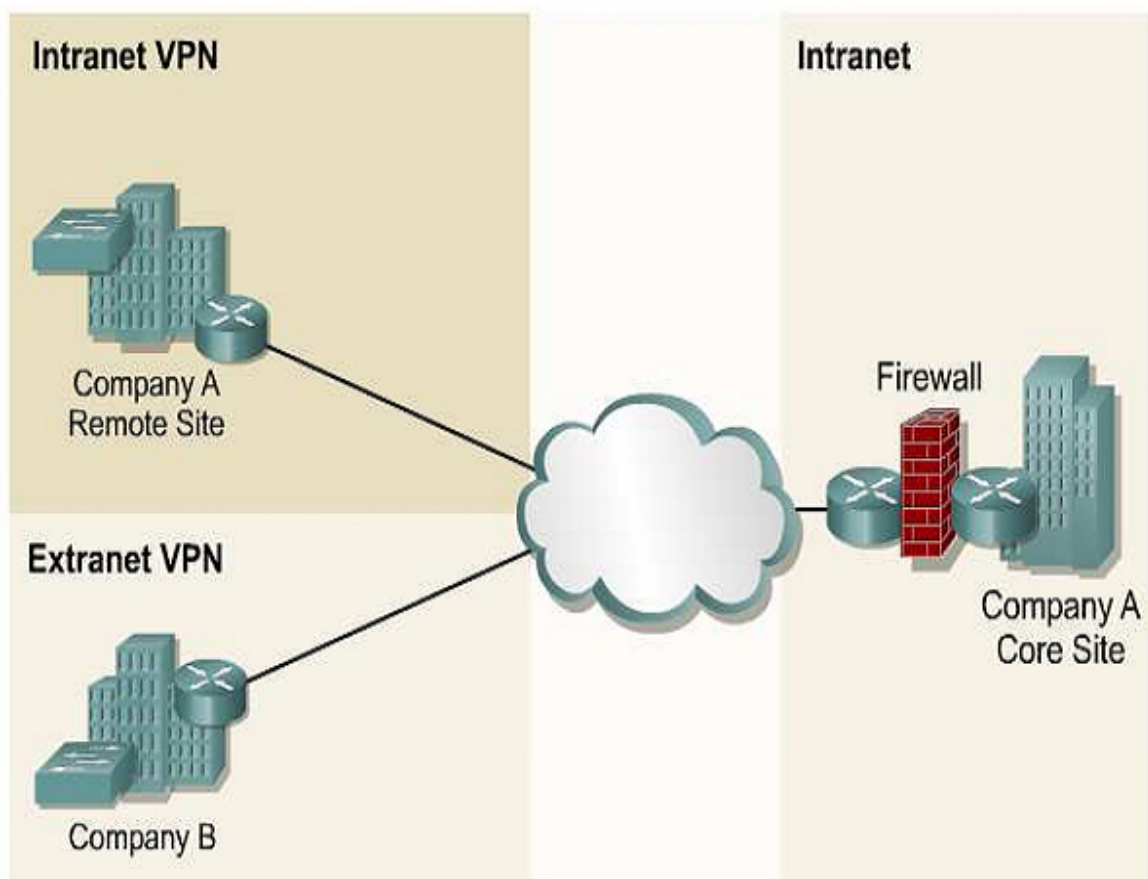


KODE MODUL

NTW.OPR.200.(2).A

SEKOLAH MENENGAH KEJURUAN
BIDANG KEAHLIAN TEKNOLOGI INFORMASI DAN KOMUNIKASI
PROGRAM KEAHLIAN TEKNIK KOMPUTER DAN JARINGAN

Instalasi Perangkat Jaringan Berbasis Luas (Wide Area Network)



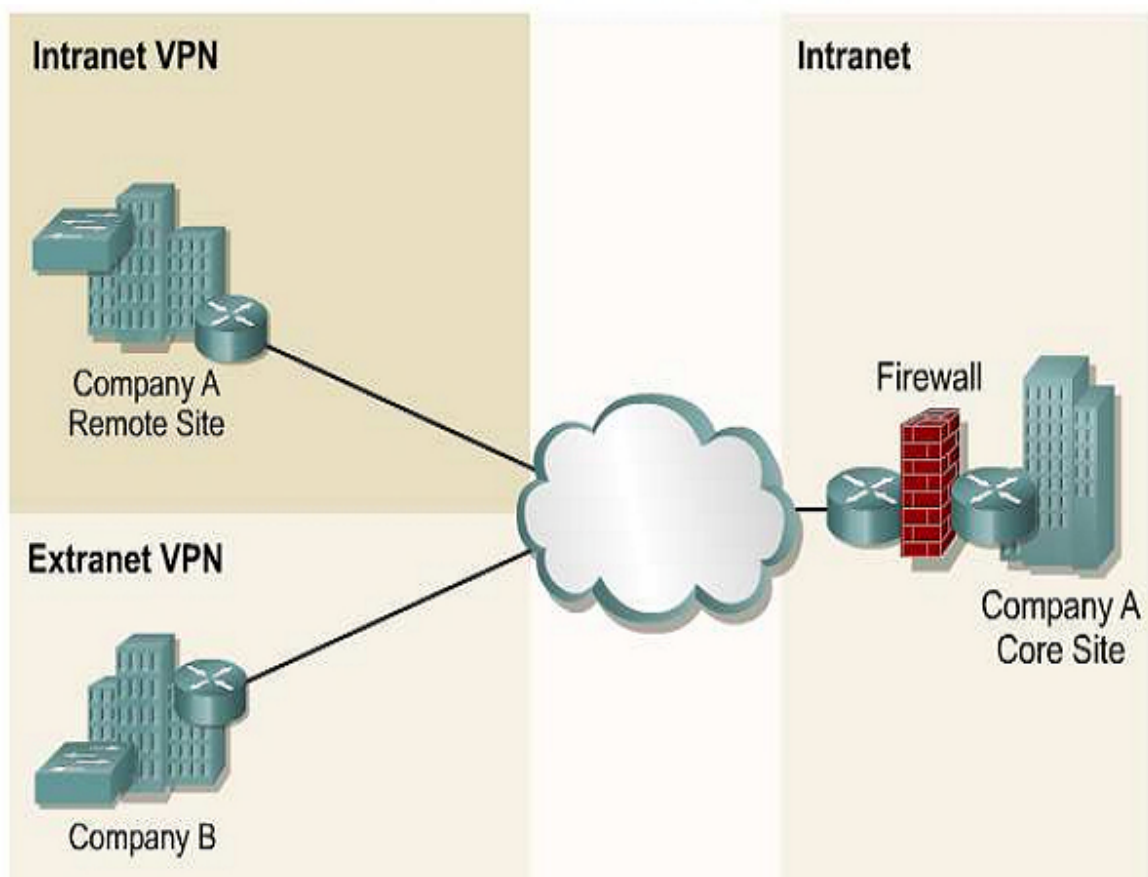
DIREKTORAT PEMBINAAN SEKOLAH MENENGAH KEJURUAN
DIREKTORAT JENDERAL MANAJEMEN PENDIDIKAN DASAR DAN MENENGAH
DEPARTEMEN PENDIDIKAN NASIONAL
2005

KODE MODUL

NTW.OPR.200.(2).A

SEKOLAH MENENGAH KEJURUAN
BIDANG KEAHLIAN TEKNOLOGI INFORMASI DAN KOMUNIKASI
PROGRAM KEAHLIAN TEKNIK KOMPUTER DAN JARINGAN

Instalasi Perangkat Jaringan Berbasis Luas (Wide Area Network)



DAFTAR ISTILAH / GLOSSARY

WAN	: Wide Area Network
Troubleshooting	: Pemecahan permasalahan yang sering terjadi
Software	: Piranti lunak, sebuah aplikasi program komputer
Topologi jaringan	: Cara menghubungkan antar komputer
Server	: Server adalah komputer yang menjadi sentral dan menyediakan fasilitas bagi komputer-komputer lain
Host	: Workstation (komputer pengguna)
Protocol	: Aturan
CPE	: Customer Premises Equipment
DCE	: Data Circuit-terminating Equipment
DTE	: Data Terminal Equipment
CSU	: Channel Service Unit
DSU	: Data Service Unit
AS	: Autonomus System
RIP	: Routing Information Protocol
OSPF	: Open Shortest Path First
IOS	: Internetworking Operating System
NVRAM	: Nonvolatile Random Access Memory
HDLC	: High-Level Data Link Control
PPP	: Point to Point Protocol
DSSS	: Direct Sequence Spread Spectrum
OFDM	: Othogonal Frequency Division Multiplexing
AP	: Access Point
SSID	: Service Set Identifier
WEP	: Wireless Equivalency Protocol
dB	: decibel
EIRP	: Effective Isotropic Radiated Power

KONSEP DASAR JARINGAN WAN

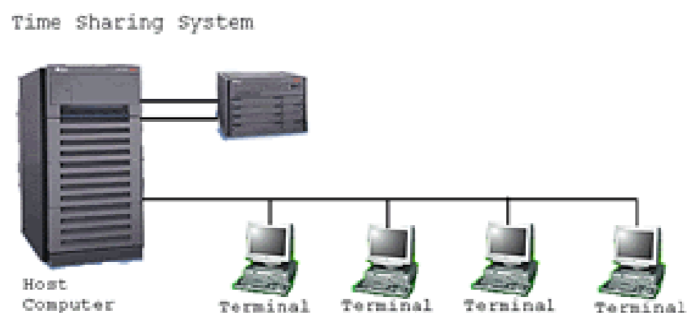
Tujuan Kegiatan Pemelajaran

Setelah mempelajari kegiatan belajar ini peserta diklat mampu menjelaskan media, perangkat, teknologi dan protocol pada jaringan berbasis luas (WAN).

Uraian Materi

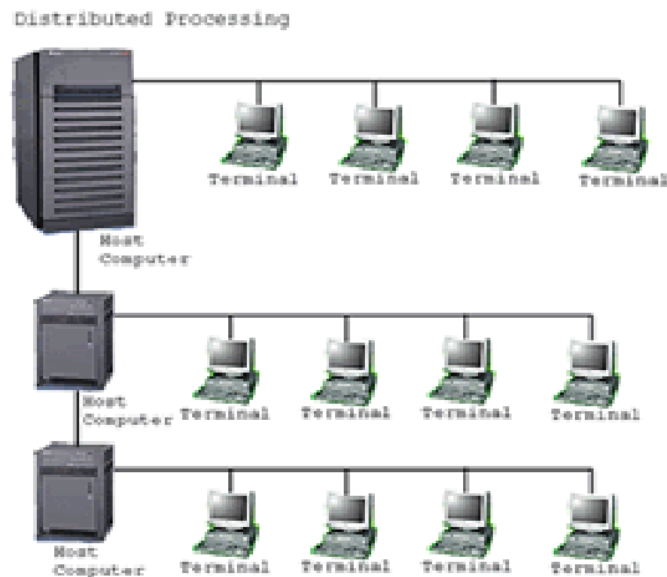
1. Latar Belakang dan Sejarah Jaringan

Pada tahun 1940-an di Amerika ada sebuah penelitian yang ingin memanfaatkan sebuah perangkat komputer secara bersama. Ditahun 1950-an ketika jenis komputer mulai membesar sampai terciptanya super komputer, karena mahalnya harga perangkat komputer maka ada tuntutan sebuah komputer mesti melayani beberapa terminal. Dari sinilah maka muncul konsep distribusi proses berdasarkan waktu yang dikenal dengan nama TSS (Time Sharing System), bentuk pertama kali jaringan (network) komputer diaplikasikan. Pada sistem TSS beberapa terminal terhubung secara seri ke sebuah host komputer.



Gambar 1

Selanjutnya konsep ini berkembang menjadi proses distribusi (Distributed Processing). Dalam proses ini beberapa host komputer mengerjakan sebuah pekerjaan besar secara paralel untuk melayani beberapa terminal yang tersambung secara seri disetiap host komputer.



Gambar 2.

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 maupun komunikasi antar komputer (Peer to Peer System) saja tanpa melalui komputer pusat. Untuk itu mulailah berkembang teknologi jaringan lokal yang dikenal dengan sebutan LAN (Local Area Network). Demikian pula ketika Internet mulai diperkenalkan, maka sebagian besar LAN yang berdiri sendiri mulai berhubungan dan terbentuklah jaringan raksasa ditingkat dunia yang disebut dengan istilah WAN (World Area Network).

2. Jenis-jenis jaringan

Secara umum jaringan komputer terdiri atas lima jenis:

a. Local Area Network (LAN)

Local Area Network (LAN), merupakan jaringan local yang digunakan oleh suatu organisasi untuk berbagi sumber daya (resources sharing) seperti printer dan file. LAN biasanya dibangun dan dikelola oleh organisasi tersebut. Teknologi LAN antara lain Ethernet, Token Ring dan FDDI.

b. Metropolitan Area Network (MAN)

Metropolitan Area Network (MAN), pada dasarnya merupakan versi LAN yang berukuran lebih besar dan biasanya menggunakan teknologi yang sama dengan LAN. MAN dapat mencakup kantor-kantor perusahaan yang letaknya berdekatan atau juga sebuah kota dan dapat dimanfaatkan untuk keperluan pribadi (swasta) atau umum. MAN mampu menunjang data dan suara, bahkan dapat berhubungan dengan jaringan televisi kabel.

c. Wide Area Network (WAN)

Wide Area Network (WAN), jangkauannya mencakup daerah geografis yang luas, seringkali mencakup sebuah negara bahkan benua. WAN memungkinkan terjadinya komunikasi diantara dua perangkat yang terpisah jarak yang sangat jauh. WAN menginterkoneksi beberapa LAN yang kemudian menyediakan akses ke komputer-komputer atau file server pada lokasi lain. Beberapa teknologi WAN antara lain adalah Modem, ISDN, DSL, Frame Relay, T1, E1, T3, E3 dan SONET.

d. Intranet

Melibatkan jaringan LAN dan Web Server yang terpasang pada jaringan LAN tersebut. Web Server digunakan untuk melayani permintaan pengguna internal suatu organisasi untuk menampilkan data dan gambar. Intranet ini mempunyai sifat tertutup yang berarti pengguna dari luar organisasi tidak dapat mengaksesnya.

e. Internet

Sebenarnya terdapat banyak jaringan di dunia ini, seringkali menggunakan perangkat keras dan perangkat lunak yang berbeda-beda. Orang yang terhubung ke jaringan sering berharap untuk bisa berkomunikasi dengan orang lain yang terhubung ke jaringan lainnya. Keinginan seperti ini memerlukan hubungan antar jaringan yang seringkali tidak kompatibel dan berbeda. Biasanya untuk melakukan hal ini diperlukan sebuah mesin yang disebut gateway guna melakukan hubungan dan melaksanakan terjemahan yang diperlukan, baik perangkat keras maupun perangkat lunaknya. Kumpulan jaringan yang terinterkoneksi inilah yang disebut dengan internet.

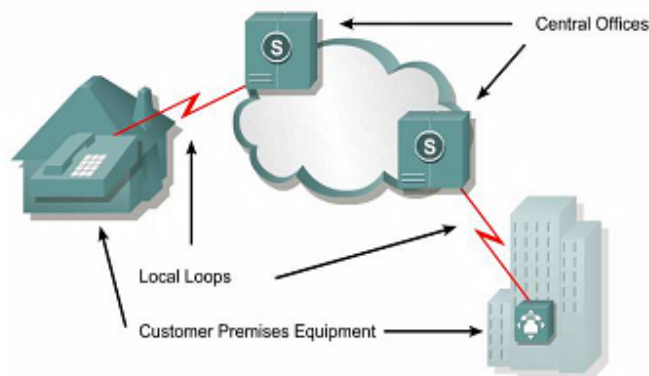
Konsep Dasar Jaringan WAN

Ketika sebuah perusahaan berkembang menjadi beberapa lokasi, maka masing–masing lokasi mengembangkan jaringan lokalnya. Ketika dibutuhkan koneksi antar LAN pada perusahaan tersebut maka terbentuklah Wide Area Network.

3. Wide Area Network

Terdapat begitu banyak pilihan yang tersedia untuk mengimplementasikan WAN yang bisa dibedakan berdasarkan teknologi, kecepatan dan biaya yang dibutuhkan.

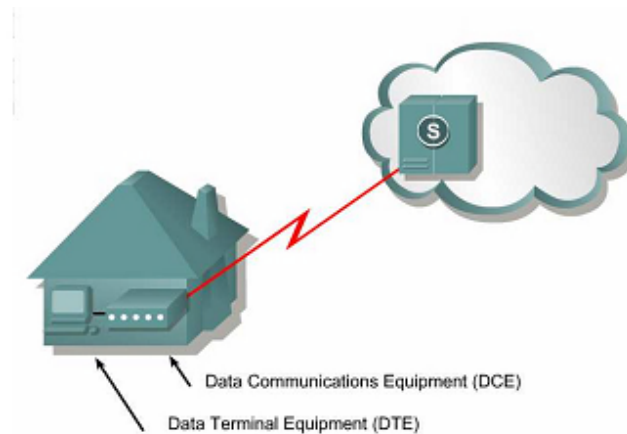
Satu perbedaan utama LAN dengan WAN adalah organisasi harus berlangganan kepada penyedia jaringan dari perusahaan penyedia jaringan yang ada. Sebuah WAN menggunakan jalur data untuk membawa data menuju ke internet dan menghubungkan lokasi–lokasi perusahaan yang terpisah–pisah. Telepon dan layanan data yang paling banyak digunakan pada WAN. Perangkat pada pelanggan disebut CPE (Customer Premises Equipment). Pelanggan memiliki sendiri atau menyewa dari service provider. Kabel tembaga, serat optik atau wireless yang digunakan untuk menghubungkan CPE ke sentral provider terdekat atau ke kantor pusat dari service provider. Media ini sering disebut dengan local loop.



Gambar 3.

Perangkat yang meletakkan data ke local loop disebut DCE (Data Circuit-terminating Equipment). Perangkat pelanggan yang melewatkan data ke DCE disebut dengan DTE (Data Terminal Equipment).

Konsep Dasar Jaringan WAN



Gambar 4.

Jalur WAN menyediakan berbagai macam kecepatan data yang diukur dalam satuan kilobits per second. Dibawah ini berbagai teknologi WAN dan kecepatan yang tersedia.

Tabel Teknologi WAN dan Kecepatannya

Line Type	Signal Standard	Bit Rate Capacity
56	DS0	56 Kbps
64	DS0	64 Kbps
T1	DS1	1.544 Mbps
E1	ZM	2.048 Mbps
E3	M3	34.064 Mbps
J1	Y1	2.048 Mbps
T3	DS3	44.736 Mbps
OC-1	SONET	51.84 Mbps
OC-3	SONET	155.54 Mbps
OC-9	SONET	466.56 Mbps
OC-12	SONET	622.08 Mbps
OC-18	SONET	933.12 Mbps
OC-24	SONET	1244.16 Mbps
OC-36	SONET	1866.24 Mbps
OC-48	SONET	2488.32 Mbps

a. Perangkat WAN

WAN menghubungkan beberapa LAN melalui jalur komunikasi dari service provider. Karena jalur komunikasi tidak bisa langsung dimasukkan ke LAN maka diperlukan beberapa perangkat interface.

Perangkat–perangkat tersebut antara lain:

1) Router

LAN mengirimkan data ke Router, kemudian Router akan menganalisa berdasarkan informasi alamat pada layer 3. Kemudian Router akan meneruskan data tersebut ke interface WAN yang sesuai berdasarkan routing table yang dimilikinya. Router adalah perangkat jaringan yang aktif dan intelegent dan dapat berpartisipasi dalam manajemen jaringan. Router mengatur jaringan dengan menyediakan kontrol dinamis melalui sumber daya dan mendukung tugas dan tujuan dari jaringan. Beberapa tujuan tersebut antara lain konektivitas, perfomansi yang reliabel, kontrol manajemen dan fleksibilitas.

2) CSU/DSU

Jalur komunikasi membutuhkan sinyal dengan format yang sesuai. Untuk jalur digital, sebuah Channel Service Unit (CSU) dan Data Service Unit (DSU) dibutuhkan. Keduanya sering digabung menjadi sebuah perangkat yang disebut CSU/DSU.

3) Modem

Modem adalah sebuah perangkat dibutuhkan untuk mempersiapkan data untuk transmisi melalui local loop. Modem lebih dibutuhkan untuk jalur komunikasi analog dibandingkan digital. Modem mengirim data melalui jalur telepon dengan memodulasi dan demodulasi sinyal. Sinyal digital ditumpangkan ke sinyal suara analog yang dimodulasi untuk ditransmisikan. Pada sisi penerima sinyal analog dikembalikan menjadi sinyal digital atau demodulasi.

4) Communication Server

Communication Server mengkonsentrasikan komunikasi pengguna dial-in dan remote akses ke LAN. Communication Server memiliki beberapa interface analog dan digital serta mampu melayani beberapa user sekaligus.

b. Standar WAN

WAN menggunakan OSI layer tetapi hanya fokus pada layer 1 dan 2. Standar WAN pada umumnya menggambarkan baik metode pengiriman layer 1 dan kebutuhan layer 2, termasuk alamat fisik, aliran data dan enkapsulasi. Dibawah ini adalah organisasi yang mengatur standar WAN.

