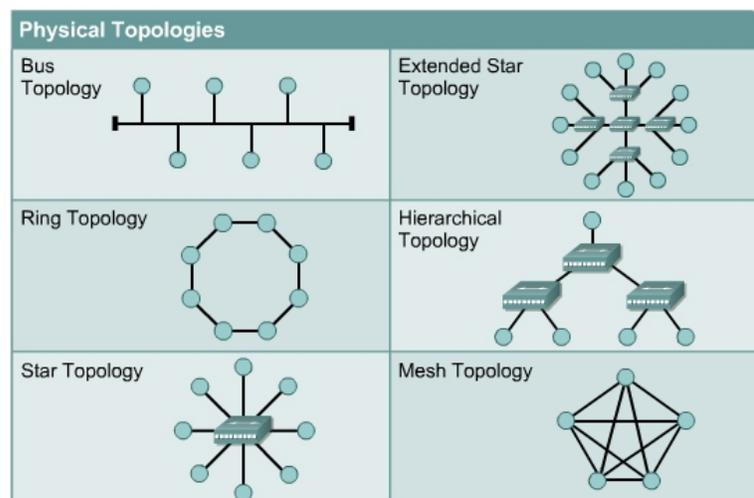
- **Straight Through**
- **Cross Over**
- **Roll Over**

Pada jaringan lokal kabel UTP ini digunakan pada topologi Star atau tree (hirarki)

2. MAC Address adalah **alamat sepanjang 48 bit yang dikenal sebagai Ethernet address** (HW Address), yang bersifat unique (dikeluarkan oleh pabrik pembuat).

Cara kerja Ethernet Card berdasarkan **broadcast network** yaitu **setiap node dalam suatu jaringan menerima setiap transmisi data yang dikirim oleh suatu node yang lain.**

3. Topologi jaringan komputer



Topologi bus dan ring menggunakan kabel coaxial, topologi star, extended star dan hirarki (tree) menggunakan kabel UTP, topologi mesh menggunakan teknologi wireless.

Topologi bus:

Keuntungan:

- murah, karena tidak memakai banyak media, kabel yang dipakai sudah umum (banyak tersedia dipasaran)





- setiap komputer dapat saling berhubungan langsung.

Kerugian:

Sering terjadi hang / crass talk, yaitu bila lebih dari satu pasang memakai jalur diwaktu yang sama, harus bergantian atau ditambah relay.

Topologi Ring

Keuntungan:

- Kegagalan koneksi akibat gangguan media, dapat diatasi dengan jalur lain yang masih terhubung.
- Penggunaan sambungan point to point membuat transmission error dapat diperkecil

Kerugian:

- Data yang dikirim bila melalui banyak komputer, transfer data menjadi lambat.

Topologi Star:

Keuntungan:

- Akses ke station lain (client atau server) cepat
- Dapat menerima workstation baru selama port di central node (hub/switch) tersedia.
- Hub/switch bertindak sebagai konsentrator.
- Hub/switch dapat disusun seri (bertingkat) untuk menambah jumlah station yang terkoneksi di jaringan.
- User dapat lebih banyak dibanding topologi bus, maupun ring.

Kerugian:

Bila traffic data cukup tinggi dan terjadi collision, maka semua komunikasi akan ditunda, dan koneksi akan dilanjutkan/dipersilahkan dengan cara random, apabila hub/switch mendetect tidak ada jalur yang sedang dipergunakan oleh node lain.

5. Baseband

*Menggunakan sinyal digital. Transmisi yang digunakan bersifat **bidirectional** dan dipakai hanya untuk topologi bus yang jangkauannya pendek.* Media yang digunakan kabel coaxial (50 ohm), dengan spesifikasi IEEE 802.3 (Ethernet), bila inti kabel coaxial berdiameter 0.4 inch dan data rate 10 Mbps, maka dengan perangkat ini kita dapat menjangkau jarak 500 m (dikenal dengan sebutan *10BASE5*). Untuk jarak yang lebih jauh dapat digunakan repeater.