Layer 1

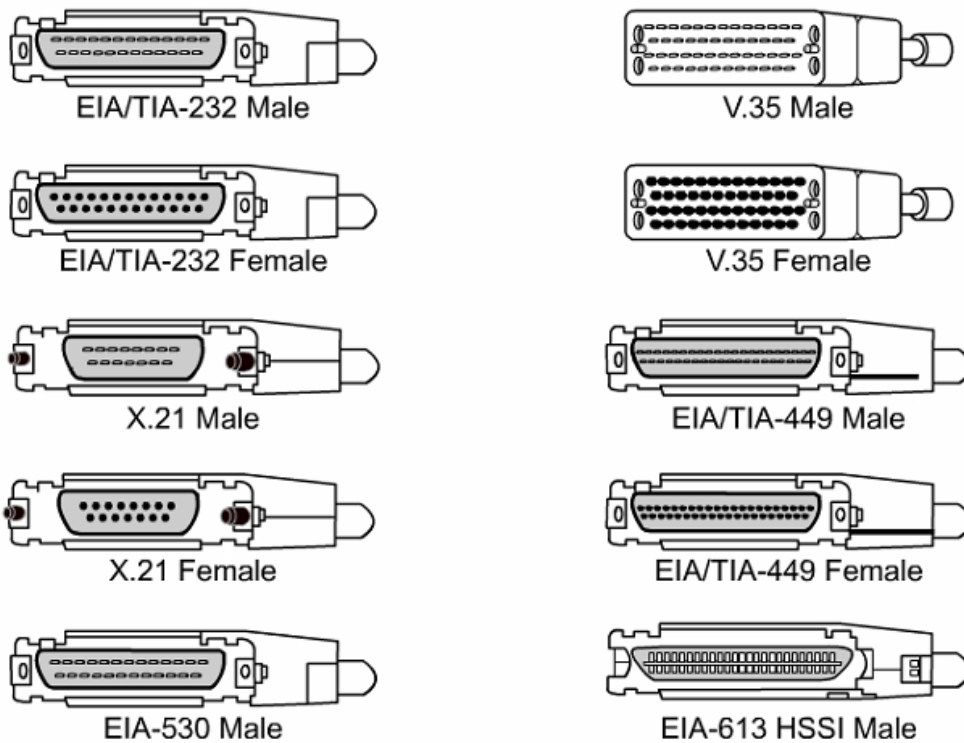
Acronym	Organization
ITU-T (was CCITT)	International Telecommunication Union Telecommunication Standardization Sector, formerly the Consultative Committee for International Telegraph and Telephone
ISO	International Organization for Standardization
IETF	Internet Engineering Task Force
EIA	Electronic Industries Association
TIA	Telecommunications Industries Association

Protokol layer 1 menjelaskan bagaimana menyediakan secara elektrik, mekanis, operasi dan fungsi koneksi yang disediakan oleh service provider. Beberapa standar fisik dan konektornya digambarkan dibawah ini.

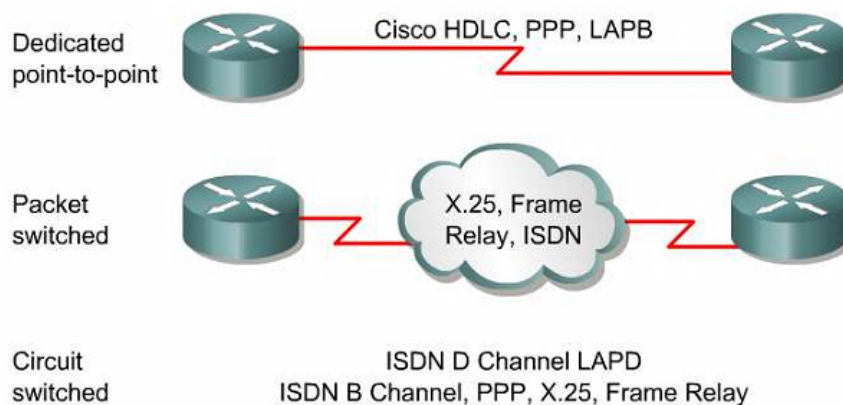
Layer 2

Standard	Description
EIA/TIA-232	Allows signal speeds of up to 64 Kbps on a 25 pin D connector over short distances. It was formerly known as RS-232. The ITU-T V.24 specification is effectively the same.
EIA/TIA-449/530	A faster (up to 2 Mbps) version of EIA/TIA-232. It uses a 36 pin D connector and is capable of longer cable runs. There are several versions. Also known as RS-422 and RS-423.
EIA/TIA-612/613	The High Speed Serial Interface (HSSI), which provides access to services at up to 52 Mbps on a 60 pin D connector.
V.35	An ITU-T standard for synchronous communications between a network access device and a packet network at speeds up to 48 Kbps. It uses a 34 pin rectangular connector.
X.21	An ITU-T standard for synchronous digital communications. It uses a 15 pin D connector.

Konsep Dasar Jaringan WAN



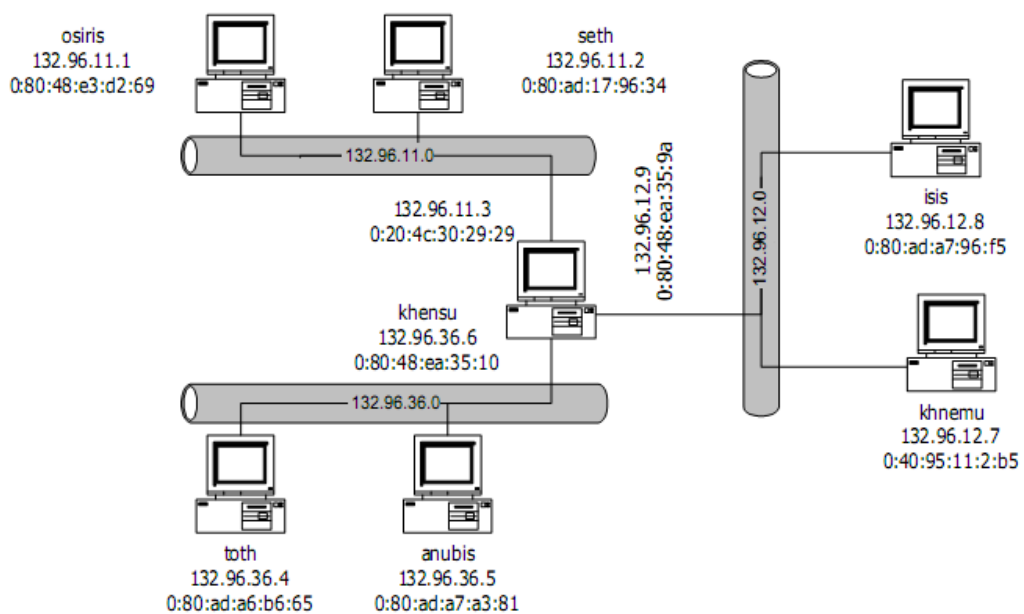
Data link layer menjelaskan bagaimana data dienkapsulasi untuk transmisi ke remote site, dan mekanisme untuk pengiriman yang menghasilkan frame. Ada bermacam-macam teknologi yang digunakan seperti ISDN, Frame Relay atau Asynchronous Transfer Mode (ATM). Protokol ini menggunakan dasar mekanisme framing yang sama, yaitu High-Level Data Link Control (HDLC) atau satu dari beberapa variannya seperti Point to Point Protocol.



4. Dasar-dasar Routing

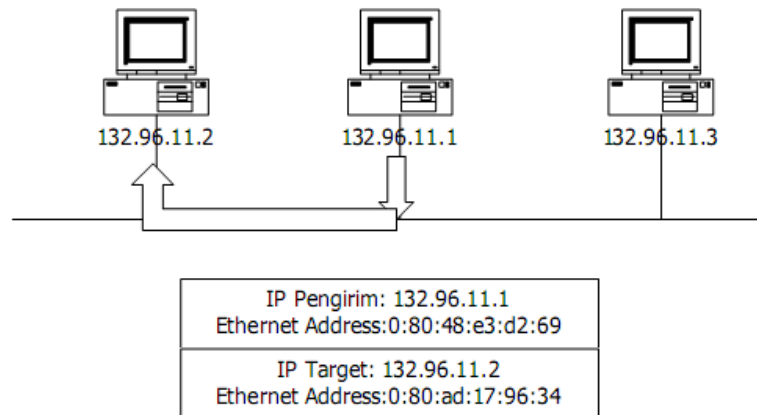
a. Routing Langsung dan Tidak Langsung

Proses pengiriman datagram IP selalu menggunakan tabel routing. Tabel routing berisi informasi yang diperlukan untuk menentukan ke mana datagram harus di kirim. Datagram dapat dikirim langsung ke host tujuan atau harus melalui host lain terlebih dahulu tergantung pada tabel routing.

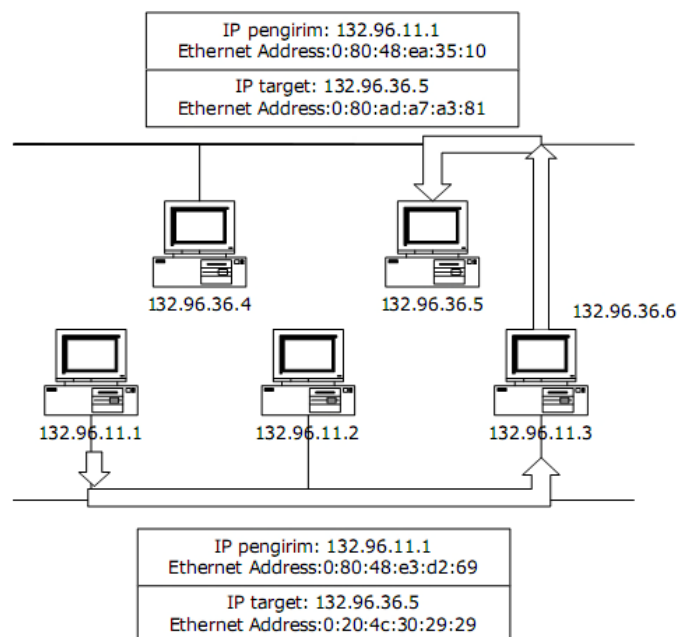


Gambar diatas memperlihatkan jaringan TCP/IP yang menggunakan teknologi Ethernet. Pada jaringan tersebut host osiris mengirimkan data ke host seth, alamat tujuan datagram adalah ip address host seth dan alamat sumber datagram adalah ip address host osiris. Frame yang dikirimkan oleh host osiris juga memiliki alamat tujuan frame MAC Address host Seth dan alamat sumbernya adalah host osiris. Pada saat host osiris mengirimkan frame, host seth membaca bahwa frame tersebut ditujukan kepada alamat ethernetnya. Setelah melepas header frame, host seth kemudian mengetahui bahwa IP address tujuan datagram tersebut juga adalah IP addressnya. Dengan demikian host seth meneruskan datagram ke lapisan transport untuk diproses lebih lanjut. Komunikasi model seperti ini disebut sebagai routing langsung.

Konsep Dasar Jaringan WAN



Pada gambar diatas terlihat bahwa host osiris dan host anubis terletak pada jaringan Ethernet yang berbeda. Kedua jaringan tersebut dihubungkan oleh host khensu. Host khensu memiliki lebih dari satu interface dan dapat melewati datagram dari satu interface ke interface lain (atau bertindak sebagai router). Ketika mengirimkan data ke host anubis, osiris memeriksa tabel routing dan mengetahui bahwa data tersebut harus melewati host khensu terlebih dahulu. Dengan kondisi seperti ini datagram yang dikirim host osiris ke host anubis memiliki alamat tujuan IP Address host anubis dan alamat sumber IP Address host osiris tetapi frame ethernet yang dikirimnya diberi alamat tujuan MAC Address host khensu dan alamat sumber MAC Address host osiris.



Konsep Dasar Jaringan WAN

Ketika host osiris mengirimkan frame ke jaringan, khensu membaca bahwa alamat ethernet yang dituju frame tersebut adalah alamat ethernetnya. Ketika host khensu melepas header frame, diketahui bahwa host yang dituju oleh datagram adalah host anubis. Host khensu kemudian memeriksa tabel routing yang dimilikinya untuk meneruskan datagram tersebut. Dari hasil pemeriksaan tabel routing, host khensu mengetahui bahwa host anubis terletak dalam satu jaringan ethernet dengannya. Dengan demikian datagram tersebut dapat langsung disampaikan oleh host khensu ke host anubis. Pada pengiriman data tersebut, alamat tujuan dan sumber datagram tetap IP Address host anubis dan host osiris tetapi alamat tujuan dan sumber frame Ethernet menjadi MAC Address host anubis dan host khensu. Komunikasi seperti ini disebut sebagai routing tak langsung karena untuk mencapai host tujuan, datagram harus melewati host lain yang bertindak sebagai router.

Pada dua kasus diatas terlihat proses yang terjadi pada lapisan internet ketika mengirimkan dan menerima datagram. Pada saat mengirimkan datagram, host harus memeriksa apakah alamat tujuan datagram terletak pada jaringan yang sama atau tidak. Jika alamat tujuan datagram terletak pada jaringan yang sama, datagram dapat langsung disampaikan. Jika ternyata alamat tujuan datagram tidak terletak pada jaringan yang sama, datagram tersebut harus disampaikan melalui host lain yang bertindak sebagai router. Pada saat menerima datagram host harus memeriksa apakah ia merujuk ke tujuan dari datagram tersebut. Jika memang demikian maka data diteruskan ke lapisan transport. Jika ia bukan tujuan dari datagram tersebut, maka datagram tersebut dibuang. Jika host yang menerima datagram tersebut sebuah router, maka ia meneruskan datagram ke interface yang menuju alamat tujuan datagram.

b. Jenis Konfigurasi Routing

Konfigurasi routing secara umum terdiri dari 3 macam yaitu:

1. Minimal Routing

Dari namanya dapat diketahui bahwa ini adalah konfigurasi yang paling sederhana tapi mutlak diperlukan. Biasanya minimal routing dipasang pada network yang terisolasi dari network lain atau dengan kata lain hanya pemakaian lokal saja .

2. Static Routing

Konfigurasi routing jenis ini biasanya dibangun dalam network yang hanya mempunyai beberapa gateway, umumnya tidak lebih dari 2 atau 3. Static routing dibuat secara manual pada masing-masing gateway. Jenis ini masih memungkinkan untuk jaringan kecil dan stabil. Stabil dalam arti kata jarang down. Jaringan yang tidak stabil yang dipasang static routing dapat membuat kacau seluruh routing, karena tabel routing yang diberikan oleh gateway tidak benar sehingga paket data yang seharusnya tidak bisa diteruskan masih saja dicoba sehingga menghabiskan bandwidth. Terlebih menyusahkan lagi apabila network semakin berkembang. Setiap penambahan sebuah router, maka router yang telah ada sebelumnya harus diberikan tabel routing tambahan secara manual. Jadi jelas, static routing tidak mungkin dipakai untuk jaringan besar, karena butuh effort yang besar untuk mengupdatenya.

1. Dynamic Routing

Dalam sebuah network dimana terdapat jalur routing lebih dari satu rute untuk mencapai tujuan yang sama biasanya menggunakan dynamic routing. Dan juga selain itu network besar yang terdapat lebih dari 3 gateway. Dengan dynamic routing, tinggal menjalankan routing protokol yang dipilih dan biarkan bekerja. Secara otomatis tabel routing yang terbaru akan didapatkan.

Seperti dua sisi uang, dynamic routing selain menguntungkan juga sedikit merugikan. Dynamic routing memerlukan routing protokol untuk membuat tabel routing dan routing protokol ini bisa memakan resource komputer.

c. Routing Protocol

Protokol routing merupakan aturan yang mempertukarkan informasi routing yang nantinya akan membentuk tabel routing sedangkan routing adalah aksi pengiriman-pengiriman paket data berdasarkan tabel routing tadi. Semua routing protokol bertujuan mencari rute tersingkat untuk mencapai tujuan. Dan masing-masing protokol mempunyai cara dan metodenya sendiri-sendiri. Secara garis besar, routing protokol dibagi menjadi Interior Routing Protocol dan Exterior Routing Protocol. Keduanya akan diterangkan sebagai berikut:

1. Interior Routing Protocol

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

- RIP (Routing Information Protocol)

Merupakan protokol routing yang paling umum dijumpai karena biasanya sudah included dalam sebuah sistem operasi, biasanya unix atau novell. RIP memakai metode distance-vector algoritma. Algoritma ini bekerja dengan menambahkan satu angka metrik kepada routing apabila melewati satu gateway. Satu kali data melewati satu gateway maka angka metriknya bertambah satu (atau dengan kata lain naik satu hop). RIP hanya bisa menangani 15 hop, jika lebih maka host tujuan dianggap tidak dapat dijangkau. Oleh karena alasan tadi maka RIP tidak mungkin untuk diterapkan di sebuah AS yang besar. Selain itu RIP juga mempunyai kekurangan dalam hal network masking. Namun kabar baiknya, implementasi RIP tidak terlalu sulit jika dibandingkan dengan OSPF yang akan diterangkan berikut ini.

- OSPF (Open Shortest Path First)

Merupakan protokol routing yang kompleks dan memakan resource komputer. Dengan protokol ini, route dapat dibagi menjadi beberapa jalan. Maksudnya untuk mencapai host tujuan dimungkinkan untuk mencapainya melalui dua atau lebih rute secara paralel. Lebih jauh tentang RIP akan diterangkan lebih lanjut.

2. Exterior Protocol

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

- EGP (Exterior Gateway Protocol)

Protokol ini mengumumkan ke AS lainnya tentang network yang berada di bawahnya. Pengumumannya kira-kira berbunyi: " Kalau hendak pergi ke AS nomor sekian dengan nomor network sekian, maka silahkan melewati saya".

Router utama menerima routing dari router-router AS yang lain tanpa mengevaluasinya. Maksudnya, rute untuk ke sebuah AS bisa jadi lebih dari satu rute dan EGP menerima semuanya tanpa mempertimbangkan rute terbaik.

- BGP (Border Gateway Protocol)

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

c. ARP

Untuk keperluan mapping IP address ke Alamat Ethernet maka di buat protokol ARP (Address Resolution Protocol). Proses mapping ini dilakukan hanya untuk datagram yaang dikirim host karena pada saat inilah host menambahkan header Ethernet pada datagram. Penerjemahan dari IP address ke alamat Ethernet dilakukan dengan melihat sebuah tabel yang disebut sebagai cache ARP, lihat tabel 1. Entri cache ARP berisi IP address host beserta alamat Ethernet untuk host tersebut. Tabel ini diperlukan karena tidak ada hubungan sama sekali antara IP address dengan alamat Ethernet. IP address suatu host bergantung pada IP address jaringan tempat host tersebut berada, sementara alamat Ethernet sebuah card bergantung pada alamat yang diberikan oleh pembuatnya.

Tabel *Cache ARP*


IP address	Alamat Ethernet
132.96.11.1	0:80:48:e3:d2:69
132.96.11.2	0:80:ad:17:96:34
132.96.11.3	0:20:4c:30:29:29

Mekanisme penterjemahan oleh ARP dapat dijelaskan sebagai berikut. Misal suatu host A dengan IP address 132.96.11.1 baru dinyalakan, lihat Gambar 1. Pada saat awal, host ini hanya mengetahui informasi mengenai interface-nya sendiri, yaitu IP address, alamat network, alamat

Konsep Dasar Jaringan WAN

broadcast dan alamat ethernet. Dari informasi awal ini, host A tidak mengetahui alamat ethernet host lain yang terletak satu network dengannya (cache ARP hanya berisi satu entri, yaitu host A). Jika host memiliki route default, maka entri yang pertama kali dicari oleh ARP adalah router default tersebut.

Misalkan terdapat datagram IP dari host A yang ditujukan kepada host B yang memiliki IP 132.96.11.2 (host B ini terletak satu subnet dengan host A). Saat ini yang diketahui oleh host A adalah IP address host B tetapi alamat ethernet B belum diketahui.

	Alamat IP	Alamat Ethernet
132.96.11.1	132.96.11.1	0:80:48:e3:d2:69

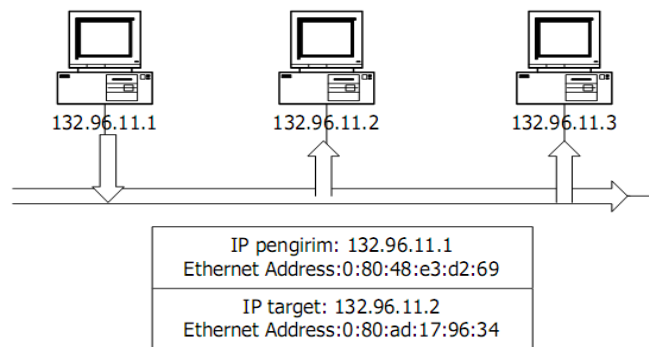
Agar dapat mengirimkan datagram ke host B, host A perlu mengisi cache ARP dengan entri host B. Karena cache ARP tidak dapat digunakan untuk menerjemahkan IP address host BB menjadi alamat Ethernet, maka host A harus melakukan dua hal yaitu:

Mengirimkan paket ARP request pada seluruh host di network menggunakan alamat broadcast Ethernet (FF:FF:FF:FF:FF:FF) untuk meminta jawaban ARP dari host B, lihat gambar 2.

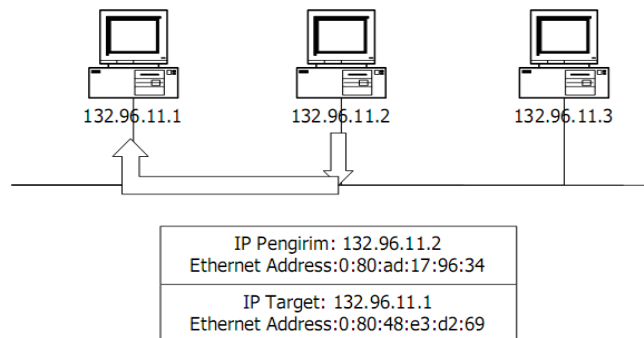
Menempatkan datagram IP yang hendak dikirim dalam antrian.

Paket ARP request yang dikirim host A kira-kira berbunyi "Jika IP address-mu adalah 132.96.11.2, mohon beritahu alamat Ethernet- mu". Karena paket ARP request dikirim ke alamat broadcast Ethernet, setiap interface Ethernet komputer yang ada dalam satu subnet (jaringan) dapat mendengarnya. Setiap host dalam jaringan tersebut kemudian memeriksa apakah IP addressnya sama dengan IP address yang diminta oleh host A.

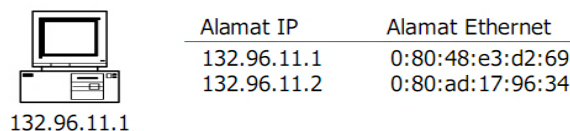
Konsep Dasar Jaringan WAN



Host B yang mengetahui bahwa yang diminta oleh host A adalah IP address yang dimilikinya langsung memberikan jawaban dengan mengirimkan paket ARP response langsung ke alamat ethernet pengirim (host A), seperti terlihat pada gambar 3. Paket ARP request tersebut kira-kira berbunyi "IP address 132.96.11.2 adalah milik saya, sekarang saya berikan alamat ethernet saya".



Paket ARP request dari host B tersebut diterima oleh host A dan host A kemudian menambahkan entri IP addresss host B beserta alamat Ethernet-nya ke dalam cache ARP, lihat gambar 4.



Saat ini host A telah memiliki entri untuk host B di tabel cache ARP, dengan demikian datagram IP yang semula dimasukkan ke dalam antrian dapat diberi header Ethernet dan dikirim ke hostB.

Secara ringkas proses ARP adalah:

1. Host mengirimkan paket ARP request dengan alamat broadcast Etehrnet.
2. Datagram IP yang dikirim dimasukkan ke dalam antrian.
3. Paket ARP respon diterima host dan host mengisi tabel ARP dengan entri baru.
4. Datagram IP yang terletak dalam antrian diberi header Ethernet.
5. Host mengirimkan frame Ethernet ke jaringan.

Setiap data ARP yang diperoleh disimpan dalam tabel cache ARP dan cache ini diberi umur. Setiap umur entri tersebut terlampaui, entri ARP dihapus dari tabel dan untuk mengisi tabel. Jika host akan mengirimkan datagram ke host yang sudah dihapus dari cache ARP, host kembali perlu melakukan langkah-langkah diatas. Dengan cara ini dimungkinkan terjadinya perubahan isi cache ARP yang dapat menunjukkan dinamika jaringan. Jika sebuah host di jaringan dimatikan, maka selang beberapa saat kemudian entri ARP untuk host tersebut dihapus karena kadaluarsa. Jika card ethernetnya diganti, maka beberapa saat kemudian entri ARP host berubah dengan informasi alamat ethernet yang baru.

5. Enkapsulasi HDLC (High-Level Data Link Control)

Pada umumnya, komunikasi serial berdasarkan protokol character oriented. Protokol bit oriented lebih efisien tetapi mereka juga proprietary. Pada tahun 1979, ISO menyetujui HDLC sebagai standar untuk protokol bit oriented pada data link layer yang mengenkapsulasi data pada synchronous serial data link. Sejak 1981, ITU-T telah mengembangkan berbagai seri dari pengembangan HDLC. Beberapa contoh dari protokol tersebut adalah:

- Link Access Procedure, Balanced (LAPB) untuk X.25
- Link Access Procedure on the D channel (LAPD) untuk ISDN
- Link Access Procedure for Modem (LAPM) dan PPP untuk modem
- Link Access for Frame Relay (LAPF) untuk Frame Relay.

HDLC menggunakan transmisi serial synchronous yang menyediakan komunikasi bebas error diantara 2 titik. HDLC menjelaskan struktur frame Layer 2 yang memperbolehkan flow control

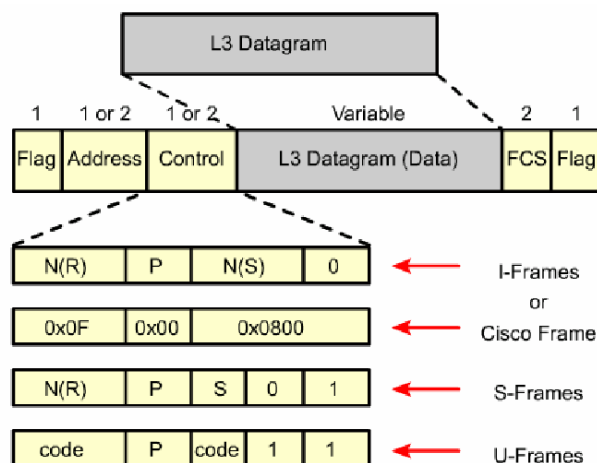
Konsep Dasar Jaringan WAN

dan error control menggunakan acknowledgment dan windowing scheme. Setiap frame memiliki format yang sama, baik frame data atau control. Pada router merk tertentu, HDLC yang digunakan merupakan proprietary sendiri. HDLC menggunakan sebuah field proprietary. Field ini memungkinkan beberapa network layer protocol untuk berbagi jalur serial yang sama. HDLC merupakan default Layer 2 protokol untuk interface serial.

HDLC mempunyai tiga tipe frame, dimana setiap frame memiliki format yang berbeda yaitu:

- Information frame (I-frames), membawa data untuk dikirimkan. Menambahkan flow dan error control, dimana data mungkin minta dikirimkan ulang (piggyback).
- Supervisory frame (S-frames), menyediakan mekanisme request dan respond ketika piggybacking tidak digunakan.
- Unnumbered frames (U-frames), menyediakan tambahan fungsi pengontrolan jalur seperti setup koneksi dll.

Satu atau 2 bit pertama dari field control mengidentifikasi tipe frame. Pada field control dari I-frames, send-sequence number menunjuk pada nomor frame yang dikirimkan selanjutnya. Receive- sequence number menunjukkan nomer dari frame yang diterima selanjutnya. Kedua pengirim dan penerima memelihara send dan receive sequence number.

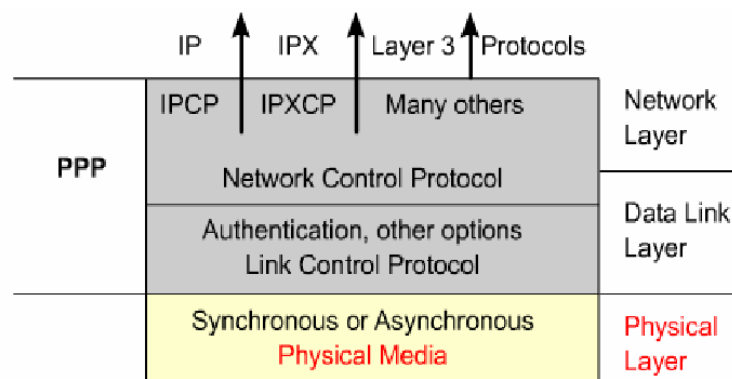


HDLC dapat digunakan untuk protokol point-to-point yang dapat digunakan pada leased line diantara dua perangkat dengan merk sejenis. Ketika berkomunikasi dengan perangkat dengan merk yang berbera maka dapat menggunakan PPP.

6. Enkapsulasi PPP (Point to Point Protocol)

PPP menggunakan arsitektur berlapis. Arsitektur berlapis adalah model logik, desain atau cetak biru yang membantu komunikasi diantara lapisan interkoneksi. OSI model adalah arsitektur berlapis yang digunakan pada jaringan. PPP menyediakan metode untuk mengenkapsulasi multi-protocol datagram melalui jalur point-to-point dan menggunakan lapisan data link untuk mengetes koneksi. PPP terdiri dari dua sub-protocol yaitu:

- Link Control Protocol (LCP), digunakan untuk membangun jalur point-to-point
- Network Control Protocol (NCP), digunakan untuk mengkonfigurasi berbagai protokol network layer.



PPP dapat mengkonfigurasi berbagai tipe interface fisik yaitu:

- Asynchronous serial
- Synchronous serial
- High-Speed Serial Interface (HSSI)
- ISDN

PPP menggunakan LCP untuk menegosiasikan dan pilihan kontrol setup pada data link WAN. PPP menggunakan komponen NCP untuk enkapsulasi dan pilihan negosiasi untuk berbagai protokol network layer. LCP berada di atas physical layer dan digunakan untuk membangun, mengkonfigurasi dan mengetes koneksi data link. PPP juga menggunakan LCP untuk secara otomatis menyetujui pilihan format enkapsulasi seperti dibawah ini:

Konsep Dasar Jaringan WAN

- Authentication, pilihan otentikasi membutuhkan sisi pemanggil untuk memasukkan informasi untuk membantu terpanggil

mendapatkan ijin sesuai setting network administrator jaringan terpanggil. Ada dua pilihan otentikasi yaitu Password Authentication Protocol (PAP) dan Challenge Handshake Authentication Protocol (CHAP).

- Compression, pilihan kompresi meningkatkan efektifitas throughput pada koneksi PPP dengan mengurangi sejumlah data pada frame yang harus melalui jalur. Protokol akan medekompres frame pada tujuan. Dua protokol kompresi yang tersedia adalah Stacker dan Predictor.

- Error detection, mekanisme error detection dengan PPP memungkinkan proses untuk mengidentifikasi kondisi.

- Multilink, CISCO IOS Release 11.1 dan sesudahnya mendukung PPP multilink. Ini alternatif yang menyediakan load balance melalui interface router dimana PPP digunakan.

- PPP Callback, untuk penangan keamanan di masa yang akan datang. Dengan pilihan LCP, sebuah router dapat berperilaku sebagai client callback atau sebagai server callback. Client melakukan inisialisasi call, meminta agar bias di callback, dan mengakhiri callback. Router callback menjawab inisialisasi call dan melakukan panggilan jawaban ke client berdasarkan konfigurasinya.

LCP juga akan melakukan:

- Menangani berbagai batas dari ukuran paket

- Mendeteksi kesalahan konfigurasi yang umum

- Mengakhiri jalur

- Memastikan ketika jalur berfungsi baik atau ketika sedang rusak PPP mengijinkan berbagai protokol network layer untuk beroperasi pada jalur komunikasi yang sama. Untuk setiap protokol network layer yang digunakan, disediakan NCP yang berbeda. Sebagai contoh, Internet Protocol (IP) menggunakan IP Control Protocol (IPCP), dan Internetwork Packet Exchange (IPX) menggunakan Novell IPX Control Protocol (IPXCP). NCP termasuk field-field functional yang berisi kode standar untuk mengidentifikasi protokol network layer yang digunakan.

Konsep Dasar Jaringan WAN

Field pada frame PPP adalah sebagai berikut:

- Flag, mengidentifikasi awal atau akhir frame dan konsisten berisi urutan biner 01111110.
- Address, berisi broadcast address standar, dimana urutan biner 11111111. PPP tidak memberikan alamat individu untuk setiap station.
- Control, 1 byte yang berisi urutan biner 00000011, dimana panggilan untuk transmisi data user tidak berurut.
- Protocol, 2 byte yang mengidentifikasi protokol yang di enkapsulasi data field data pada frame.
- Data, 0 atau lebih byte yang berisi datagram untuk protokol yang dispesifikasikan pada field protocol. Akhir field data dapat ditemukan dengan lokasi dari urutan flag penutup. Maksimum panjang field default adalah 1.500 byte.
- FCS, normalnya 16 bit atau 2 byte yang menunjukkan karakter extra yang ditambahkan pada frame untuk fungsi error control.

Value (in hex)	Protocol Name
8021	Internet Protocol Control Protocol
8023	OSI Network Layer Control Protocol
8029	Appletalk Control Protocol
802b	Novell IPX Control Protocol
c021	Link Control Protocol
c023	Password Authentication Protocol
c223	Challenge Handshake Authentication Protocol

Membangun sesi PPP melalui tiga fase. Fase tersebut adalah pembangunan jalur, autentikasi dan fase network layer. Frame LCP digunakan untuk memastikan kerja setiap LCP fase. Tiga kelas dari LCP frame yang digunakan untuk PPP adalah:

- Frame Pembangunan Jalur digunakan untuk membangun dan mengkonfigurasi jalur.
- Frame Terminasi Jalur digunakan untuk mengakhiri jalur.
- Frame Pemeliharaan Jalur digunakan untuk mengatur dan melakukan debug terhadap jalur.

Tiga sesi pembangunan PPP adalah:

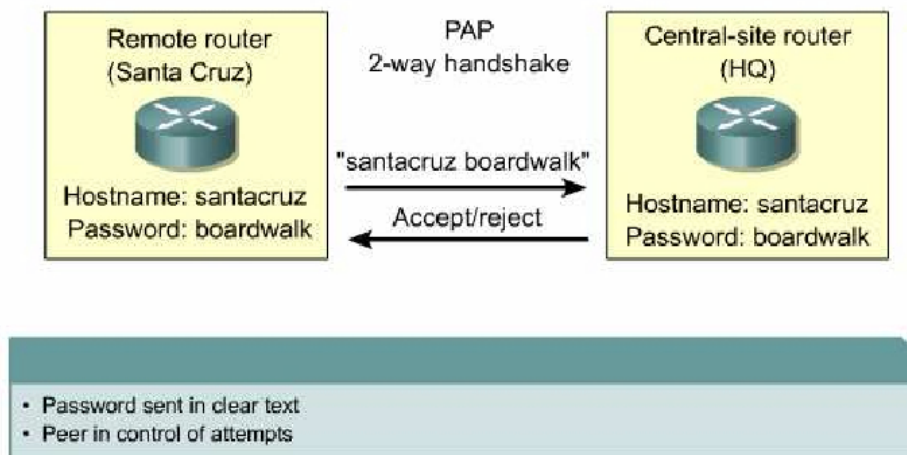
- Fase Pembangunan Jalur, pada fase ini perangkat PPP mengirim LCP frame untuk mengkonfigurasi dan mengetes jalur data. Frame LCP berisi configuration option field yang memungkinkan perangkat untuk menegosiasikan pilihan yang digunakan seperti maksimum transmission unit (MTU), kompresi dari beberapa field PP dan protokol otentikasi field. Jika sebuah pilihan konfigurasi tidak termasuk dalam paket LCP, nilai default untuk konfigurasi tersebut yang digunakan. Sebelum beberapa paket network layer dapat dikirimkan, LCP pertama-tama harus membuka koneksi dan menegosiasikan parameter konfigurasi. Fase ini selesai ketika sebuah frame configuration acknowledgment telah dikirim dan diterima.
- Fase Authentication (boleh ada boleh tidak), setelah jalur dibangun dan protokol otentikasi diputuskan, maka melakukan proses otentikasi. Otentikasi jika digunakan mengambil tempat sebelum memasuki fase protokol network layer. Sebagai bagian dari fase ini, LCP juga memperbolehkan sebuah pilihan untuk memastikan kualitas jalur. Link ini di tes untuk memastikan kualitas jalur apakah cukup baik untuk membawa data protokol network layer.
- Fase Protokol Network Layer, pada fase ini perangkat PPP mengirim paket NCP untuk memilih dan mengkonfigurasi satu atau lebih protokol network layer seperti IP. Setiap protokol network layer yang telah dikonfigurasi, satu paket dari setiap network layer dapat dikirimkan melalui jalur. Jika LCP menutup jalur, hal tersebut diinformasikan ke protokol network layer sehingga mampu melakukan aksi yang sesuai. Perintah show interface menunjukkan kondisi LCP dan NCP dalam konfigurasi PPP.

Jalur PPP meninggalkan konfigurasi untuk komunikasi jalur sampai frame LCP atau NCP menutup jalur atau sampai timer inactivity habis untuk mengintervensi pengguna. Pilihan otentikasi membutuhkan sisi pemanggil dari jalur memasuki informasi otentikasi. Hal ini membantu untuk memastikan pengguna memiliki ijin dari network administrator untuk membuat panggilan. Ketika mengkonfigurasi otentikasi PPP, network administrator dapat memilih Password Authentication Protocol (PAP) atau Challenge Handshake Authentication Protocol (CHAP). Umumnya CHAP lebih sering digunakan.

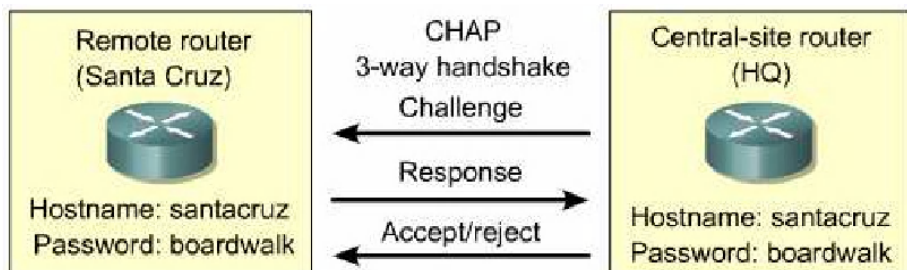
PAP menyediakan metode sederhana untuk meremote node untuk mengidentifikasi pembangunan, menggunakan two way handshake. Setelah jalur PPP dibangun, username/password secara terus menerus dikirim dari node tujuan melalui jalur sampai

Konsep Dasar Jaringan WAN

otentikasi telah disetujui atau koneksi diakhiri. PAP bukan merupakan protokol yang kuat. Password dikirim melalui jalur dengan bentuk clear text dan tidak ada proteksi. Remote node yang akan mengontrol frekuensi dan waktu dari masuknya login.



CHAP digunakan pada startup jalur dan secara periodic di verifikasi untuk mengidentifikasi remote node menggunakan three-way handshake. CHAP menampilkan pembangunan jalur dan diulang selama jalur dibangun.



Uses a secret password known only to authenticator and peer.

Setelah fase pembangunan jalur PPP selesai, router local mengirim sebuah pesan "challenge" ke remote node. Remote node merespon dengan nilai yang dikalkulasi menggunakan fungsi one-way hash, dimana umumnya Message Digest 5 (MD5). Responsenya berdasarkan password dan pesan challenge. Lokal router akan mengecek respon dengan kalkulasi miliknya sendiri dengan nilai hash yang diharapkan. Jika nilai sesuai, otentikasi di setujui, sebaliknya koneksinya akan segera diakhiri.

Konsep Dasar Jaringan WAN

CHAP menyediakan proteksi melawan serangan playback melalui penggunaan berbagai nilai challenge yang unik dan tidak dapat diprediksi. Jika challenge unik dan acak, maka nilai hasil hash juga akan unik dan acak. Penggunaan challenge yang diulang-ulang akan meningkatkan waktu untuk sebuah serangan. Router local atau server otentikasi pihak ketiga yang akan mengontrol frekuensi dan waktu challenge.

Rangkuman Konsep Dasar Jaringan WAN:

1. JARINGAN komputer adalah kumpulan komputer, printer dan peralatan lainnya yang terhubung dalam satu kesatuan. Informasi dan data bergerak melalui kabel-kabel atau tanpa kabel sehingga memungkinkan pengguna jaringan komputer dapat saling bertukar dokumen dan data, mencetak pada printer yang sama dan bersama-sama menggunakan hardware/software yang terhubung dalam jaringan.
2. Ada lima jenis jaringan komputer, Local Area Network (LAN), Metropolitan Area Network (MAN), Wide Area Network (WAN), Intranet dan Internet.
3. Perangkat yang meletakkan data ke local loop disebut DCE (Data Circuit-terminating Equipment). Perangkat pelanggan yang melewati data ke DCE disebut dengan DTE (Data Terminal Equipment).
4. Perangkat WAN adalah Router, CSU/DSU, Modem dan Communication Server.
5. Ada dua jenis routing yaitu routing langsung dan tidak langsung.
6. Ada 3 jenis konfigurasi routing yaitu minimal routing, static routing dan dynamic routing.
7. Routing Protocol ada 2 jenis yaitu Interior Routing Protocol dan Exterior Routing Protocol.

MENGINSTALASI PERANGKAT KERAS WIDE AREA NETWORK

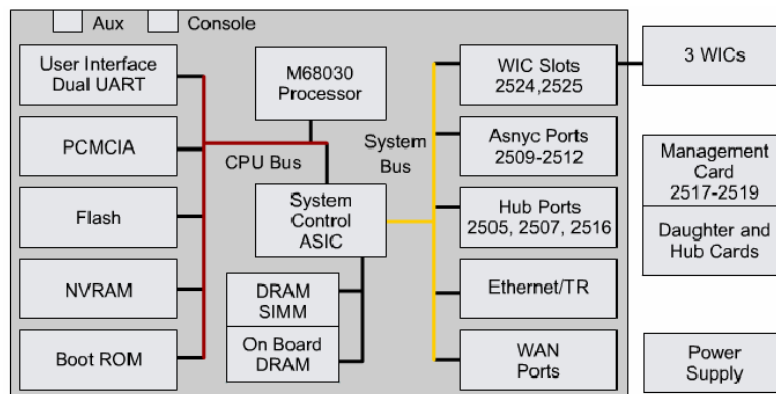
Tujuan Kegiatan Pemelajaran

Setelah mempelajari kegiatan belajar ini peserta diklat mampu menjelaskan instalasi perangkat keras Wide Area Network.

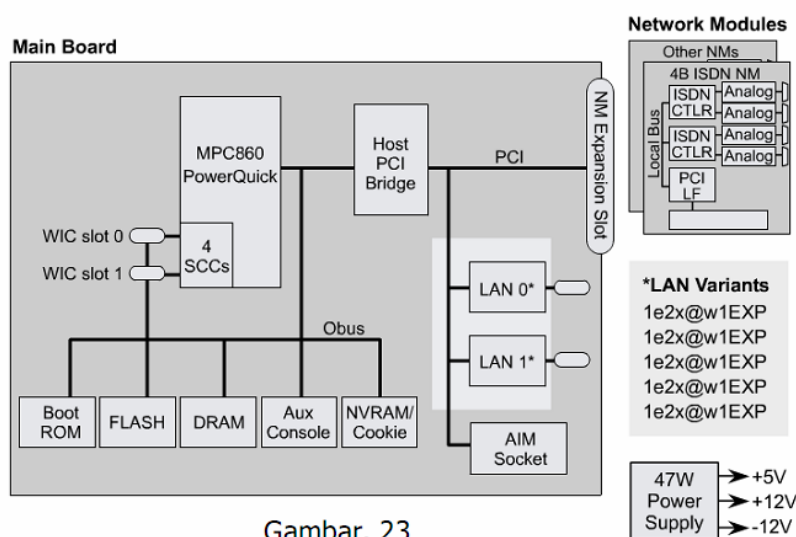
Uraian materi

1. Router

Sebenarnya tidak ada arsitektur yang eksak dari sebuah router karena berbeda-beda tergantung merek dan jenisnya. Di bawah ini adalah gambar arsitektur router dari merek CISCO.



Gambar. 22



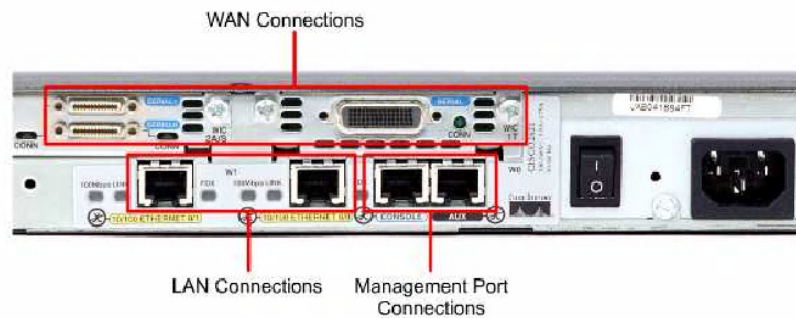
Gambar. 23

Komponen-komponen dari Router adalah:

- a. CPU, Central Processing Unit mengeksekusi instruksi pada Operating System. Fungsi yang lain adalah inisialisasi sistem, fungsi routing dan mengontrol network interface. Router yang besar memiliki beberapa CPU.
- b. RAM, Random Access Memory digunakan untuk informasi routing table, fast switching cache, running configuration dan packet queue. RAM biasanya dibagi dua secara logik yaitu memori processor utama dan memory shared input/output (I/O). Memory shared I/O adalah berbagi antara berbagai interface I/O untuk menyimpan paket secara sementara. Isi RAM akan hilang begitu power dari Router dimatikan.
- c. Flash, digunakan untuk menyimpan keseluruhan IOS (Internetworking Operating System) software image. Router umumnya mencari operating system pada flash. IOS dapat diupgrade dengan mengisi IOS baru pada flash. IOS mungkin berbentuk compressed atau uncompressed.
- d. NVRAM, Nonvolatile Random Access Memory (NVRAM) digunakan untuk menyimpan startup configuration. Di beberapa perangkat NVRAM diimplementasikan menggunakan EEPROM yang terpisah dari perangkat tersebut.
- e. Bus, kebanyakan router berisi sebuah system bus dan CPU bus. System bus digunakan untuk komunikasi diantara CPU dan interface. System bus mengirimkan data dari dan ke interface. CPU bus digunakan oleh CPU untuk mengakses komponen dari media penyimpan router.
- f. ROM, Read Only Memory digunakan untuk menyimpan permanen startup diagnostic code (ROM Monitor). Tugas utama untuk ROM adalah diagnosa hardware selama router melakukan bootup dan memindahkan software IOS dari Flash ke RAM.
- g. Interface adalah koneksi router keluar. Ada tiga tipe interface yaitu Local Area Network (LAN), Wide Area Network (WAN) dan Management. Interface LAN biasanya berupa salah satu dari jenis Ethernet atau Token Ring. Interface WAN termasuk serial, ISDN dan integrated Channel Service Unit (CSU). Management port berisi port Console dan AUX adalah port serial yang digunakan untuk menghubungkan router dengan administrator. Port ini bukan merupakan

port jaringan. Port ini menggunakan aplikasi tertentu yang dijalankan pada sebuah komputer yang dihubungkan melalui port komunikasi pada komputer atau menggunakan modem.