Broadband

*Menggunakan sinyal analog dengan **Frequency Division Multiplexing (FDM)**. Spektrum media transmisi dapat dibagi sesuai keperluan, jarak yang dijangkau lebih jauh dibanding baseband dan mendukung topologi tree.*

BAB 3. INTRANET, EXTRANET & INTERNET

1. **Intranet** adalah sebuah jaringan komputer berbasis protokol TCP/IP seperti internet, hanya saja digunakan dalam internal perusahaan/kantor, dengan aplikasi berbasis web dan teknologi komunikasi data seperti internet.





*Jika sebuah badan usaha / bisnis / institusi mengekspose sebagian dari internal jaringannya ke komunitas di luar, maka hal ini yang disebut dengan **ekstranet**.*

***Internet** merupakan koneksi jaringan komputer global yang menghubungkan seluruh komputer didunia meskipun berbeda mesin dan sistem operasi.*

2. Persamaan yang dimiliki antara intranet dan internet, yakni: **keduanya merupakan jaringan komputer berbasis protokol TCP/IP, aplikasi yang dipergunakan berbasis web**, teknologi komunikasi data (perangkat hardware yang digunakan) relatif sama.
3. Sebuah LAN bisa saja merupakan intranet, apabila ia tidak dapat diakses oleh jaringan luar, dan aplikasi yang dibangun didalamnya berbasis web. Namun intranet bisa lebih besar dari sebuah jaringan lokal (LAN), apabila sebuah institusi (kantor) membangun jaringan antar kantor dalam satu wilayah (MAN atau WAN) dengan menggunakan teknologi/jalur internet namun hanya membuat jalur private/khusus yang tidak dapat diakses jaringan lain diluar institusi (kantor) tersebut.
4. Komponen-komponen pembentuk intranet antara lain:
 1. Aplikasi browser
 2. Komputer server
 3. Perangkat jaringan dan
 4. Protokol TCP/IP
 5. Bahasa pemrograman
 6. Komputer client
 7. Perangkat bantu pengembang (development tool) u/ manajemen jaringan lokal.
5. Meskipun intranet dan sistem Client Server dibangun dengan basic topologi TCP/IP, namun intranet membutuhkan perhatian yang lebih besar terhadap proses suatu bisnis, perubahan suatu data/informasi harus dilakukan secara continue dan uptodate, administrator jaringan memegang peranan penting dalam mengatur otoritas pembuat informasi dan akses yang diperkenankan bagi penerima informasi.

Pada sistem client server biasa, yang memegang peranan penting adalah programmer atau analis system yang membuat/ merancang system dan program serta mengatur otoritas bagi yang mengelola (entry) data dan penerima informasi.

6. Ada banyak teknologi yang dapat kita gunakan untuk melakukan koneksi ke internet, seperti:
 - ❖ Dial-up melalui jalur PSTN (Public Line)
 - ❖ Dial-up dengan teknologi GPRS dan CDMA
 - ❖ DSL (Digital Subscriber Line)
 - ❖ ADSL (Asynchronous Digital Subscriber Line)
 - ❖ ISDN (*Integrated Services Digital Network*)
 - ❖ PLC (PowerLine Communication)
 - ❖ Leased-Line (Dedicated Line)
 - ❖ Terrestrial
 - ❖ Frame Relay
 - ❖ Wireless (Wi-Fi, Microwave, WiMAX)
 - ❖ VSAT (Very Small Aperture Terminal)
7. Jenis-jenis pelanggaran di Internet, diantaranya:
 - a. Pemalsuan identitas
 - b. Pembobolan kartu kredit milik orang lain.