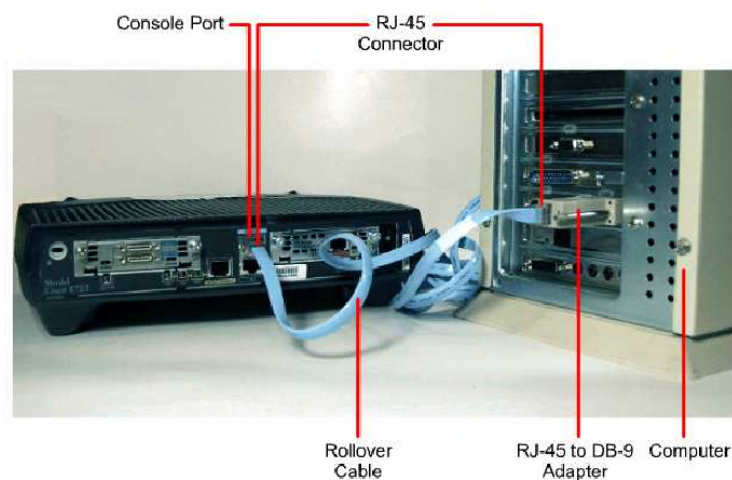
h. Power Supply, menyediakan power yang dibutuhkan untuk mengoperasikan komponen internal.



Gambar. 24

2. Koneksi Komputer atau Terminal Console ke Router

Port Console atau AUX adalah port manajemen. Port tersebut adalah port serial asynchronous yang tidak didesain sebagai port jaringan. Satu dari kedua port tersebut dibutuhkan untuk melakukan konfigurasi router. Port Console dianjurkan untuk konfigurasi awal karena tidak semua router mempunyai port AUX.



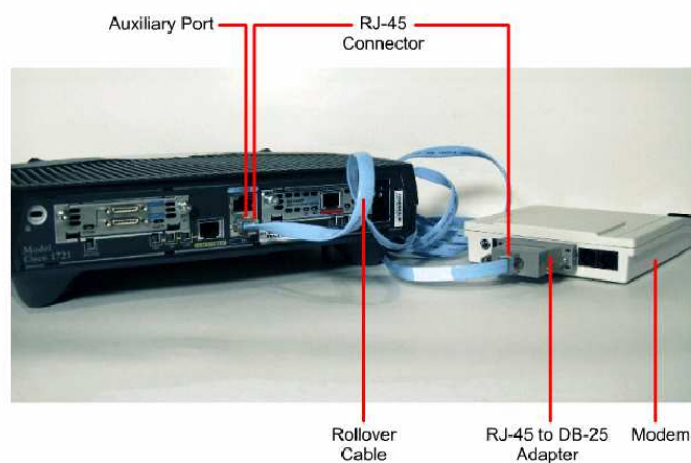
Gambar. 25

Menginstalasi Perangkat Keras WAN

Ketika router pertama kali dijalankan, belum ada parameter jaringan yang dimasukkan. Oleh karena itu router tidak dapat berkomunikasi satu sama lain dengan perangkat jaringan lainnya. Untuk menyiapkan konfigurasi awal pasanglah pada komputer atau terminal RS-232 ASCII ke port console pada router. Kemudian masukkan perintah konfigurasi kedalamnya.

Satu kali konfigurasi tersimpan pada router maka router sudah dapat berkomunikasi dengan perangkat lainnya. Gunakan komputer atau terminal tersebut untuk melakukan perbaikan atau monitoring jaringan. Router juga dapat dikonfigurasi dari jarak jauh dengan melakukan koneksi melalui modem yang dihubungkan ke port Auxiliary. Kemudian modem dihubungkan ke jalur telepon. Administrator dapat melakukan koneksi melalui komputer yang terhubung ke modem menuju router tersebut.

Kemudian konfigurasi software terminal emulation (contohnya Hyperterminal) pada PC untuk: - Port serial (com) yang sesuai. - 9600 baud - 8 data bits - No Parity - 1 stop bit - No flow control



Gambar. 26

Kemudian konfigurasi software terminal emulation (contohnya Hyperterminal) pada PC untuk: - Port serial (com) yang sesuai. - 9600 baud - 8 data bits - No Parity - 1 stop bit - No flow control

3. Koneksi ke Interface LAN

Pada jaringan LAN biasanya menggunakan interface Ethernet atau Fast Ethernet. Interface Ethernet tersebut dihubungkan ke switch menggunakan kabel straight through. Jika langsung ke komputer dapat menggunakan kabel cross over.

4. WAN Physical Layer

Implementasi Physical Layer berbeda-beda tergantung pada layanan, kecepatan dan tipe dari layanan itu sendiri. Koneksi serial digunakan untuk mendukung layanan WAN seperti dedicated leased line yang menjalankan Point to Point Protocol (PPP) atau Frame Relay. Kecepatan koneksi tersebut berkisar dari 2400 bps sampai dengan layanan T1 pada kecepatan 1,544 Mbps dan layanan E1 pada kecepatan 2,048 Mbps.

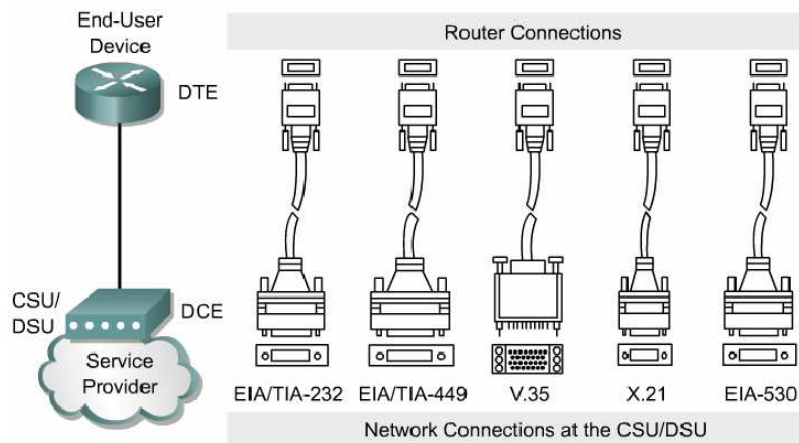
Cisco HDLC	PPP	Frame Relay	ISDN BRI (with PPP)	DSL Modem	Cable Modem
EIA/TIA-232 EIA/TIA-449 X.21 V.24 V.35 High Speed Serial Interface (HSSI)			RJ-45 Note: ISDN BRI cable pinouts are different than the pinouts for Ethernet	RJ-11 Note: Works over telephone line	BNC Note: Works over Cable TV line

Gambar. 27

ISDN menawarkan koneksi dial-on-demand atau layanan backup menggunakan dialup. Pada ISDN Basic Rate Interface (BRI) adalah gabungan dua buah 64 kbps bearer channel (B channel) untuk data dan satu delta channel (D channel) pada kecepatan 16 kbps yang digunakan untuk persinyalan dan tugas manajemen jalur lainnya. PPP biasanya digunakan untuk membawa data melalui B channel. Dengan meningkatnya kebutuhan layanan broadband kecepatan tinggi untuk perumahan, Digital Subscriber Line (DSL) dan kabel model menjadi lebih populer. Untuk contoh, pelanggan DSL rumah bisa mendapatkan kecepatan T1/E1 melalui jalur telepon yang ada. Layanan kabel modem menggunakan kabel televisi coaxial yang ada. Jalur kabel coaxial menyediakan koneksi kecepatan tinggi yang menyamai bahkan melebihi DSL.

5. WAN Serial

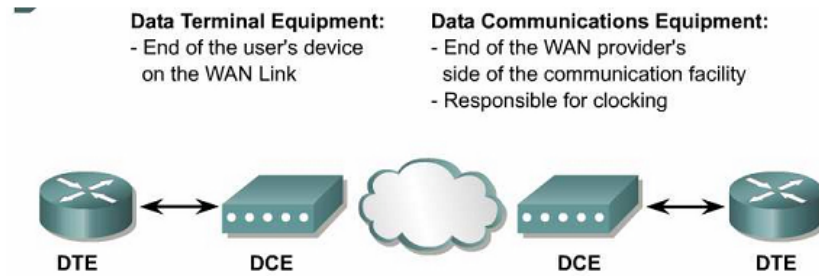
Untuk komunikasi jarak jauh, WAN menggunakan transmisi serial. Ini adalah proses dimana bit dari data dikirimkan melalui satu channel. Proses ini menyediakan komunikasi jarak jauh yang lebih reliabel dan menggunakan spesifikasi elektromagnetik atau range frekuensi optikal yang khusus.



Gambar. 28

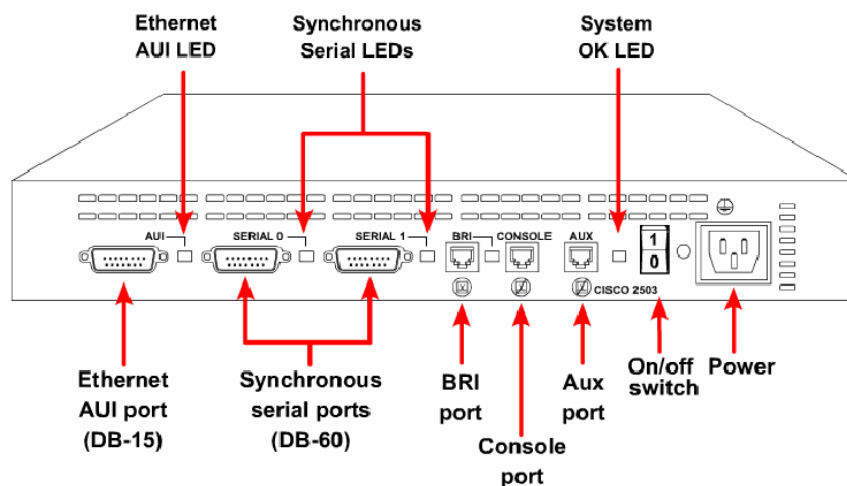
Router bertanggung jawab untuk meroutekan paket data dari sumber ke tujuan didalam LAN dan menyediakan koneksi ke WAN. Sebagai tambahan untuk menentukan tipe kabel, diperlukan untuk memastikan apakah kabel DTE atau kabel DCE yang dibutuhkan. DTE adalah endpoint dari perangkat user pada jalur WAN. DCE biasanya titik yang bertanggung jawab untuk mengirimkan data menuju ke tangan service provider.

Jika koneksi dibuat langsung ke penyedia layanan, atau ke perangkat yang menyediakan sinyal clocking seperti CSU/DSU, router akan menjadi perangkat DTE dan menggunakan kabel DTE. Bagaimanapun, adakalanya router dibutuhkan untuk menyediakan kecepatan clock dan router tersebut menggunakan kabel DCE.



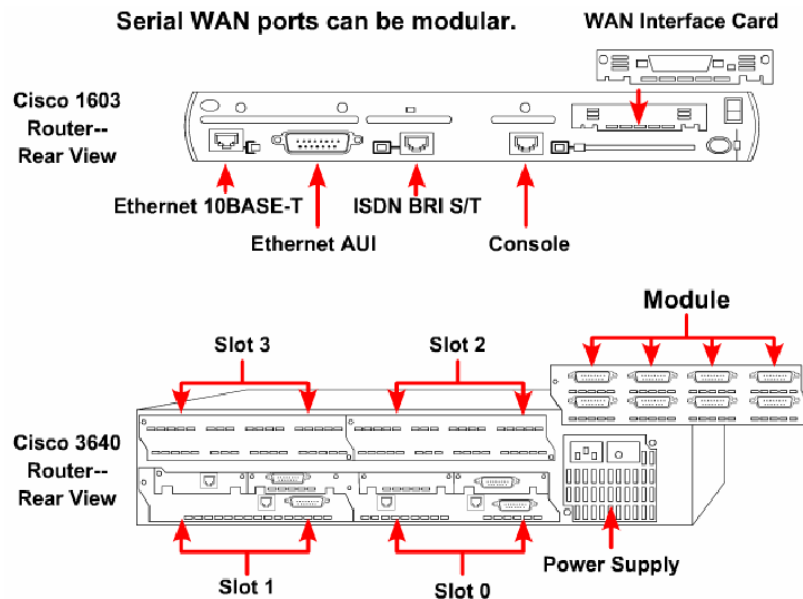
Gambar. 29

Pada sisi router juga dibutuhkan port yang sesuai dengan tipe kabel dan konektor yang digunakan. Port tersebut bisa berupa port yang tetap atau modular. Tipe port yang digunakan akan mempengaruhi sintaks yang digunakan untuk mengkonfigurasi router. Interface pada port serial yang tetap akan dilabeli dengan tipe port dan nomor port.



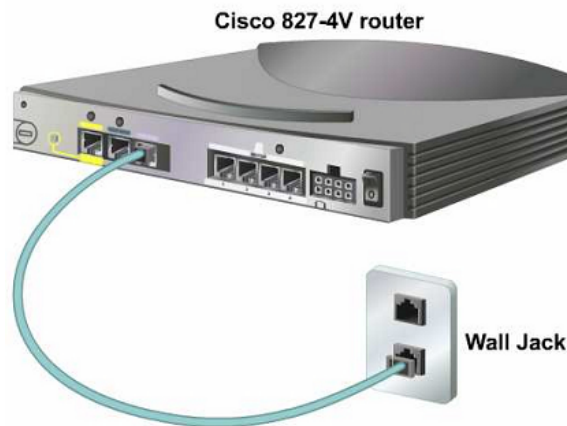
Gambar. 30

Interface pada router dengan port serial modular dilabeli untuk tipe port, slot dan lokasi dari modul. Untuk mengkonfigurasi port pada card modular, dibutuhkan untuk mengspesifikasi interface menggunakan sintaks "tipe port nomor slot/nomor port".



Gambar. 31

- Untuk koneksi ke ADSL dibutuhkan interface Asymmetric Digital Subscriber Liner (ADSL). Untuk menghubungkan jalur ADSL ke port pada router, lakukan langkah-langkah sebagai berikut:
- koneksikan kabel telepon ke port ADSL pada router
 - koneksikan ujung yang lain pada jack telepon.

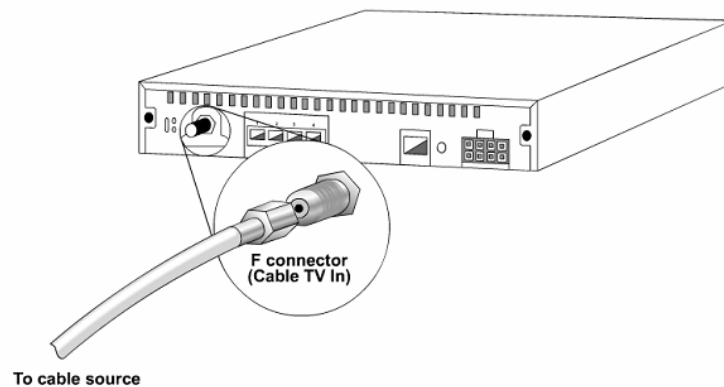


Gambar. 32

Untuk menghubungkan router ke layanan DSL, gunakan kabel telepon dengan jack RJ-11. DSL bekerja melalui standar line telepon menggunakan pin 3 dan 4 pada standar konektor RJ-11. Untuk menghubungkan router ke layanan kabel modem diperlukan interface khusus yang

memiliki konektor F untuk kabel coaxial. Kabel coaxial dan konektor BNC digunakan untuk menghubungkan router dan layanan kabel modem. Lakukan langkah–langkah dibawah ini untuk menghubungkan router ke layanan kabel modem:

- Pastikan router tidak terhubung ke power.
- Carilah kabel coaxial RF pada wall outlet untuk TV kabel.
- Instal cable splitter/directional coupler, jika dibutuhkan, untuk memisahkan sinyal untuk TV dan untuk komputer. Jika dibutuhkan, install juga high-pass filter untuk mencegah interferensi antara siTV dan komputer.
- Hubungkan kabel coaxial ke konektor F pada router. Kencangkonektor dengan memutar searah jarum jam.



Gambar. 33

MENGATUR PERANGKAT MENGGUNAKAN SOFTWARE

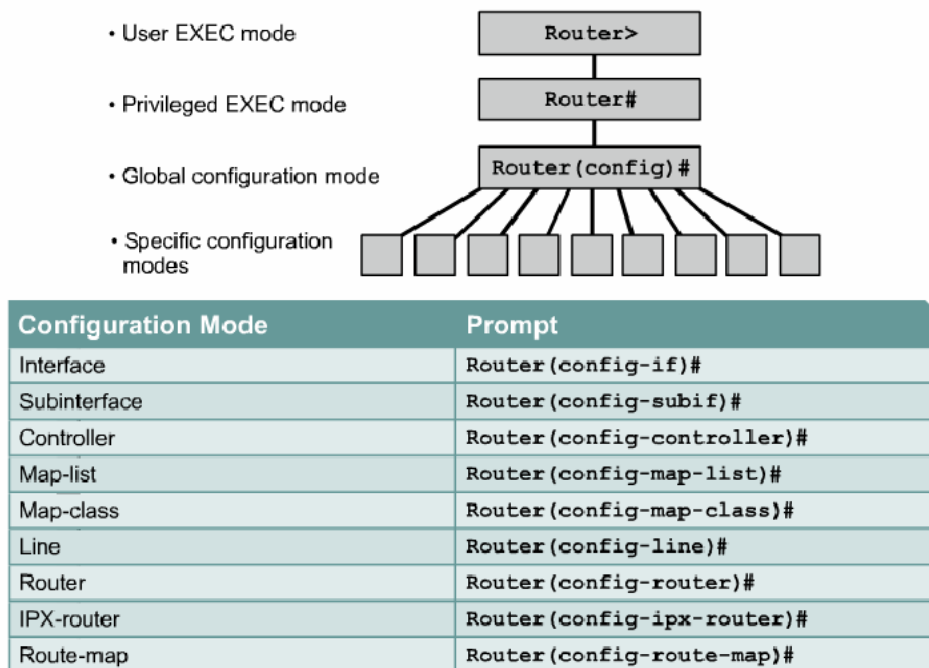
Tujuan Pembelajaran

Setelah mempelajari kegiatan belajar ini peserta diklat mampu menjelaskan pengaturan perangkat menggunakan software.

Uraian materi

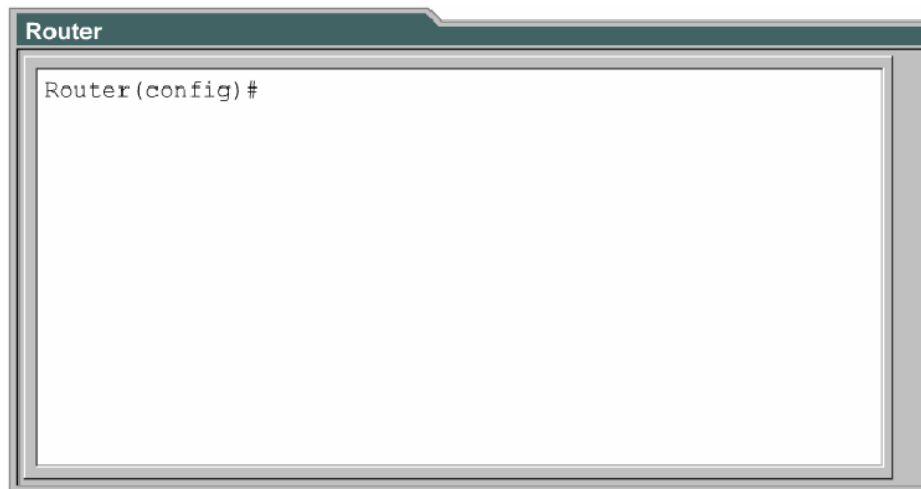
1. CLI Command Mode

CLI (Command-Line interface) adalah suatu interface dari user ke router menggunakan perintah berbasis teks. CLI menggunakan struktur berhirarki. Struktur ini membutuhkan user untuk memasuki suatu mode tertentu untuk menjalankan suatu perintah. Perintah-perintah dalam CLI hanya berlaku untuk satu mode saja, sehingga apabila user tidak dalam kondisi mode tersebut maka user tidak dapat memberikan perintah tersebut ke router.



Gambar. 34

Administrator memberikan perintah ke router melalui software terminal emulation (hyperterminal). Perintah tersebut dilakukan sesuai dengan prompt yang menandakan pada mode mana router sedang bekerja.



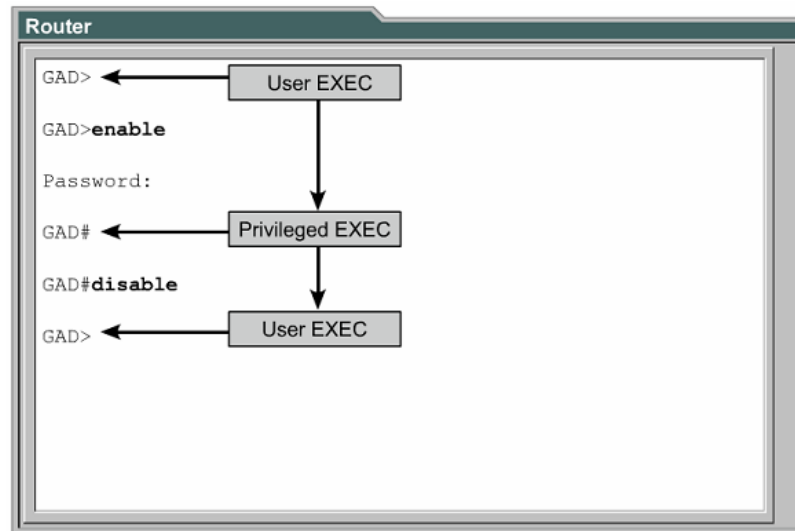
Gambar. 35

IOS menyediakan sebuah command interpreter yang disebut command executive (EXEC). Setelah perintah EXEC ini dimasukkan, EXEC akan mengvalidasi dan menjalankan perintah. Untuk memberikan keamanan, EXEC dibagi menjadi dua level. Level tersebut adalah user EXEC mode dan privileged mode.

User EXEC mode memperbolehkan hanya beberapa perintah monitoring terbatas. Sering disebut mode "view only". User mode tidak memperbolehkan perintah apapun yang dapat mengganti konfigurasi router. User mode dapat diidentifikasi dengan prompt ">".

Privileged EXEC mode mampu mengakses seluruh perintah router. Mode ini dapat dikonfigurasi untuk membutuhkan password ketika user akan mencoba mengaksesnya. Global configuration mode dan mode lainnya dapat diakses setelah user mengakses mode ini.

Untuk mengakses privileged exec mode dari user exec mode menggunakan perintah "enable", untuk sebaliknya menggunakan perintah "disable".



Gambar. 36

Global configuration mode digunakan pada router untuk mengaplikasikan perintah konfigurasi yang berefek pada keseluruhan router. Perintah berikut ini memindahkan dari mode privileged ke global configuration mode.

```
Router#configure terminal
```

```
Router(config)#
```

Dari global configuration mode dapat masuk ke menu configuration yang lain. Ketika mode specific dimasuki, prompt pada router akan berubah yang mengindikasikan mode configuration yang sekarang berjalan. Untuk kembali ke global configuration mode ketiklah perintah "exit". Tekanlah Ctrl+Z untuk keluar dari configuration mode dan kembali ke privileged mode.

2. Mengkonfigurasi Nama Router

Ketika pertama dikonfigurasi, router harus diberi nama yang unik. Tugas ini dapat dilakukan pada global configuration mode. Perintahnya adalah sebagai berikut

```
Router(config)#hostname <namahost>
```


3. Mengkonfigurasi Password Router

Password membatasi akses ke router. Password seharusnya dikonfigurasi untuk jalur virtual terminal (melalui telnet) dan console. Password juga digunakan untuk membatasi akses ke privileged mode sehingga hanya user yang berhak saja yang dapat mengaksesnya. Perintah dibawah ini digunakan untuk memberikan password ke port console.

```
Router(config)#line console 0  
Router(config-line)#password <password>  
Router(config-line)#login
```

Password juga diberikan ke satu atau lebih virtual terminal (VTY) untuk pengguna yang mengakses router melalui telnet. Biasanya router mendukung 5 jalur vty yang diberi nama vty 0 sampai dengan vty 4. Masing-masing jalur dapat diberi password yang sama atau berbeda. Dibawah ini perintah untuk memberikan password pada virtual terminal.

```
Router(config)#line vty 0 4  
Router(config-line)#password <password>  
Router(config-line)#login
```

Enable password dan enable secret digunakan untuk membatasi akses ke privileged mode. Enable password digunakan jika enable secret belum diset. Direkomendasikan menggunakan enable secret karena dilakukan enkripsi terhadap passwordnya. Perintah dibawah ini digunakan untuk memberikan enable password dan enable secret.

```
Router(config)#enable password <password>  
Router(config)#enable secret <password>
```

4. Menjalankan Perintah Show

Ada banyak perintah show yang dapat digunakan untuk memastikan isi dari konfigurasi yang telah diberikan. Pada privileged maupun user mode dapat diketik perintah "show ?" untuk menampilkan perintah apa saja yang dapat dijalankan setelah perintah show.

Mengatur Perangkat Menggunakan Software

Dibawah ini beberapa contoh perintah show yang dapat dijalankan.

- **show interface**, menampilkan seluruh statistik untuk seluruh interface pada router. Untuk melihat interface yang khusus , ketiklah perintah show interface diikuti nama interfacenya. Untuk contoh: Router#**show interfaces serial 0/1**
- **show controller serial**, menampilkan informasi spesifik dari hardware interface.
- **show clock**, menampilkan waktu yang diset pada router.
- **show host**, menampilkan cached list yang berisi nama host dan alamatnya.
- **show users**, menampilkan seluruh user yang terhubung ke router.
- **show history**, menampilkan perintah-perintah yang telah dimasukkan.
- **show flash**, menampilkan informasi mengenai memory flash dan IOS yang disimpan didalamnya.
- **show version**, menampilkan informasi mengenai router dan IOS yang tersimpan dalam RAM.
- **show ARP**, menampilkan ARP table dari router.
- **show protocol**, menampilkan status global dan interface yang telah dikonfigurasi menggunakan alamat layer 3.
- **show startup-configuration**, menampilkan konfigurasi yang telah tersimpan pada NVRAM.
- **show running-configuration**, menampilkan konfigurasi yang berjalan dan disimpan pada RAM.

5. Mengkonfigurasi Interface

Serial interface dapat dikonfigurasi melalui console atau jalur virtual terminal. Untuk mengkonfigurasi serial interface langkah-langkahnya adalah sebagai berikut:

- Masuk ke global configuration mode
- Masuk ke interface configuration mode, dilakukan dengan memberikan perintah Router(config)#interface <type port> (contohnya interface serial 0) Atau Router(config)#interface <type slot/port> (contohnya interface serial 0/1)
- Masukkan IP Address dan Subnet Masknya dengan perintah Router(config-if)#ip address <ip address> <subnet mask> (contohnya ip address 192.168.0.1 255.255.255.0).

Mengatur Perangkat Menggunakan Software

- Untuk port serial, aturlah clock rate jika kabel DCE yang terpasang. Tidak usah dilakukan jika kabel DTE yang terpasang pada interface tersebut. Perintahnya adalah sebagai berikut
Router(config-if)#clock rate <clock ratenya>
- Hidupkan interface tersebut. Defaultnya sebuah interface adalah mati. Untuk menghidupkan menggunakan perintah
Router(config-if)#no shutdown
- Untuk mematikan sebuah interface dapat menggunakan perintah
Router(config-if)#shutdown

6. Menyimpan dan Menghapus Konfigurasi

Untuk menyimpan konfigurasi yang sedang berjalan ke NVRAM menggunakan perintah

```
Router#copy running-config startup-config
```

Dengan memberikan perintah diatas maka konfigurasi yang sedang berjalan maka konfigurasi akan dipanggil lagi apabila router mati. Untuk menghapus konfigurasi yang sudah disimpan di NVRAM menggunakan perintah

```
Router#erase startup-config
```

```
Router#reload
```

7. Mengkonfigurasi Host Name Resolution

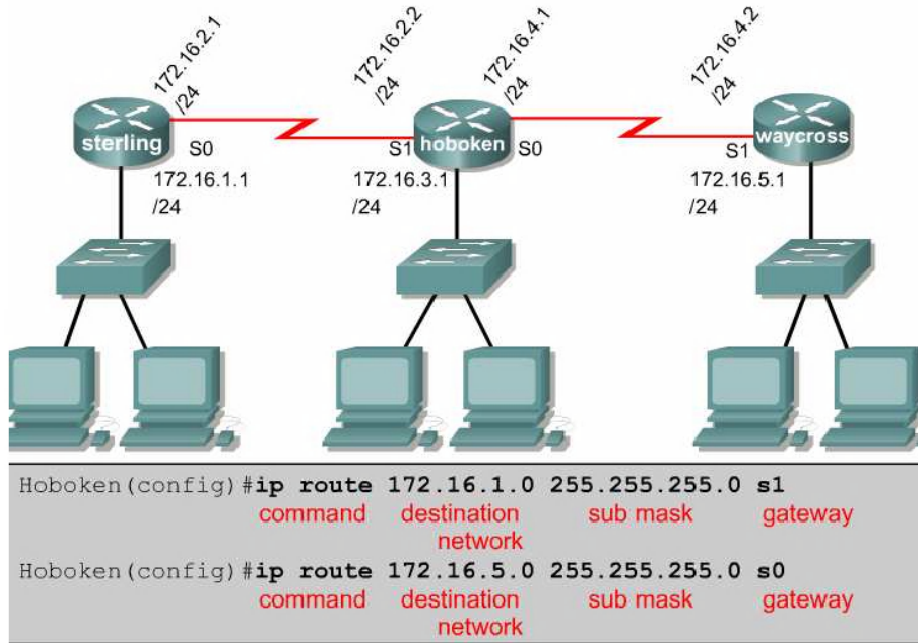
Host name resolution adalah proses dimana sistem komputer mengasosiasikan nama host dengan IP Address. Untuk menggunakan host name untuk berkomunikasi dengan perangkat jaringan lainnya, router harus mampu mengasosiasikan host name dengan IP Address. Daftar yang berisi host name dan IP Address yang berasosiasi dengannya disebut host table. Perintah untuk mengkonfigurasi host name resolution adalah "ip host" yang diikuti nama hostnya dan ip address yang diasosiasikan. IP Address yang dimasukkan bisa lebih dari satu tetapi yang diasosiasikan pertama kali adalah IP Address yang dicantumkan pertama kali dan diusahakan adalah IP Address yang terdekat dari Router. Perintahnya adalah sebagai berikut.

```
Router(config)#ip host <nama host> <ip address>
```

8. Mengkonfigurasi Static Route

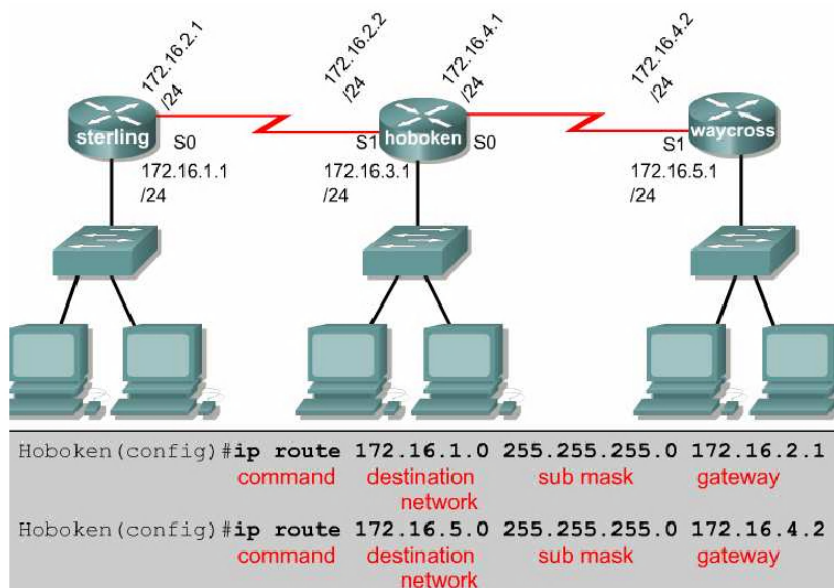
Static Route dikonfigurasi dengan memberi perintah "ip route". Ada 3 jenis static route yang dapat digunakan yaitu:

- Menggunakan interface sebagai gateway



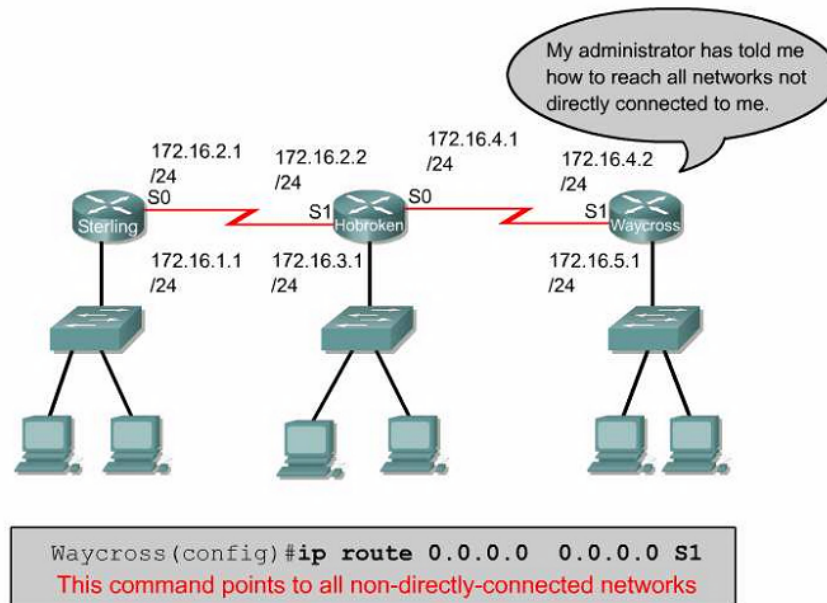
Gambar. 38

- Menggunakan hop berikutnya



Gambar. 39

- Jaringan yang tidak terhubung langsung



Gambar. 40

9. Mengkonfigurasi RIP

Routing Information Protocol (RIP) dikonfigurasi dengan memberikan perintah. Router(config)#router rip Router(config-router)#network <network address> Perintah yang kedua diberikan sebanyak jumlah network yang terhubung ke router tersebut secara langsung. Alamat jaringan yang dimasukkan adalah network address bukan subnet address atau alamat IP Address salah satu host.

10. Mengkonfigurasi Enkapsulasi HDLC

Enkapsulasi default yang digunakan HDLC. Jika interface serial telah dikonfigurasi dengan protokol enkapsulasi lainnya, dan enkapsulasi harus dirubah kembali menjadi HDLC maka langkahnya adalah:

1. Dari user mode ketik **enable**
2. Dari privileged mode ketik **configure terminal**
3. Ketik Interface nama interface contoh **interface serial 0/0**
4. Ketik encapsulation **hdlc**

11. Mengkonfigurasi Enkapsulasi PPP

Langkah–langkah mengkonfigurasi PPP:

1. Dari user mode ketik **enable**
2. Dari privileged mode ketik **configure terminal**
3. Ketik Interface nama interface contoh **interface serial 0/0**
4. Ketik **encapsulation ppp**

Software kompresi point to point dapat dikonfigurasi pada serial interface dimana menggunakan enkapsulasi. Kompresi diberikan pada software dan mungkin secara signifikan berakibat pada performansi system. Kompresi tidak dianjurkan jika sebagian besar trafik berisi file terkompresi (contoh *.zip, *.rar).

Untuk mengkonfigurasi kompresi melalui PPP, langkah–langkahnya adalah:

1. Dari user mode ketik **enable**
2. Dari privileged mode ketik **configure terminal**
3. Ketik Interface nama interface contoh **interface serial 0/0**
4. Ketik **encapsulation ppp**
5. Ketik **compress [predictor | stac]**

Untuk memonitor rusaknya data pada jalur, dan mencegah looping frame lakukan langkah sebagai berikut:

1. dari user mode ketik **enable**
2. dari privileged mode ketik **configure terminal**
3. ketik Interface nama interface contoh **interface serial 0/0**
4. ketik **encapsulation ppp**
5. ketik **ppp quality percentage**

Perintah berikut ini memberikan layanan load balancing melalui multiple link

1. dari user mode ketik **enable**
2. dari privileged mode ketik **configure terminal**
3. ketik Interface nama interface contoh **interface serial 0/0**
4. ketik **encapsulation ppp**
5. ketik **ppp multilink**

Mengatur Perangkat Menggunakan Software

Perintah berikut ini melakukan konfigurasi otentikasi PPP

1. dari user mode ketik **enable**
2. dari privileged mode ketik **configure terminal**
3. ketik **username name password secret cact:**
 - name diisi nama host dari remote router (case sensitive)
 - secret, pada router CISCO, secret password harus sama untuk 2 router
4. ketik Interface nama interface contoh **interface serial 0/0**
5. ketik **encapsulation ppp**
6. ketik **ppp authentication {chap | chap pap | pap chap | pap}**

Jika CHAP dan PAP di enabled, kemudian metode pertama akan diminta selama proses fase negosiasi jalur. Jika sama maka menyarankan menggunakan metode kedua atau jika menolak metode pertama, kemudian metode kedua akan dicoba. Pada IOS Release 11.1 atau sesudahnya, PAP harus dienablekan pada interface, jika tidak maka secara default akan didisablekan. Perintahnya adalah pada interface configuration mode ketik **ppp pap sent-username username password password**

Menyambung Perangkat dan Setting Perangkat Menggunakan Software

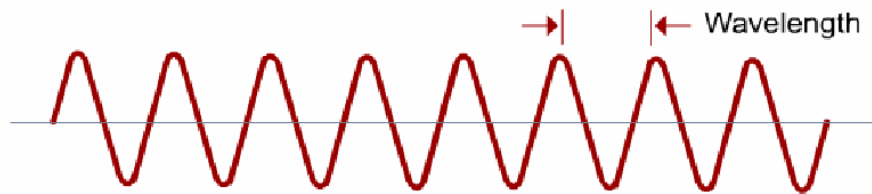
Tujuan Pembelajaran

Setelah mempelajari kegiatan belajar ini peserta diklat mampu menjelaskan spektrum frekuensi dan fungsinya pada standar waveLAN serta prinsip kerja kabel serat optik berdasarkan pada prinsip cermin dan pembiasan cahaya.

Uraian materi

1. Spektrum Elektromagnetik

Ketika sebuah tegangan elektrik berpindah, sebuah tipe energi yang disebut energi elektromagnetik terbuat. Energi ini dalam bentuk gelombang dapat berpindah melalui ruang hampa, udara dan melalui beberapa material seperti gelas. Satu hal yang penting dalam setiap gelombang energi adalah panjang gelombang.



Gambar. 42

Radio, gelombang micro, radar, sinar yang terlihat, sinar x dan sinar gamma kelihatan sebagai hal yang sangat berbeda. Sebenarnya kesemua hal tersebut adalah tipe dari energi elektromagnetik. Jika semua tipe dari gelombang elektromagnetik disusun dari panjang gelombang tertinggi sampai dengan terendah, maka susunan tersebut disebut spektrum elektromagnetik.

Panjang gelombang ditentukan dari bagaimana frekuensi dari tegangan elektrik membuat gelombang naik dan turun. Jika gelombang naik dan turun dengan lambat, panjang gelombangnya akan besar. Karena gelombang elektromagnetik dibuat dengan cara yang sama, maka semua gelombang elektromagnetik mempunyai sifat yang sama. Gelombang-gelombang tersebut melakukan perjalanan dengan kecepatan 3×10^8 m/dtk melalui ruang hampa udara.

Menyambung Perangkat dan Setting Perangkat Menggunakan Software

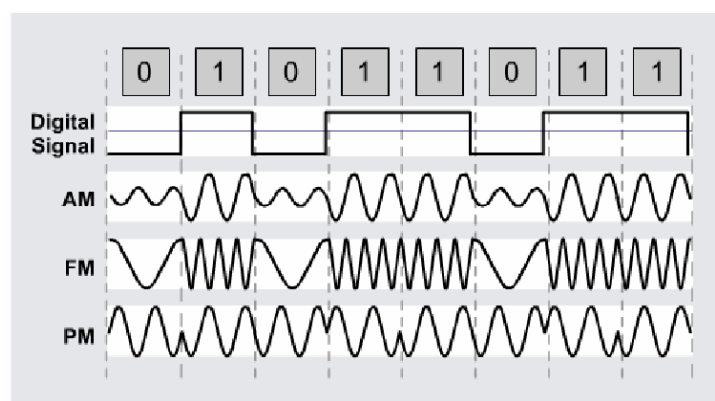
2. Spektrum Gelombang Radio dan Microwave

Komputer mengirimkan sinyal data elektronik. Pengirim merubah sinyal tersebut ke bentuk gelombang radio. Perubahan arus elektrik pada antena dari pengirim menciptakan gelombang radio. Gelombang radio tersebut mengitari keluar pada garis lurus dari antena. Kemudian gelombang tersebut mengalami hambatan setelah keluar dari antena. Pada WaveLAN, sinyal radio diukur dari jarak hanya 10 meter dari antena pengirim hanya akan mempunyai kekuatan 1/10 dari kekuatan asalnya. Seperti cahaya, gelombang radio dapat dihambat oleh beberapa material dan dipantulkan oleh material lainnya.

Karena sinyal radio melemah ketika melakukan perjalanan keluar dari pengirim, penerima harus dilengkapi juga dengan sebuah antena. Ketika gelombang radio mengenai antena dari penerima, gelombang arus yang lemah terbuat di antena. Gelombang tersebut dikuatkan sehingga sama dengan gelombang dari pengirim.

Pada pengirim, sinyal elektronik dari komputer atau LAN tidak dikirim secara langsung ke antena dari pengirim. Sinyal data tersebut ditumpangkan dahulu pada sinyal kedua, yaitu sebuah sinyal yang kuat yang disebut sinyal pembawa (carrier signal).

Proses menumpangkan ke sinyal pembawa yang akan dimasukkan ke antena pengirim disebut modulasi. Ada tiga cara dasar dimana sinyal pembawa dapat dimodulasi. Yang pertama adalah Amplitude Modulation (AM), dimana tinggi (amplitudo) sinyal pembawa berubah-ubah sesuai dengan sinyal data. Kedua adalah Frequency Modulation (FM), dimana kerapatan (frekuensi) sinyal pembawa berubah-ubah sesuai dengan amplitudo sinyal data. Ketiga adalah Phase Modulation (PM), dimana fase sinyal pembawa berubah-ubah sesuai dengan perubahan sinyal data. Pada WaveLAN, digunakan cara yang ketiga yaitu Phase Modulation (PM).



Gambar. 42

Menyambung Perangkat dan Setting Perangkat Menggunakan Software

Penerima melakukan demodulasi sinyal pembawa yang sampai ke antenanya. Penerima menerjemahkan perubahan fase dari sinyal pembawa dan membentuk ulang ke sinyal data aslinya.

3. Standar WaveLAN

Seperti halnya pada jaringan kabel, IEEE adalah organisasi utama yang membahas mengenai jaringan wireless. Standar dibuat dalam kerangka kerja yang dibuat oleh Federal Communications Commission (FCC).

Teknologi kunci dalam standar 802.11 adalah Direct Sequence Spread Spectrum (DSSS). DSSS menerapkan ke perangkat wireless untuk bekerja pada range 1 sampai dengan 2 Mbps. Sistem DSSS mungkin beroperasi sampai dengan 11 Mbps tetapi tidak dianggap diatas 2 Mbps. Standar berikutnya yaitu 802.11b, dimana kemampuan transmisi ditingkatkan sampai dengan 11 Mbps.