- c. Pemilikan / penggunaan software secara illegal.
 - d. Penyebaran pornografi
 - e. Pencemaran nama baik
 - f. Pelanggaran kode etik
 - g. Penyalahgunaan wewenang admin
 - h. Penyusupan / akses kesistem lain secara illegal
 - i. Perusakan dan perubahan system atau tampilan situs
 - j. dll.
8. **Indonesia sudah memiliki undang-undang perlindungan HaKI**, Hukum yang mengatur tentang pelecehan dan pornografi, kegiatan kriminal di internet, **namun belum semua masalah yang timbul akibat kegiatan pelanggaran di internet dapat dituntut secara hukum**, karena hukum yang khusus untuk menyelesaikan masalah-masalah yang timbul didunia maya (cyberlaw belum ditetapkan). Belum lagi kesiapan SDM pelindung dan aparat penegak hukum tersebut, pengetahuan dan pemahaman tentang teknologi internet ini juga belum merata pada semua komponen bangsa ini.
9. Seperti dua sisi mata uang logam, yang masing-masing sisi punya pandangan (tampilan) yang berbeda. **Kegiatan hacking menurut praktisi jaringan bisa saja merupakan kegiatan positif** untuk mengembangkan pengetahuan (aktifitasnya positif, hasilnya positif), termotifasi untuk belajar lebih dibandingkan orang lain, dan berbagi pengetahuan tanpa pamrih materi yang berlebihan. **Tapi bagi pemilik system atau orang-orang yang tidak mengerti dan sudah ter-provokasi dengan pengertian negatif maka kegiatan tersebut dapat digolongkan dengan kegiatan kriminal.**
- Demikian juga dengan kegiatan carding, bagi pelaku aktifitas tersebut bisa dianggap seperti kegiatan iseng-iseng berhadiah, atau pembuktian keterampilan yang dimiliki, namun bagi pemilik rekening yang dananya diambil tanpa izin, serta aparat penegak hukum, maka carding bisa digolongkan sama dengan kegiatan pencurian, penipuan (pemalsuan identitas), dan seabrek tuduhan lain.
10. Hotspot merupakan coverage area yang menyediakan koneksi internet bagi perangkat wireless yang terhubung. Biasanya pengguna komputer Laptop sering memanfaatkan fasilitas ini disuatu tempat yang menyediakan hotspot. Pada laptop model terbaru biasanya sudah terdapat fasilitas Wi-Fi 802,11 b/g yang dijadikan standar koneksi jaringan tanpa kabel (jarak dekat).

BAB 4. TCP/IP & IP ADDRESS

1. a. TCP/IP
2. a. Dapat dipakai oleh semua jenis mesin komputer,
b. Kemampuannya untuk menjamin paket sampai ketujuan,
c. Dapat diterapkan pada semua Sistem Operasi
3. a. Terciptanya protokol-protokol umum,
b. Meningkatkan efesiensi komunikasi data,
c. Dapat dipadukan dengan teknologi WAN yang ada &
d. Mudah di konfigurasikan
4. a. Pengiriman/pengambilan file (FTP) dari komputer lain
b. Remote login (telnet)





5. c. ICMP
6. c. Tidak ada duplikasi paket
d. Tidak menjamin paket akan sampai ketujuan
7. b. 202.159.23.45
8. a. 11001010.10011111.00010111.00000000
9. c. APJII,
d. ISP / PJI
10. b. APNIC

BAB 5. SUBNET & KONSEP ROUTING

Soal 1.

Network : 192.168.0/25
 Netmask : 255.255.255.128 **11111111.11111111.11111111.10000000**
 Wildcard : 0 .0 .0 .127 00000000.00000000.00000000 .01111111

Net Address : 192.168.0.0 **11000000.10101000.00000000.00000001**
 IP Host Awal: 192.168.0.1 11000000.10101000.00000000 .00000001
 IP HostAkhir: 192.168.0.126 11000000.10101000.00000000. 01111110
 Broadcast : 192.168.0.127 11000000.10101000.00000000 .01111111
 Hosts/Net : 126 (1 Network)

Net Address : 192.168.0.128 **11000000.10101000.00000000.1 0000000**
 IP Host Awal: 192.168.0.129 11000000.10101000.00000000.1 0000001
 IP HostAkhir: 192.168.0.254 11000000.10101000.00000000.1 1111110
 Broadcast : 192.168.0.255 11000000.10101000.00000000.1 1111111
 Hosts/Net : 126 (1 Network)

Subnets : 2 Network
 Hosts Max : 252

Soal 2.