802.11b juga sering disebut WiFi atau wireless kecepatan tinggi dan mengacu pada sistem DSSS yang beroperasi pada 1 Mbps, 2 Mbps, 5,5 Mbps, dan 11 Mbps. Seluruh sistem 802.11b adalah backward compliant dimana mampu mendukung 802.11 untuk kecepatan data 1 atau 2 Mbps hanya untuk sistem DSSS. Backward compatibility adalah sangat penting untuk memungkinkan upgrade jaringan wireless tanpa mengganti NIC atau Access Point.

Perangkat 802.11b mendapat kecepatan data yang lebih tinggi dengan menggunakan teknik pengkodean yang berbeda dibandingkan 802.11, yang memungkinkan jumlah data yang lebih besar dapat dikirim pada frame yang sama. Kebanyakan perangkat 802.11b gagal mencapai kecepatan transfer data 11 Mbps dan umumnya bekerja pada kecepatan antara 2 sampai dengan 4 Mbps.

802.11a melayani semua perangkat wireless yang beroperasi pada band frekuensi 5 GHz. Menggunakan C-Band (5.725–5.875 GHz) tidak memungkinkan bekerjasama dengan 802.11b yang beroperasi pada S-Band (2.4–2.5 GHz). 802.11a mampu mensuplai throughput data pada 54 Mbps dan dengan teknologi yang dikenal dengan "rate doubling" dapat mencapai 108 Mbps. Pada umumnya standar yang digunakan adalah 20-26 Mbps. 802.11g menyediakan throughput yang sama dengan 802.11a tetapi dengan backward compatibility untuk perangkat 802.11b menggunakan teknologi modulasi Orthogonal Frequency Division Multiplexing (OFDM).

Menyambung Perangkat dan Setting Perangkat Menggunakan Software

Keuntungan menggunakan WaveLAN adalah sebagai berikut:

- Mobility, kemampuan perangkat untuk lebih mudah berpindah seperti laptop, PDA, Smart Device dll).
- Scalability, kemampuan jaringan untuk berkembang mengikuti kebutuhan pengguna.
- Flexibility, kemampuan jaringan untuk menyesuaikan dengan kondisi lingkungan dimana jaringan akan dipasang.
- Short and long term cost saving, kemampuan jaringan untuk mengefisienkan biaya untuk jangka waktu pendek dan panjang.
- Instalasi yang lebih mudah dan cepat.
- Mampu bertahan dalam lingkungan kerja yang keras.

4. Perangkat WaveLAN

Jaringan wireless mungkin berisi sedikitnya dua perangkat. PC atau laptop yang dilengkapi dengan NIC wireless dapat membangun jaringan yang sama dengan jaringan peer to peer pada jaringan wireline. Kedua perangkat tersebut berperilaku sebagai server dan client. Probleminya adalah keamanan yang minim dan NIC dari produsen yang berbeda mungkin tidak dapat berkomunikasi.

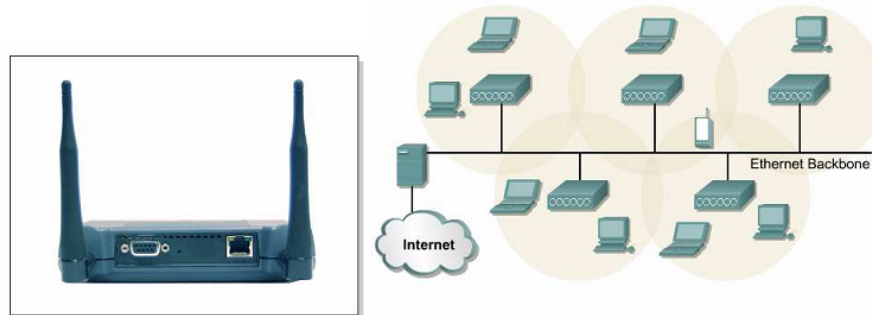


Gambar. 43

Untuk mengatasi hal tersebut, sebuah Access Point (AP) biasanya dipasang sebagai hub pusat untuk infrastruktur WaveLAN (Wireless LAN). AP menyediakan port untuk koneksi ke LAN dengan kabel. AP dilengkapi antena dan menyediakan koneksi ke area khusus yang disebut cell. Ukuran cell bervariasi tergantung pada komposisi struktur dari lokasi dimana AP dipasang dan ukuran serta gain dari antena. Umumnya jarak dari 91,44 m sampai dengan 152,4 m. Untuk melayani area yang luas, beberapa access point akan dipasang dengan sebuah sudut yang saling menumpuk (overlap). Overlap memungkinkan "roaming" diantara cell. Hal ini sama dengan layanan yang diberika oleh perusahaan telepon seluler. Meskipun tidak dijelaskan pada standar IEEE, overlap sekitar 20%-30% dibutuhkan. Banyaknya overlap memungkinkan roaming diantara cell, memungkinkan untuk memutuskan dan menyambung lagi koneksi tanpa interupsi

Menyambung Perangkat dan Setting Perangkat Menggunakan Software

layanan. Sebaiknya seluruh cell menggunakan SSID yang sama untuk menyediakan roaming pada jaringan tersebut.



Gambar. 44

Ketika client aktif dalam WaveLAN, client akan mulai "mendengar" untuk perangkat yang sesuai yang kemudian akan berkomunikasi. Hal ini disebut "scanning" dan mungkin aktif atau pasif.

Scanning aktif menyebabkan probe request dikirimkan dari host untuk bergabung ke jaringan. Probe request berisi Service Set Identifier (SSID) dari jaringan yang diharapkan akan bergabung. Ketika Access Point dengan SSID yang sama ditemukan, Access Point akan membalas probe request tersebut. Langkah autentikasi dan asosiasi telah selesai.

Scanning pasif akan membuat host mendengar beacon management frames (beacons), yang dikirimkan oleh Access Point atau host lainnya. Ketika host menerima sebuah beacon yang berisi SSID dari jaringan dan berusaha bergabung.

Diantara dua perangkat yang akan dihubungkan seharusnya dapat saling bertatapapan (line of sight). Dibawah ini adalah hal-hal yang memungkinkan adanya halangan (obstacle) diantara dua perangkat tersebut antara lain:

- Topografi seperti gunung atau bukit.
- Lingkaran bumi
- Gedung atau objek buatan manusia lainnya.
- Pepohonan
- Logam
- Tembok atau partisi ruangan lainnya.

Perangkat yang digunakan untuk menghubungkan dua atau lebih jaringan yang biasanya berada pada gedung atau lokasi yang berbeda disebut bridge. Digunakan juga antena untuk berkomunikasi antar gedung. Ada beberapa jenis antena dan spesifikasi yang berbeda-beda.

Menyambung Perangkat dan Setting Perangkat Menggunakan Software

Dilihat dari arahnya ada dua jenis antena yaitu Omni directional yaitu antena yang memancar ke segala arah (360°) dan Directional yaitu antena yang memancar dengan sudut tertentu.

	 Rubber dipole	 Pillar Mount	 Patch Wall	 Ceiling Mount	 Ceiling Mount High Gain
Type	omni	omni	Directional	omni	omni
Gain	2.15 dBi	5.2 dBi	8.5 dBi	2.2 dBi	5.2 dBi
Beamwidth	360° H 75° V	360° H 75° V	60° H 55° V	360° H 75° V	360° H 75° V
Indoor Range at 1Mbps	300' 91.4 m	497' 151.5 m	700' 213.4 m	350' 106.7 m	497' 151.5 m
Indoor Range at 11Mbps	100' 30.5 m	142' 43.3 m	200' 61 m	100' 30.5 m	142' 43.3 m
Cable Length	N/A	3' 0.9 m	3' 0.9 m	9' 2.7 m	3' 0.9 m

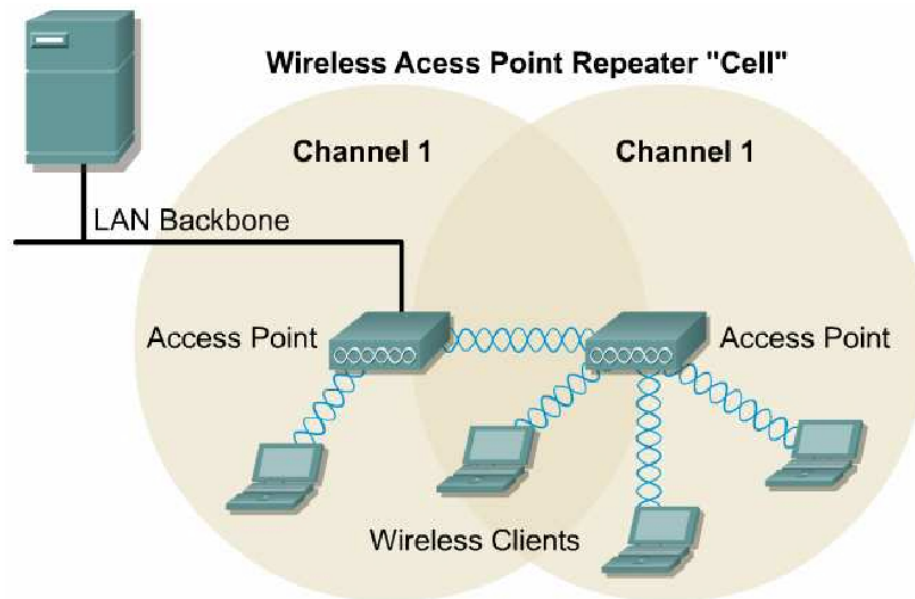
Gambar. 45

	 Patch Wall	 Mast Mount	 Mast Mount High Gain	 Yagi Mast	 Solid Dish
Type	Directional	Omni	Omni	Directional	Directional
Gain	8 dBi	5.2 dBi	12 dBi	13.5 dBi	21 dBi
Beamwidth	60° H 55° V	360° H 75° V	360° H 75° V	30° H 25° V	12.4° H 12.4° V
Approximate Range at 2 Mbps	2.0 miles 3.21 k	5000' 1,524 m	4.6 miles 7.4 k	6.5 miles 10.46 k	25 miles 40.23 k
Approximate Range at 11 Mbps	3390' 1,033.2 m	1580' 481.5 m	1.4 miles 2.25 k	2 miles 3.21 k	11.5 miles 18.50 k
Cable Length	3' .91 m	3' .91 m	1' .305 m	1.5' .457 m	2' .609 m

Gambar. 46

Wireless repeater adalah Access Point yang tidak terhubung ke kabel backbone. Membutuhkan overlapping sebanyak 50% dari Access Point yang terhubung ke kabel backbone. Throughput untuk perangkat yang terhubung ke repeater menjadi lebih kecil. Administrator dapat membuat rantai dari beberapa repeater, tetapi setiap penambahan rantai tersebut throughput menjadi setengah dari yang seharusnya. Disarankan untuk tidak lebih dari dua hop untuk setiap rantainya.

Menyambung Perangkat dan Setting Perangkat Menggunakan Software



Gambar. 47

5. Komunikasi Pada Wave LAN

Setelah pembangunan koneksi ke WaveLAN, node akan melewatkan frame sama seperti jaringan 802.x lainnya. Ada tiga tipe frame yaitu control, management dan data. Hanya frame data yang sama dengan frame 802.3. Beban pada frame 802.3 adalah 1500 byte, walaupun panjang frame 802.3 mungkin tidak lebih dari 1518 byte, sedangkan pada WaveLAN frame dapat mencapai 2346 byte. Biasanya frame yang akan dikirimkan ke LAN kabel mempunyai panjang tidak lebih dari 1518 byte.

Management Frames
<ul style="list-style-type: none">• Association request frame• Association response frame• Probe request frame• Probe response frame• Beacon frame• Authentication frame
Control Frames
<ul style="list-style-type: none">• Request to send (RTS)• Clear to send (CTS)• Acknowledgment
Data Frames

Gambar. 48

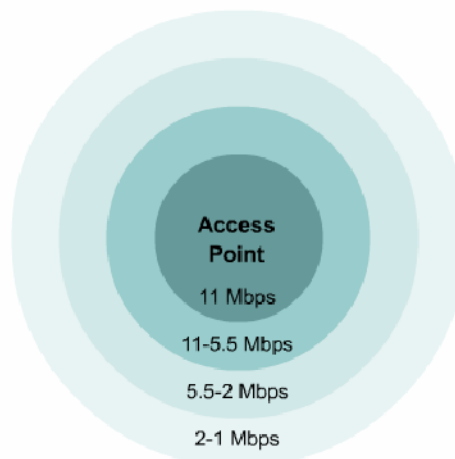
Karena frekuensi radio adalah media yang digunakan bersama-sama, collision (tabrakan) dapat terjadi seperti halnya pada jaringan kabel. Perbedaan utamanya adalah tidak adanya metode

Menyambung Perangkat dan Setting Perangkat Menggunakan Software

dimana sumber dapat mendeteksi adanya collision. Untuk alasan tersebut WaveLAN menggunakan Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA). Teknologi tersebut setara dengan CSMA/CD pada jaringan kabel.

Ketika sumber mengirimkan sebuah frame, penerima akan mengembalikan Acknowledgment positif. Hal ini menggunakan 50% dari bandwidth yang tersedia. Overhead ini ketika digabungkan dengan protokol collision avoidance mengurangi throughput menjadi maksimum 5 sampai dengan 5,5 Mbps pada jaringan 802.11b yang mempunyai kecepatan 11 Mbps.

Perfomansi dari jaringan juga akan dipengaruhi oleh kekuatan sinyal dan degradasi pada kualitas sinyal yang disebabkan jarak dan interferensi. Sinyal yang menjadi melemah, Adaptive Rate Selection (ARS) mungkin akan dilibatkan. Kecepatan data akan turun dari 11 Mbps menjadi 5,5 Mbps, dari 5,5 Mbps menjadi 2 Mbps atau dari 2 Mbps menjadi 1 Mbps jika jarak antara client dan Access Point bertambah.



Gambar. 49

6. Autentikasi dan Asosiasi

Autentikasi WaveLAN terjadi pada layer 2. Itu adalah proses autentikasi yang dilakukan oleh perangkat bukan pengguna. Ini adalah titik penting yang harus diingat ketika mempertimbangkan keamanan WaveLAN, mengatasi masalahnya dan mengatur WaveLAN.

Autentikasi mungkin merupakan proses yang tidak ada, pada kasus sebuah Access Point dan NIC baru dengan konfigurasi standar. Client akan mengirimkan frame authentication request ke

Menyambung Perangkat dan Setting Perangkat Menggunakan Software

AP dan frame tersebut akan diterima atau ditolak oleh AP. Client diberitahu jawaban melalui frame authentication response. AP mungkin juga dikonfigurasi untuk menyerahkan tugas autentikasi ke sebuah authentication server, dimana server tersebut akan melakukan proses autentikasi yang lebih baik.

Ada tiga tipe autentikasi dan asosiasi yaitu:

- Unauthenticated and unassociated Host akan diputuskan dari jaringan dan tidak diasosiasikan dengan AP.
- Authenticated and unassociated Host yang telah diautentikasi pada jaringan tetapi belum diasosiasikan dengan AP.
- Authenticated and associated Host terhubung ke jaringan dan mampu untuk mengirim dan menerima data melalui access point.

Ada dua tipe proses autentikasi berdasarkan standar 802.11 yaitu:

a. Open system

Proses ini adalah standar koneksi yang terbuka dimana hanya SSID yang harus sama.

b. Shared key

Proses ini membutuhkan penggunaan enkripsi WEP (Wireless Equivalency Protocol). WEP adalah algoritma sederhana menggunakan kunci 64 dan 128 bit. AP dikonfigurasi dengan kunci enkripsi dan host yang mencoba mengakses jaringan melalui AP harus mempunyai kunci yang cocok. Menggunakan proses ini lebih bagus dibandingkan open system walaupun bukan berarti tahan "hack". Problem keamanan pada WaveLAN diatasi dengan beberapa solusi teknologi keamanan yang baru.

7. Sinyal dan Noise pada WaveLAN

Pada jaringan ethernet dengan kabel, proses untuk mengidentifikasi penyebab interferensi dapat dilakukan dengan lebih mudah dibandingkan pada WaveLAN. Ketika menggunakan teknologi frekuensi radio, ada begitu banyak interferensi yang harus diperhatikan.

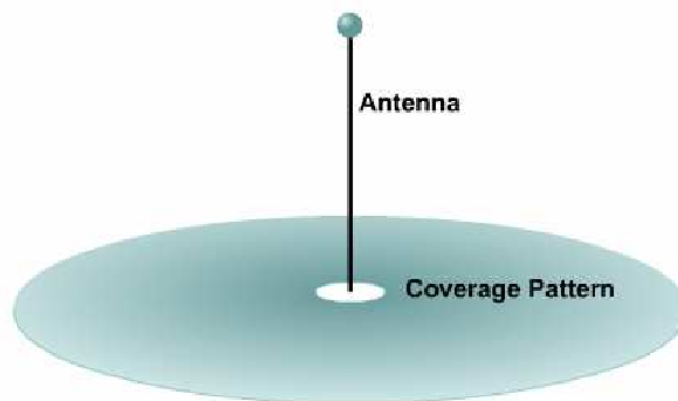
Narrowband adalah kebalikan dari teknologi spread spectrum. Sesuai dengan namanya, narrowband tidak akan berpengaruh terhadap keseluruhan spektrum frekuensi dari sinyal wireless. Salah satu solusi untuk mengatasi masalah interferensi pada narrowband adalah dengan mengganti channel yang digunakan oleh AP. Untuk mengidentifikasi sumber interferensi dibutuhkan alat yang disebut spectrum analyzer dan alat tersebut relatif mahal.

Menyambung Perangkat dan Setting Perangkat Menggunakan Software

Terdapat juga interferensi yang berakibat pada keseluruhan frekuensi yang tersedia. Teknologi Bluetooth melalui frekuensi 2,4 GHz beberapa kali per detik dan dapat menyebabkan interferensi yang signifikan pada jaringan 802.11b. Di rumah dan kantor, peralatan yang sering menyebabkan interferensi adalah oven microwave. Kebocoran dari microwave walaupun kecil dapat menyebabkan gangguan yang besar dalam WaveLAN. Telepon seluler yang beroperasi pada frekuensi 2,4 GHz juga dapat menyebabkan interferensi.

Umumnya sinyal frekuensi radio tidak akan dipengaruhi oleh kondisi cuaca apapun. Tetapi, kabut atau kondisi yang sangat lembab dapat berakibat pada WaveLAN. Pencahayaan dapat juga berakibat pada atmosfer dan berakibat pada sinyal WaveLAN.

Sumber utama dari sumber masalah sinyal adalah station pengirim dan tipe antenna. Station pengirim yang tinggi akan mengirimkan sinyal lebih jauh dan antenna jenis parabola dish dapat mengkonsentrasikan sinyal yang akan meningkatkan jarak transmisi. Jenis antenna twin omnidirectional pada access point juga dapat mengurangi jarak komunikasi.



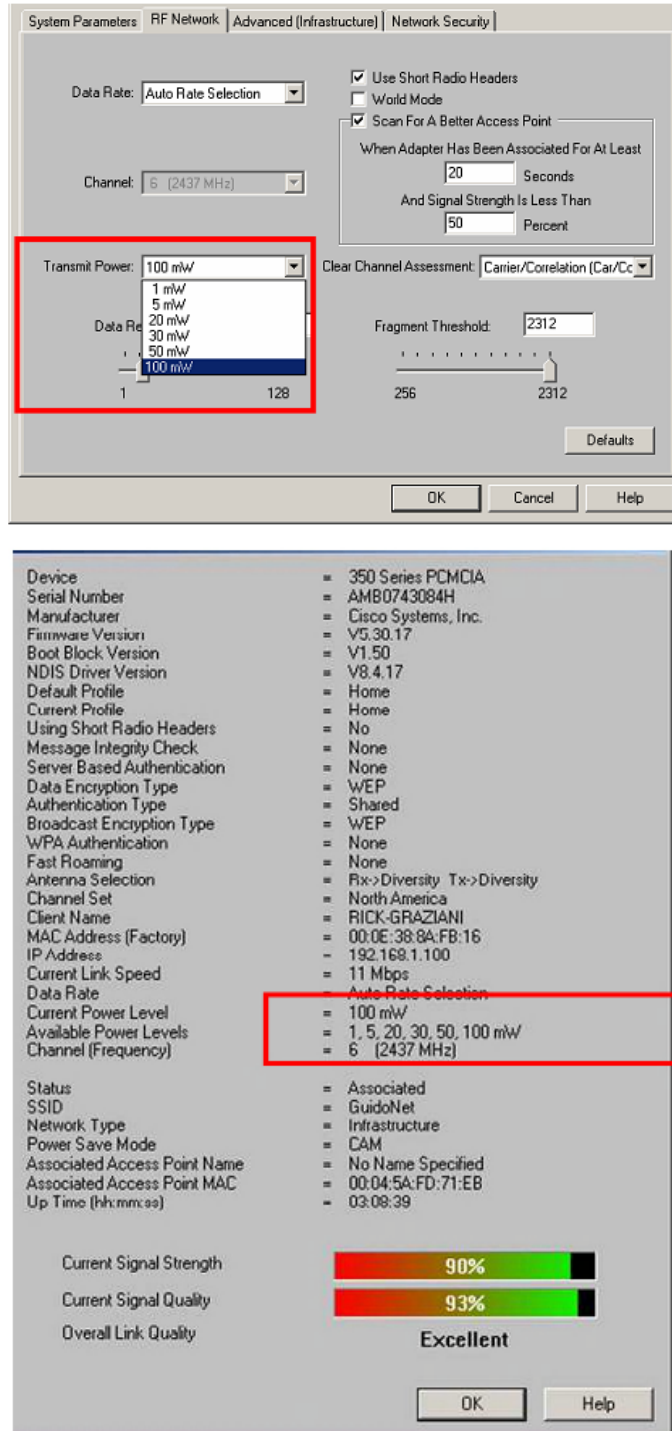
Gambar. 50

8. Mengubah Ukuran Energi pada WaveLAN

Ukuran energi pada sebuah segmen WaveLAN jarang diatas 100 mW. Energi diatas 100 mW cukup untuk berkomunikasi sampai dengan 3–4 km. Access Pont umumnya memiliki kemampuan dari 30–100 mW. Perangkat outdoor (bridges) menggunakan energi diatas 100 mW.

Untuk merubah ukuran energi dapat dilakukan dari perangkat lunak yang disertakan dalam perangkat tersebut. Administrator juga dapat melihat ukuran energi dari perangkat lunak tersebut.