172.16.12/27

Jumlah maximum host tiap LAN = 30 bh

Subnet Mask = 255.255.255.224

Subnet	Struktur IP Address	Network Address	Broadcast Address
Subnet 1	172.16.12. hhhhh 000	172.16.12.0	172.16.12.31
Subnet 2	172.16.12. hhhhh 001	172.16.12.32	172.16.12.63





Subnet 3	172.16.12. hhhhh	010	172.16.12.64	172.16.12.95
Subnet 4	172.16.12. hhhhh	011	172.16.12.96	172.16.12.127
Subnet 5	172.16.12. hhhhh	100	172.16.12.128	172.16.12.159
Subnet 6	172.16.12. hhhhh	101	172.16.12.160	172.16.12.191
Subnet 7	172.16.12. hhhhh	110	172.16.12.192	172.16.12.223
Subnet 8	172.16.12. hhhhh	111	172.16.12.224	172.16.12.255

Soal 3.

Net Address **202.152.204.64**
 Net Mask 255.255.255.224
 IP Address host pertama 202.152.204.65
 IP Address host terakhir 202.152.204.94
 IP Broadcast **202.152.204.95**
Host / Net = 30

Soal 4.

192.168.10.0/26
 Net Mask = 255.255.255.192
Jumlah Subnet = 4
 Host / LAN = 30

Soal 5.

Bit Maske d	Bit Host ID	CID R	Subnet	Net Mask	Host Max	Host per Networ k
0	8	/24	1	255.255.255.0	254	254
1	7	/25	2	255.255.255.128	252	126
2	6	/26	4	255.255.255.192	248	62
3	5	/27	8	255.255.255.224	240	30
4	4	/28	16	255.255.255.240	224	14
5	3	/29	32	255.255.255.248	192	6
6	2	/30	64	255.255.255.252	128	2

Soal 6.





- a. Subnetting merupakan proses memecah satu kelas IP Address menjadi beberapa subnet dengan jumlah host yang lebih sedikit, dan untuk menentukan batas network ID dalam suatu subnet, digunakan subnet mask.
 - b. Konsep subnetting dari IP Address merupakan teknik yang umum digunakan di Internet untuk mengefisienkan alokasi IP Address dalam sebuah jaringan supaya bisa memaksimalkan penggunaan IP Address.
 - c. Esensi dari subnetting adalah “memindahkan” garis pemisah antara bagian network dan bagian host dari suatu IP Address. Beberapa bit dari bagian hostID dialokasikan menjadi bit tambahan pada bagian networkID.
 - d. Tujuan dari subnetting adalah memecah satu kelas dari IP Address menjadi beberapa subnet, untuk mengefisienkan alokasi IP Address dalam suatu jaringan. Tujuan lain dari subnetting yang tidak kalah pentingnya adalah untuk mengurangi tingkat kongesti (gangguan/tabrakan) lalu lintas data dalam suatu network
- 7. b. Network Address
 - 8. c. Broadcast Address
 - 9. d. Host; host itu sendiri
 - 10. a. 127.0.0.1
 - 11. a. Network Prefix dengan netmask 255.255.255.0
c. Blok IP Address dengan host maksimal 254
 - 12. a. Interior Gateway Protocol
 - 13. b. Routing Loop
 - 14. b. Paket yang dikirim tidak mencapai tujuan
c. Paket yang dikirim akan dibuang
 - 15. a. RIP
d. IGRP
 - 16. a. IGRP c. OSPF
b. EIGRP d. NLSP
 - 17. d. Split Horizon
 - 18. b. Distance vector
d. Hop Count
 - 19. a. Static Routing
b. Default Routing
c. Dynamic Routing
 - 20. a. Route Poisoning

BAB 6. NAT (NETWORK ADDRESS TRANSLATION)