Menyambung Perangkat dan Setting Perangkat Menggunakan Software



Gambar. 51

Ukuran energi selain menggunakan Watt, juga menggunakan satuan decibel (dB). dB diukur berdasarkan logaritma berbasis 10, artinya kalo terjadi selisih sebesar 1 dB sama dengan selisih energi sebesar 10 kali lipat. Skala ini memudahkan untuk bekerja pada angka-angka besar.

Menyambung Perangkat dan Setting Perangkat Menggunakan Software

Menghitung dB dilakukan menggunakan rumus sebagai berikut:

$$\text{dB} = 10 \log_{10}(P_{\text{akhir}}/P_{\text{awal}})$$

dimana: dB = banyaknya energi dalam decibel

P_{akhir} = energi akhir, yaitu ukuran energi setelah proses terjadi.

P_{awal} = energi awal, yaitu ukuran energi sebelum proses terjadi.

Satuan decibel memiliki beberapa varian. dBx dimana x menggambarkan suatu nilai tertentu, sering digunakan untuk menggantikan dB. Di bawah ini adalah referensi untuk decibel yaitu:

- dBm, dimana m adalah miliwatt. Jika dibutuhkan nilai dBm bisa dikembalikan lagi ke nilai watt. Energi yang hilang atau dikuatkan dari sinyal dapat diketahui dengan melihat titik referensi yang tetap yaitu miliwatt

mW (milliwatts)	W (Watts)	dBm (decibels per 1 mW)	dBW (decibels per 1 Watt)
1	.001	0	-30
2	.002	3	-27
5	.005	7	-23
10	.01	10	-20
20	.02	13	-17
50	.05	17	-13
100	.1	20	-10
1,000	1	30	0
2,000	2	33	3
4,000	4	36	6

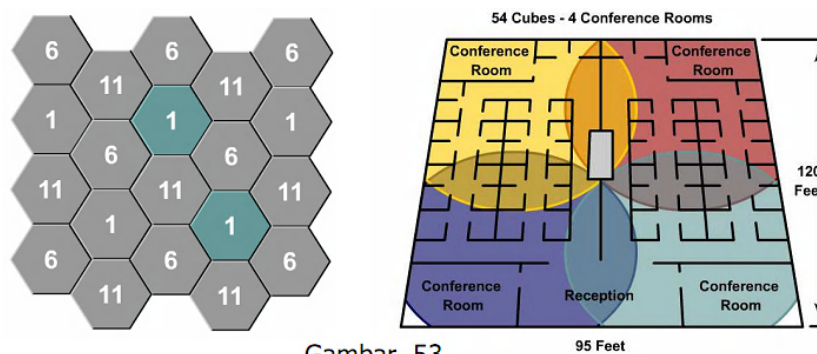
Gambar. 52

- dBd, dimana d adalah dipole. Satuan ini menunjukkan penguatan yang dimiliki oleh antena, yang dibandingkan dengan antena dipole pada frekuensi yang sama. Antena dipole adalah antena terkecil dimana antena tersebut adalah antena dengan penguatan paling sedikit yang dapat dibuat.
- dBi, dimana i adalah isotropic. Satuan ini sama dengan dBd tetapi pembandingnya adalah teori isotropic. Teori isotropic untuk antena tidak dapat diwujudkan tetapi berguna untuk menghitung secara teoritis coverage dan fade area.
- EIRP (Effective Isotropic Radiated Power). EIRP adalah energi efektif yang didapat pada main lobe dari antena pengirim. Menghitung EIRP adalah dengan menjumlahkan penguatan antena (dalam satuan dBi) dengan level energi (dalam satuan dBm) pada antena tersebut.

9. Setup Channel dan Topologi Bridge

Ada dua langkah penting dalam pengembangan WaveLAN yaitu:

- Tentukan penempatan dari Access Point atau bridge, termasuk jumlah dari Access Point atau bridge yang dibutuhkan untuk melayani seluruh area. Pastikan juga bahwa daerah yang tidak terlayani berukuran kecil
- Petakan pemberian channel, usahakan overlap sesedikit mungkin diantara channel yang menggunakan frekuensi yang sama. Tentukan juga level energi untuk setiap Access Point. Besarnya level energi menentukan luas daerah yang dilayani. Ada kalanya dibutuhkan menurunkan energi untuk membentuk pico-cell, yaitu cell dengan ukuran kecil. Hal ini dilakukan untuk mencegah overlapping yang terlalu banyak dan cell tersebut keluar gedung yang tentunya akan menimbulkan masalah dalam keamanannya. Level energi juga tidak melebihi maksimum level yang diperbolehkan oleh organisasi yang mengaturnya.



Gambar. 53

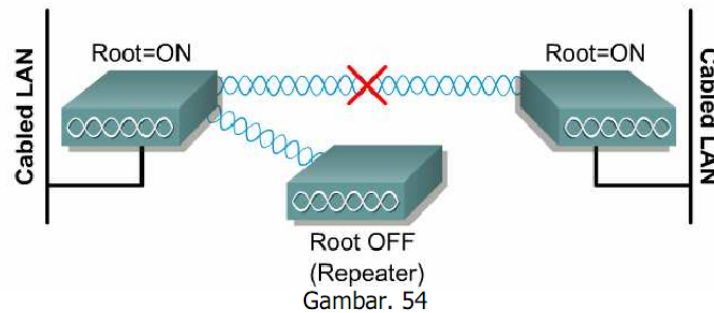
Dalam menentukan channel dan frekuensi yang digunakan, sebaiknya mengetahui frekuensi yang sudah digunakan oleh organisasi atau perusahaan yang lokasinya berdekatan. Hal ini karena frekuensi 2,4 dan 5 GHz merupakan frekuensi yang tidak berlisensi, artinya setiap orang berhak menggunakan frekuensi tersebut tanpa diatur oleh organisasi manapun. Pengukuran dapat menggunakan spectrum analyzer dan bertujuan untuk mencegah adanya interferensi karena menggunakan frekuensi yang sama.

Sebuah bridge dapat diatur mode rootnya. Ada dua mode root yaitu:

- On, artinya bridge atau Access Point menjadi root. Bridge tersebut disebut master bridge. Bridge ini hanya berkomunikasi dengan client dan repeater. Tidak akan berkomunikasi dengan sesama root bridge lainnya. Sebuah jaringan dapat berisi lebih dari satu root bridge.

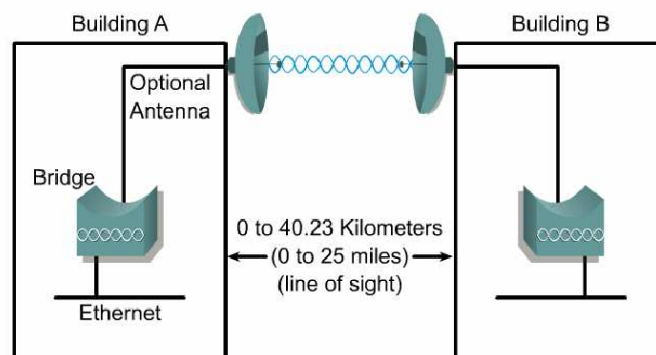
Menyambung Perangkat dan Setting Perangkat Menggunakan Software

- Off, artinya non root bridge. Bridge ini dapat berkomunikasi dengan bridge root atau bridge non root lainnya yang berasosiasi dengan root bridge. Mampu berkomunikasi dengan client selama terhubung ke root bridge. Interface ethernet pada bridge ini dimatikan.



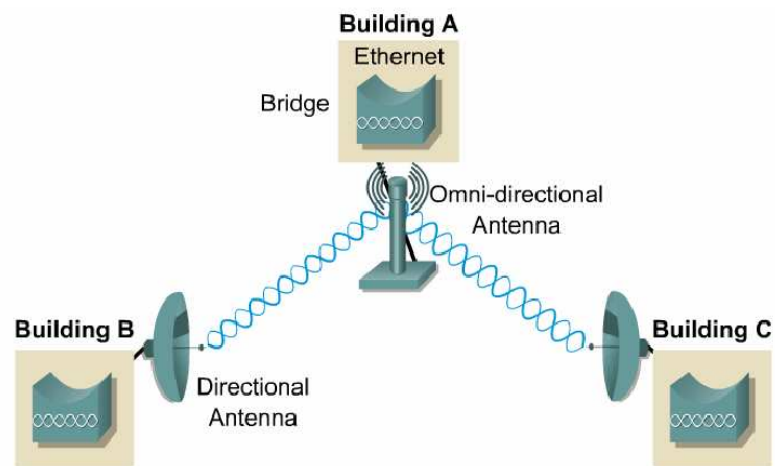
Untuk komunikasi antara bridge dapat menggunakan dua konfigurasi yaitu:

- Point to point, dua buah antenna saling berhadapan dan harus line of sight. Dalam konfigurasi ini kedua segment berperilaku sebagai menjadi satu segment. Jarak diantara dua buah antenna bisa mencapai 40 km. Konfigurasi ini menggunakan antenna directional untuk setiap sitenya.



- Point to multipoint, dimana terdapat sebuah antenna omni directional yang berperilaku sebagai main site. Antena directional digunakan pada remote site. Pada konfigurasi ini LAN berperilaku sebagai satu segmen. Traffic dari satu area akan dikirimkan ke main site dan diteruskan ke area lainnya. Diantara remote site tidak dapat berkomunikasi secara langsung dan harus melibatkan main site. Line of sight diantara masing-masing remote site terhadap main site.

Menyambung Perangkat dan Setting Perangkat Menggunakan Software

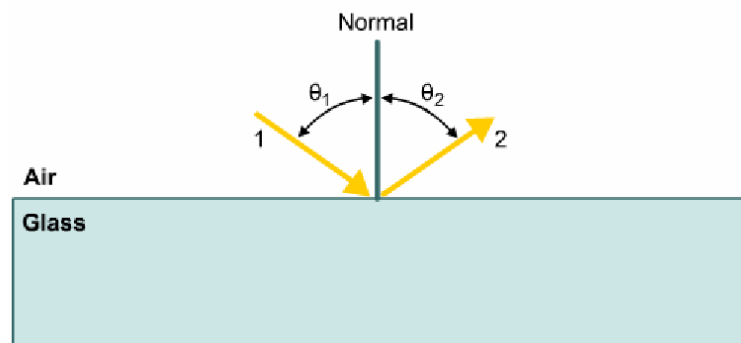


Gambar. 56

10. Sinar Cahaya

Ketika gelombang elektromagnetik keluar dari sumber, gelombang tersebut akan menempuh suatu garis lurus. Garis lurus yang keluar dari sumber disebut sinar. Pada vacuum, cahaya akan menembus dengan kecepatan 300.000 kilometer per detik dalam suatu garis lurus. Cahaya akan memiliki kecepatan yang lebih rendah apabila melalui material lainnya seperti udara, air dan gelas. Ketika sinar cahaya melalui batas sebuah material dengan material lainnya, beberapa energi cahaya tersebut akan dipantulkan kembali. Hal ini yang menyebabkan kita dapat melihat bayangan diri kita di cermin. Cahaya yang memantul disebut sinar pantul (reflected ray).

Sudut diantara sinar datang dan garis tegak lurus dengan permukaan sebuah material disebut sudut datang. Garis tegak lurus tersebut disebut garis normal. Sudut diantara garis normal dengan sinar pantul disebut sudut pantul. Hukum pemantulan cahaya menyebutkan bahwa sudut datang sama dengan sudut pantul.



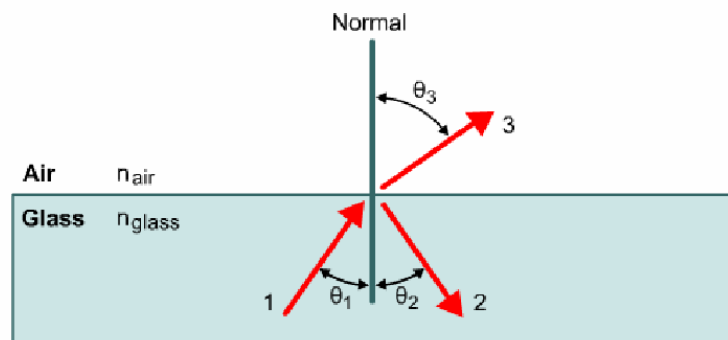
Gambar. 57

Menyambung Perangkat dan Setting Perangkat Menggunakan Software

Energi cahaya yang tidak memantul akan masuk ke material tersebut. Cahaya yang masuk akan dibelokkan dari jalur yang seharusnya. Cahaya ini disebut sinar bias (refracted ray). Berapa banyak sudut yang terbentuk diantara sinar datang dan sinar bias tergantung pada sudut diantara sinar datang dan permukaan material serta perbedaan kecepatan cahaya ketika cahaya melalui kedua material tersebut. Pembelokan sinar cahaya pada batas diantara dua material tersebut yang menjadi sebab kenapa sebuah cahaya dapat menempuh perjalanan melalui serat optik. Indeks bias adalah satuan yang menggambarkan besarnya hambatan yang didapat sebuah cahaya ketika menempuh sebuah material. Semakin besar indeks bias maka semakin besar juga penurunan kecepatan cahaya ketika menempuh material tersebut dibandingkan ketika menempuh perjalanan pada vacuum. Rumus menghitung indeks bias adalah sebagai berikut:

$$\text{Indeks bias} = n = \frac{\text{kecepatan cahaya pada vacuum}}{\text{Kecepatan cahaya pada material}}$$

Jika sinar datang membentuk 90 derajat terhadap permukaan material maka sinar tersebut akan masuk lurus ke material tersebut tanpa dibiaskan. Jika sinar datang dari material dengan indeks bias lebih tinggi, sinar bias akan menjauhi garis normal, begitu juga sebaliknya.

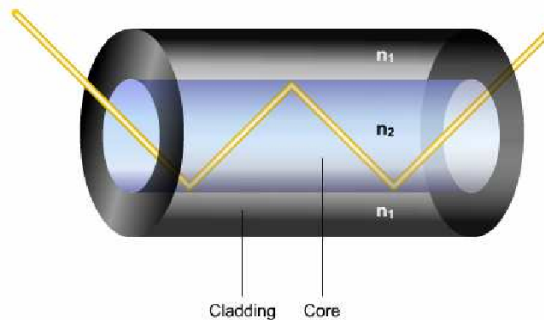


Gambar. 58

11. Pemantulan sempurna pada serat optik

Cahaya digunakan untuk membawa data melalui serat optik. Sinar cahaya harus dijaga selalu berada di dalam serat optik sampai ke tujuan. Sinar harus tidak dibiaskan ke material yang membungkus serat optik. Pembiasan akan menyebabkan hilangnya sebagian energi dari cahaya tersebut.

Menyambung Perangkat dan Setting Perangkat Menggunakan Software



Gambar. 59

Hukum pemantulan dan pembiasan cahaya menggambarkan bagaimana mendesain sebuah serat yang mampu menuntun cahaya melalui serat optik dengan kehilangan energi yang paling minimal. Ada dua kondisi yang harus didapatkan untuk sebuah sinar cahaya pada serat optik agar dapat dipantulkan kembali ke dalam serat optik tanpa kehilangan energi akibat pembiasan yaitu:

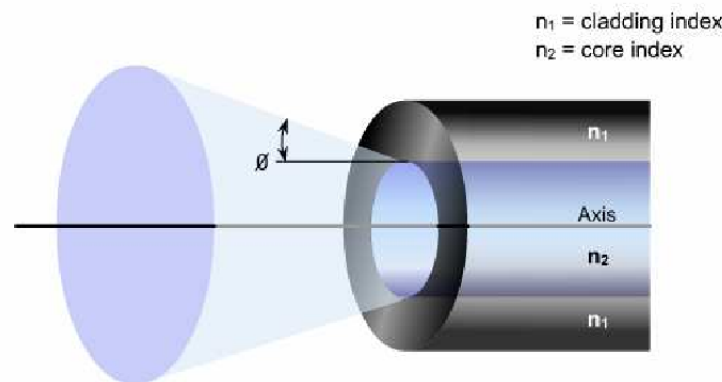
- Inti dari serat optik harus memiliki indeks bias lebih tinggi dari material yang mengelilinginya. Material yang mengelilingi core disebut cladding.
- Sudut datang dari sinar harus lebih besar dari sudut kritis dari core dan cladding. Sudut datang dari sinar harus lebih besar dari sudut kritis dari core dan cladding. Sudut kritis adalah sudut terbesar yang memungkinkan cahaya akan dibiaskan dan dipantulkan.

Ketika kedua kondisi tersebut didapatkan, maka semua sinar datang akan dipantulkan kembali ke dalam serat optik. Ini disebut pemantulan sempurna, yang merupakan dasar pembuatan serat optik. Cahaya akan menempuh jalur zigzag di dalam core serat optik.

Serat optik yang memenuhi kondisi pertama dapat mudah dibuat. Sebagai tambahan, sudut datang yang masuk ke core serat optik dapat dikontrol. Ada dua faktor yang membatasi sudut datang yaitu:

- Numerical aperture dari serat (NA), yaitu range dari sudut datang yang masuk ke core dan akan dipantulkan sempurna.
- Modes, jalur dimana sinar cahaya dapat diikuti ketika masuk ke serat optik.

Menyambung Perangkat dan Setting Perangkat Menggunakan Software

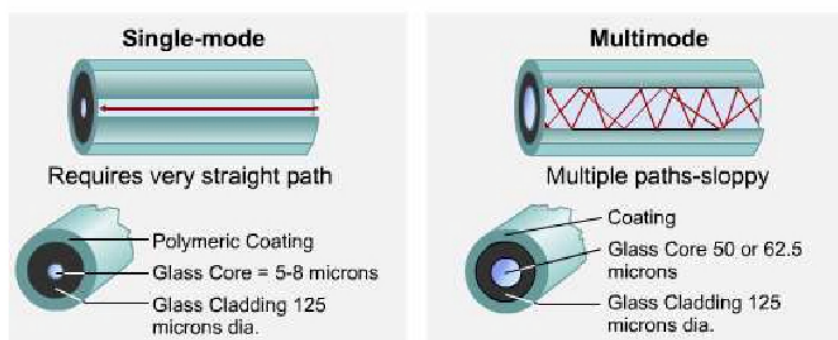


Gambar. 60

Dengan mengontrol kedua kondisi tersebut, serat optik akan melakukan pemantulan sempurna.

12. Kabel serat optik

Bagian dari serat optik dimana cahaya melakukan perjalanan disebut core. Sinar cahaya dapat masuk ke core jika sudut datang berada pada range numerical aperture. Core memiliki jumlah jalur optik yang terbatas. Jalur optik tersebut dinamakan mode. Jika diameter dari core cukup besar sehingga ada banyak jalur yang dapat dilalui melalui serat optik, serat tersebut dinamakan multimode. Serat optik single mode memiliki core yang lebih kecil sehingga hanya memungkinkan satu mode saja yang dapat melalui serat optik.



Gambar. 61

Setiap kabel serat optik yang digunakan untuk jaringan terdiri dua buah serat optik yang dibungkus oleh perisai yang terpisah. Satu serat digunakan untuk membawa data dari A ke B, satunya lagi digunakan untuk sebaliknya. Hal ini menjadikan jalur komunikasi full duplex.

Menyambung Perangkat dan Setting Perangkat Menggunakan Software

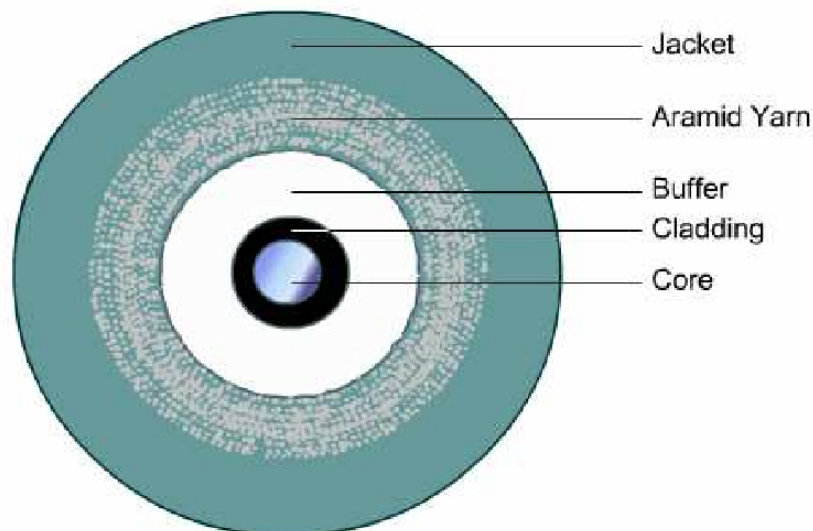
Biasanya dua kabel tersebut akan berada dalam satu outer jacket sampai ke ujung dimana konektor terpasang.



Gambar. 62

Serat optik tidak membutuhkan twisting ataupun shielding, karena tidak ada sinar yang mampu keluar ketika berada didalam serat optik. Ini berarti, serat optik tahan terhadap crosstalk. Hal ini memungkinkan ada banyak serat optik didalam satu kabel. Satu kabel dapat berisi 2 sampai dengan 48 serat yang terpisah.

Biasanya ada lima bagian yang membentuk serat optik yaitu core, cladding, sebuah buffer, material yang kuat dan outer jacket.



Gambar. 63

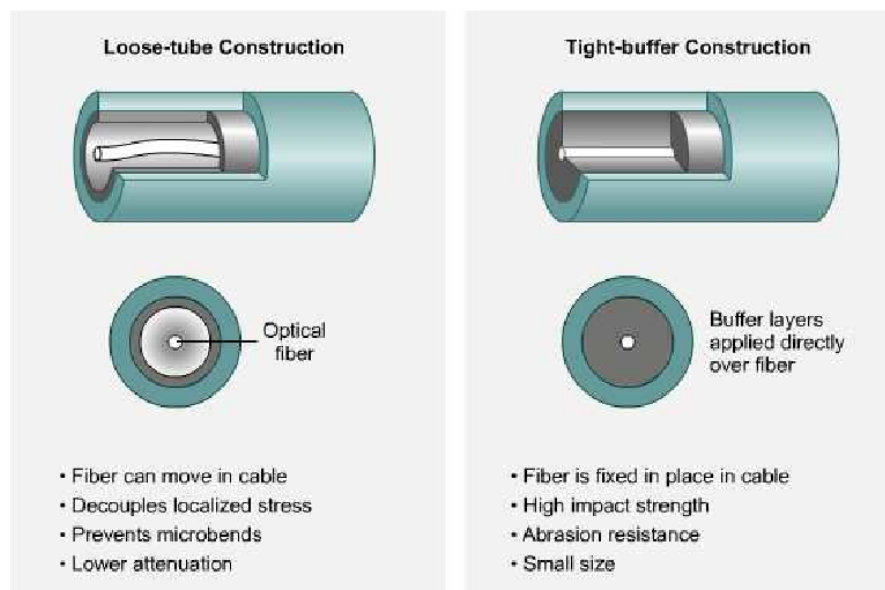
Core adalah element transmisi cahaya yang berada pada pusat serat optik. Seluruh sinar cahaya melewati core. Core umumnya terbuat dari gelas yang merupakan kombinasi dari silicon dioxide (silica) dan elemen lainnya. Multimode menggunakan tipe gelas yang disebut graded index glass. Gelas ini memiliki indeks bias makin mengecil. Dengan kata lain, bagian terluar gelas memiliki indeks bias terkecil, sedangkan bagian terdalam memiliki indeks bias terbesar. Desain ini dibuat agar sinar yang melalui bagian terdalam dan menempuh jarak yang paling pendek

Menyambung Perangkat dan Setting Perangkat Menggunakan Software

dapat tiba bersamaan dengan sinar yang memantul di bagian luar core dan menempuh jarak paling jauh.

Cladding adalah bagian yang mengelilingi core. Cladding juga dibuat dari silica tetapi memiliki indeks bias terendah dibandingkan core. Sinar cahaya akan dipantulkan kembali oleh cladding ke dalam core. Kabel serat optik multimode standar banyak digunakan untuk LAN. Kabel ini memiliki diameter cladding 125 micron.

Mengelilingi cladding adalah buffer yang biasanya terbuat dari plastik. Material ini membantu melindungi core dan cladding dari kerusakan. Ada dua desain dasar kabel yaitu loose tube dan tight-buffered. Kebanyakan desain yang digunakan adalah tight-buffered. Kabel tight-buffered memiliki material buffer yang bersentuhan langsung dengan cladding. Sedangkan pada loose tube, buffer tidak bersentuhan langsung tetapi memiliki rongga udara diantaranya. Tight-buffered banyak digunakan untuk didalam gedung sedangkan loose tube digunakan untuk diluar gedung.



Gambar. 64

Material yang kuat digunakan untuk mengelilingi buffer dan digunakan untuk mencegah kabel tertarik ketika pemasangan. Material yang banyak digunakan adalah kevlar, bahan yang sama untuk rompi anti peluru. Bagian yang terakhir adalah outer jacket. Outer jacket mengelilingi kabel untuk melindungi serat dari lecet, kerusakan dan kontaminasi lainnya. Warna dari outer jacket untuk kabel multimode biasanya oranye sedangkan untuk single mode adalah kuning walau mungkin menggunakan warna lainnya.

Menyambung Perangkat dan Setting Perangkat Menggunakan Software

Multimode memiliki spesifikasi sebagai berikut:

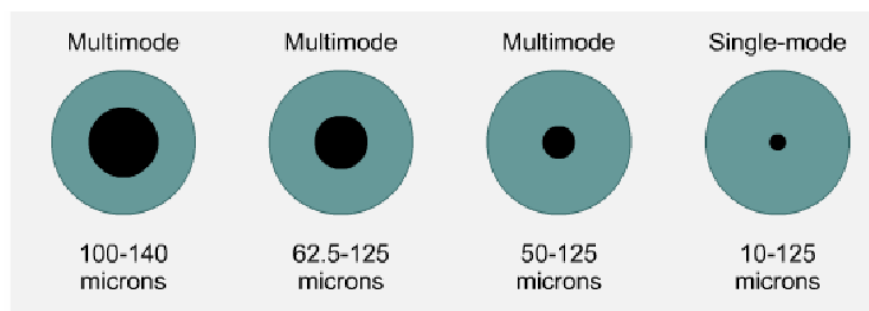
- Ukuran core yang lebih besar dari single mode yaitu 50 atau 62,5 micron atau lebih besar.
- Memungkinkan adanya dispersi (penghamburan) yang lebih besar, sehingga memungkinkan hilangnya sinyal lebih besar.
- Panjang maksimum 2 km (lebih pendek dari single mode).
- Menggunakan LED sebagai sumber cahaya.

Single mode memiliki spesifikasi sebagai berikut:

- Ukuran core yang lebih kecil yaitu 5–8 micron.
- Dispersi yang lebih kecil.
- Cocok untuk penggunaan jarak jauh.
- Menggunakan laser sebagai sumber cahaya.

Pada serat optik single mode, sudut datang adalah 90 derajat terhadap permukaan serat optik yang menyebabkan sinar melalui garis lurus didalam core serat optik. Hal ini menyebabkan peningkatan kecepatan dan jarak yang dapat ditempuh.

Karena desain tersebut, single mode memiliki bandwidth yang lebih besar serta jarak yang lebih jauh dari multimode. Hanya kabel ini relatif lebih mahal dari multimode dan menggunakan laser yang lebih mahal dari LED. Melihat spesifikasinya single mode banyak digunakan untuk koneksi antar gedung.

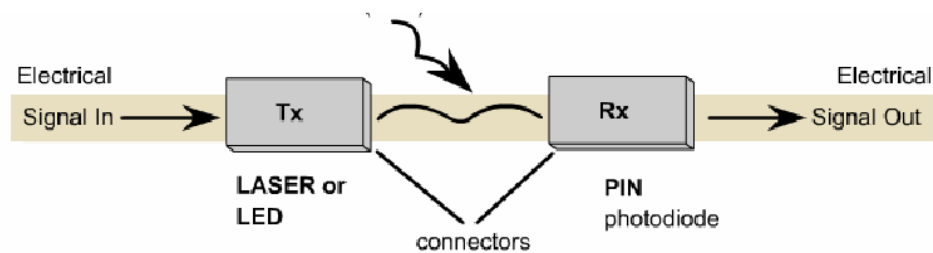


Gambar. 65

Perlu diperhatikan penggunaan laser pada single mode. Laser dapat merusak mata. Oleh karena itu jangan pernah melihat ujung jauh dari kabel single mode yang sudah terpasang, atau melihat transmit port dari Router, Switch atau NIC yang menggunakan kabel single mode. Pastikan untuk selalu memasang tutup pelindung pada ujung dari kabel serat optik single mode dan memasangnya pada port optical dari switch atau router.

13. Perangkat transmisi serat optik

Kebanyakan data yang dikirimkan melalui LAN dalam bentuk sinyal elektronik. Oleh karena itu dibutuhkan perangkat yang merubah sinyal elektrik ke dalam bentuk cahaya dan sebaliknya. Hal ini berarti dibutuhkan trasmitter dan receiver.



Gambar. 66

Transmitter menerima data untuk dikirimkan dari router atau switch. Data ini dalam bentuk sinyal elektronik. Transmitter merubah sinyal elektronik kedalam bentuk gelombang cahaya. Ada dua sumber cahaya yang digunakan yaitu:

- LED (Light Emitting Diode) yang menghasilkan sinar infra merah dengan panjang gelombang 850 nm atau 1310 nm. Lensa digunakan untuk memfokuskan sinar infra merah pada ujung penerima.
- LASER (Light Amplification by Stimulated Emission Radiation) yang akan menghasilkan sinar tipis dengan panjang gelombang 1310 nm atau 1550 nm.

Setiap sumber cahaya tersebut dapat mati dan hidup dengan sangat cepat untuk mengirim data (0 atau 1) pada jumlah bit yang banyak setiap detik.

Pada ujung lainnya dari serat optik dipasang alat yang disebut receiver. Ketika cahaya mengenai receiver, akan menimbulkan energi listrik. Tugas pertama dari receiver adalah mendeteksi cahaya yang datang dari serat optik. Kemudian receiver merubah cahaya tersebut menjadi sinyal elektronik sehingga dapat dikirimkan kembali ke jaringan. Perangkat semikonduktor yang digunakan sebagai receiver adalah pintrinsic-n diode (PIN photodiodes). PIN photodiode didesain agar sensitif terhadap cahaya dengan panjang gelombang 850, 1310 atau 1510 nm.

Konektor dibutuhkan agar kabel serat optik dapat terpasang pada port yang tersedia. Tipe konektor yang banyak digunakan untuk kabel serat optik multimode adalah Subscriber

Menyambung Perangkat dan Setting Perangkat Menggunakan Software

Connector (SC Connector). Pada single mode menggunakan konektor Straight Tip (ST Connector).



Gambar. 67

Perangkat lainnya adalah repeater. Repeater digunakan untuk menguatkan sinyal optik supaya menempuh jarak yang lebih jauh dengan mengembalikan sinyal tersebut ke dalam bentuk, kekuatan dan timing yang sama dengan aslinya. Dengan adanya repeater maka jarak yang lebih jauh dari spesifikasi serat optik dapat dilalui.

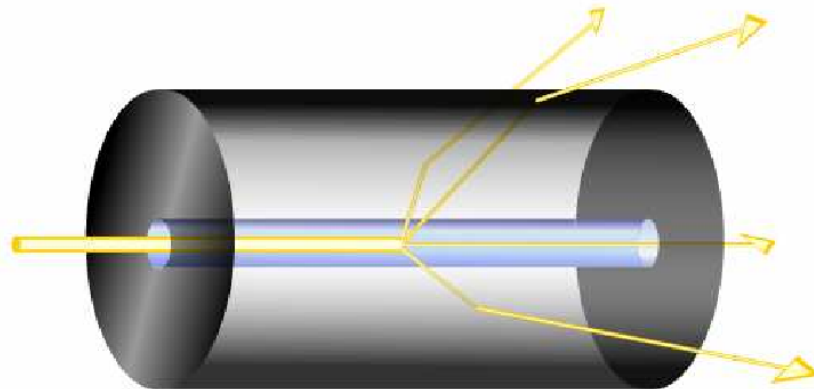
14. Sinyal dan Noise pada Serat Optik

Kabel serat optik tidak dipengaruhi oleh sumber noise dari luar yang menyebabkan problem seperti kabel tembaga karena cahaya luar tidak dapat masuk pada serat optik kecuali pada transmitter. Buffer dan outer jacket dapat mencegah sinar masuk atau keluar dari kabel.

Lebih lanjut, transmisi cahaya dari satu serat tidak akan menciptakan interferensi ke serat lainnya. Artinya serat optik tidak memiliki masalah crosstalk seperti halnya kabel tembaga. Meskipun serat optic merupakan media transmisi terbaik untuk membawa data berukuran besar dengan jarak yang jauh, bukan berarti tidak memiliki masalah.

Ketika cahaya melalui serat, ada beberapa energi cahaya yang hilang. Pengurangan sinyal terjadi karena beberapa faktor yang melibatkan sifat alami serat optik. Faktor utama yaitu scattering (penghamburan). Scattering cahaya dalam serat optik disebabkan microscopic nonuniformity (distorsi) pada serat yang memantulkan dan menghamburkan beberapa energi cahaya.

Menyambung Perangkat dan Setting Perangkat Menggunakan Software

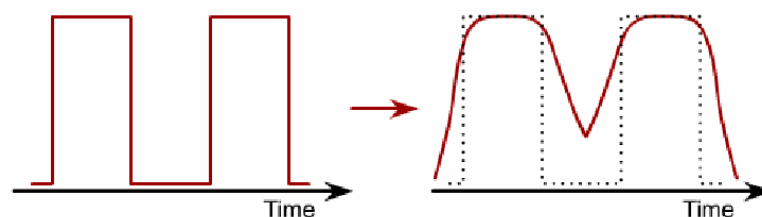


Gambar. 68

Absorption adalah faktor lain hilangnya energi. Ketika sinar cahaya menghantam beberapa bahan kimia yang tidak murni dalam serat, bahan tersebut menyerap sebagian energi. Energi cahaya tersebut dirubah ke sejumlah kecil energi panas.

Faktor lain yang menyebabkan attenuation (pengurangan) dari sinyal cahaya adalah pembuatan batas core dan cladding yang tidak baik. Energi hilang karena kurang sempurnanya pemantulan yang disebabkan kasarnya pembuatan kabel tersebut. Setiap ketidaksempurnaan walaupun berukuran kecil akan mengurangi energi cahaya tersebut.

Penghamburan (dispersion) cahaya juga membatasi jarak dari sebuah cahaya. Dispersion adalah istilah teknik untuk pelebaran pulsa sinyal ketika menempuh perjalanan didalam serat optik.



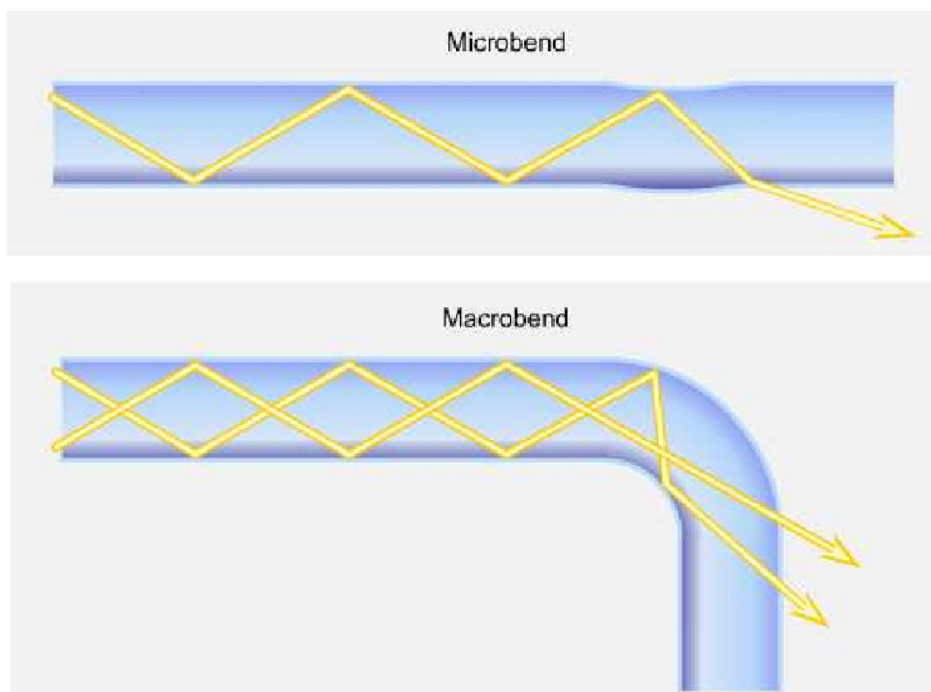
Gambar. 69

Chromatic dispersion terjadi ketika beberapa panjang gelombang suatu cahaya melakukan perjalanan pada kecepatan yang sedikit berbeda melalui sebuah gelas dan melakukan seperti panjang gelombang lainnya. Idealnya, sumber cahaya LED atau laser mengeluarkan cahaya dalam satu frekuensi. Sayangnya laser, apalagi LED mengeluarkan sekumpulan cahaya dengan panjang gelombang berdekatan yang menyebabkan chromatic dispersion. Hal ini membatasi panjang dari serat optik. Jika sinyal dikirim terlalu jauh akan menyebabkan sinyal melebar,

Menyambung Perangkat dan Setting Perangkat Menggunakan Software

terpisah dan gelap ketika mencapai penerima. Penerima tidak akan mampu membedakan bit 1 dengan 0.

Penyebab utama attenuation pada kabel serat optik adalah instalasi yang tidak sesuai. Jika serat optik ditarik atau dilengkungkan terlalu ketat, akan menyebabkan patah yang kecil pada core serat optik dan membuat sinar menjadi menghambur. Menekuk serat optik terlalu kuat juga merubah sudut datang dari sinar. Kemudian sinar datang akan menjadi kurang dari sudut kritis untuk pemantulan sempurna. Hal ini menyebabkan beberapa sinar akan membias ke cladding dan hilang.

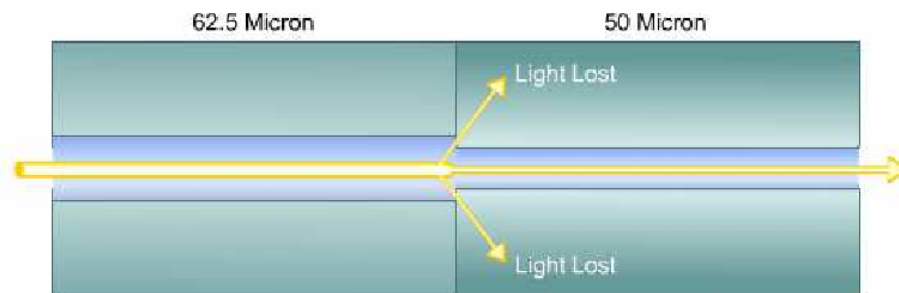


Gambar. 70

Untuk mencegah serat optik tertekuk terlalu tajam, biasanya serat optik dimasukkan kedalam pipa yang disebut interducting. Interducting jauh lebih kaku dari serat optik dan tidak dapat ditekuk terlalu tajam. Interducting melindungi serat optik, membuat lebih mudah menarik serat optik dan memastikan batas pelengkungan serat optik tidak dilalui.

Ketika serat optik telah dipasang, ujung dari serat optik harus dipotong dan dihaluskan untuk memastikan ujungnya menjadi lebih halus. Mikroskop atau instrumen test lainnya digunakan untuk memastikan ujungnya lebih tajam dan halus. Kemudian konektor dipasang secara hati-hati. Pemasangan konektor yang tidak sesuai, penyambungan yang tidak sesuai atau menyambungkan dua serat yang berbeda ukuran corenya dapat mengurangi kekuatan sinyal.

Menyambung Perangkat dan Setting Perangkat Menggunakan Software



Gambar. 71

Setelah kabel serat optik dan konektor terpasang, konektor dan ujung serat optik harus dijaga untuk selalu bersih. Ujung dari serat optik harus ditutup pelindung untuk mencegah kerusakan pada ujungnya. Ketika penutupnya dilepas untuk memasang kabel tersebut maka ujung serat optik harus dijaga kebersihannya. Bersihkan ujung kabel dengan kain tisu pembersih lensa yang diberi alkohol isopropyl murni. Port serat optik pada switch atau router juga harus dibersihkan. Ujung yang kotor dapat menyebabkan hilangnya sinyal yang menuju penerima.

Sebelum menggunakan kabel serat optik, ujilah kabel tersebut untuk memastikan sinyal dapat diterima dengan baik. Ketika merencanakan jalur serat optik, hitunglah kehilangan energi yang masih dapat ditoleransi. Hal tersebut disebut optical link loss budget. Alat ukur yang digunakan untuk menguji serat optik adalah Optical Loss Meter dan Optical Time Domain Reflectometers (OTDR). OTDR memiliki kelebihan untuk menguji serat optik lebih lanjut dan dapat digunakan untuk mengatasi masalah pada serat optik.

MENGUJI WIDE AREA NETWORK

Tujuan Pemelajaran

Setelah mempelajari kegiatan belajar ini peserta diklat mampu menjelaskan pengujian Wide Area Network dan alat-alat yang dibutuhkan.

Uraian materi

1. Spectrum Analyzer

Alat ini digunakan untuk mengetahui spektrum frekuensi yang telah digunakan oleh jaringan WaveLAN lainnya. Dengan alat ini juga dapat diketahui apakah channel yang kita gunakan sesuai dengan alokasi frekuensi yang seharusnya.

2. OTDR (Optical Time Domain Reflectometers)

Alat ini digunakan untuk menguji serat optik. Dengan alat ini dapat diketahui apakah sinyal serat optik dapat diterima dengan baik oleh penerima. Alat ini juga dapat menghitung kehilangan energi yang didapat dari serat optik

3. Loss Power Meter

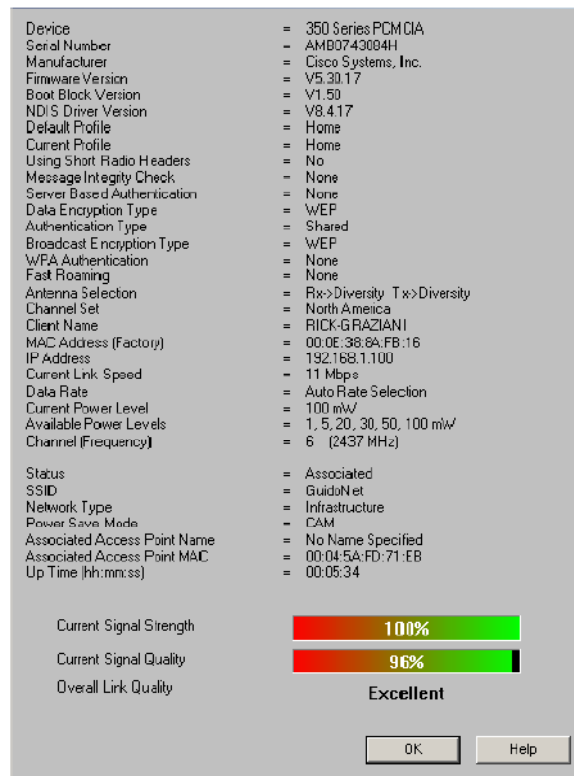
Alat ini digunakan untuk menghitung kehilangan energi yang didapat dari serat optik. Hasilnya dapat dibandingkan dengan teori optical link loss budget.



Gambar. 73

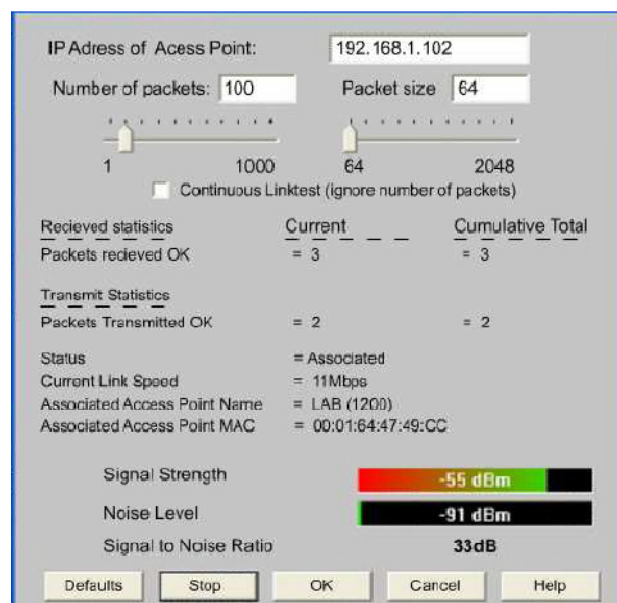
4. Software Client Utility Status

Software ini merupakan bawaan dari perangkat client WaveLAN yang kita beli. Dari software ini kita dapat melihat kekuatan sinyal dan kualitas sinyal.



5. Software Link Test

Software ini juga merupakan bawaan dari perangkat client WaveLAN. Dengan software ini kita dapat mengukur level noise yang didapat pada sebuah jaringan WaveLAN.



Gambar. 75