1. Gateway berfungsi untuk menghubungkan dua network yang berbeda. *Gateway* bisa berupa komputer yang memiliki minimal 2 buah *network interface* untuk menghubungkan 2 buah jaringan atau lebih atau berupa perangkat router atau juga berupa software.
2. Proxy server merupakan aplikasi yang bisa di install pada komputer gateway. Komputer proxy server akan menyimpan halaman web yang pernah di telusuri pengguna komputer dalam jaringan, dan menyimpannya di dalam cache memori untuk jangka waktu tertentu tergantung *setting*-nya, untuk sewaktu-waktu bila ada *request* halaman web yang sama, tidak perlu lagi mengambil dari web server, tetapi cukup dari cache memori komputer proxy server, sehingga akses akan kelihatan menjadi lebih cepat.
3. Yang membedakan NAT dengan system proxy adalah

Suatu jaringan kecil dengan *proxy* bisa menempatkan beberapa mesin untuk mengakses *web* dibelakang sebuah mesin yang memiliki IP *address* valid. *Proxy* server ini tidak sesuai untuk jaringan yang besar, kalau tempat penyimpanan hanya mengandalkan cache memori. Menambah *hard disk* dan RAM pada server *proxy* supaya *proxy* berjalan efisien dapat dilakukan (kecuali ada masalah dengan biaya). Karena persentase *web page* yang bisa dilayani oleh *cache proxy* akan makin menurun sejalan dengan semakin menipisnya ruang kosong di *hard disk*, sehingga penggunaan *cache proxy* menjadi tidak lebih baik dari pada sambungan langsung.

NAT menawarkan solusi yang lebih fleksibel dan *scalable*. NAT menghilangkan keharusan mengkonfigurasi *proxy/sock* dalam tiap *client*. NAT lebih cepat dan mampu menangani trafik *network* untuk beribu-ribu *user* secara simultan.

4. Mengapa sebuah jaringan memerlukan NAT dan kapan sebaiknya NAT digunakan

NAT digunakan untuk menyelesaikan masalah pengalamatan IP

Teknologi NAT memungkinkan alamat IP lokal/'private' terhubung ke jaringan publik seperti Internet. Sebuah router NAT ditempatkan antara jaringan lokal (inside network) dan jaringan publik (outside network), dan mentranslasikan alamat lokal/internal menjadi alamat IP global yang unik sebelum mengirimkan paket ke jaringan luar seperti Internet.

Dengan NAT, jaringan internal/lokal, tidak akan terlihat oleh dunia luar/internet. IP lokal yang cukup banyak dapat dilewatkan ke Internet hanya dengan melalui translasi ke satu IP publik/global.

Kapan sebaiknya NAT Digunakan?

Gunakan NAT Jika:

- Anda membutuhkan koneksi ke Internet dan hosts/komputer-komputer anda tidak mempunyai alamat IP global.
- Anda berganti ke ISP baru dan anda diharuskan menggunakan alamat IP dari ISP baru tersebut untuk jaringan anda.

Keuntungan menggunakan NAT

Jika anda harus merubah alamat IP internal anda, dikarenakan anda berganti ISP atau dua intranet digabungkan (misalnya penggabungan dua perusahaan), NAT dapat digunakan untuk mentranslasikan alamat IP yang sesuai. NAT memungkinkan anda menambah alamat IP, tanpa merubah alamat IP pada hosts atau komputer anda. Dengan demikian akan menghilangkan duplicate IP tanpa pengalamatan kembali host atau komputer anda.

5. Bagaimana cara kerja NAT, jelaskan secara singkat

NAT dapat melewatkan alamat jaringan lokal ('private') menuju jaringan 'public' seperti Internet. Alamat 'private' yang berada pada jaringan lokal, mengirim paket melalui router NAT, yang kemudian dirubah





oleh router NAT menjadi alamat IP Publik dari ISP sehingga paket tersebut dapat diteruskan melewati jaringan publik atau internet.

Dengan NAT, aturan bahwa untuk berkomunikasi harus menggunakan IP *address* legal, dilanggar. NAT bekerja dengan jalan mengkonversikan IP *address* ke satu atau lebih IP *address* lain. IP *address* yang dikonversi adalah IP *address* yang diberikan untuk tiap mesin dalam jaringan internal (bisa sembarang IP). IP *address* yang menjadi hasil konversi terletak di luar jaringan internal tersebut dan merupakan IP *address* legal yang valid/routable.

