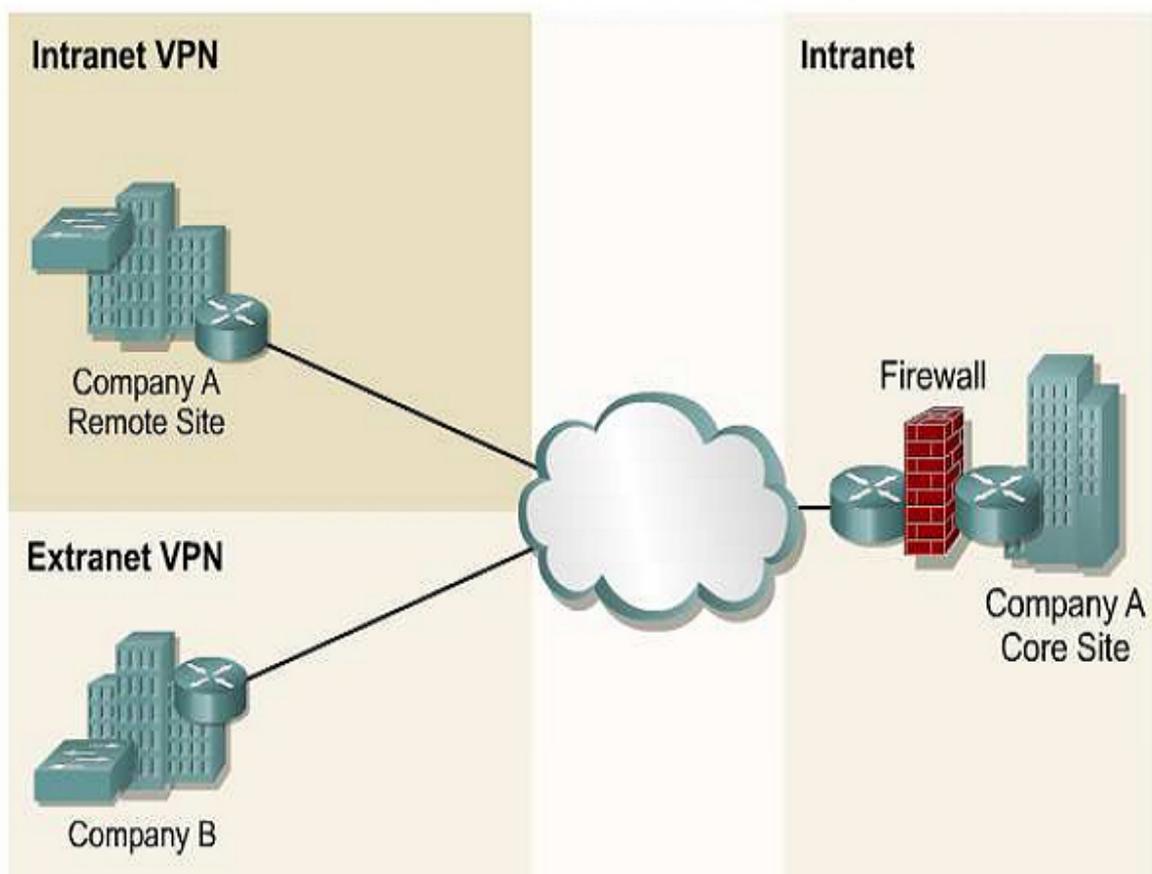


KODE MODUL

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

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

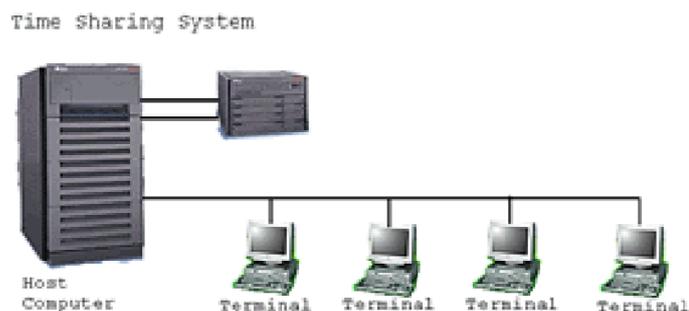
Tujuan Kegiatan Pembelajaran

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

Uraian Materi

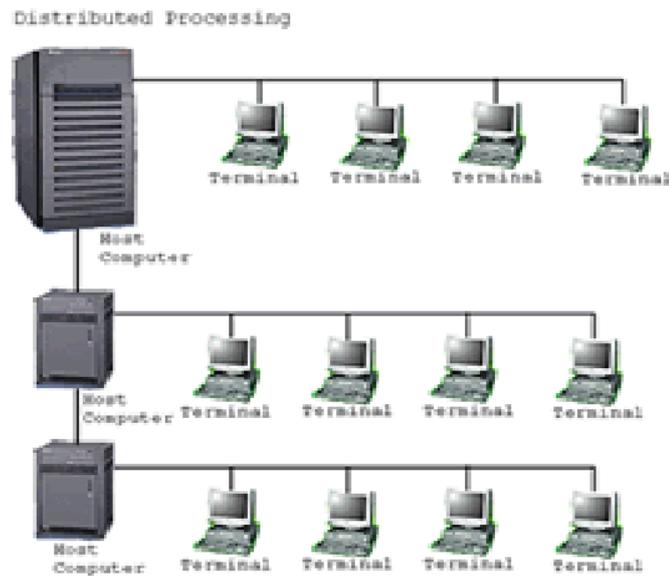
1. Latar Belakang dan Sejarah Jaringan

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.

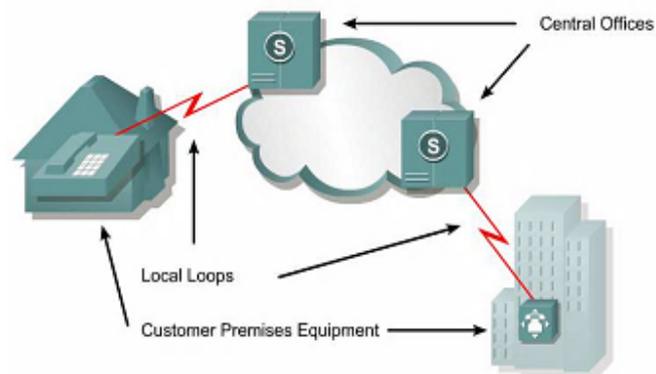
Konsep Dasar Jaringan WAN

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.

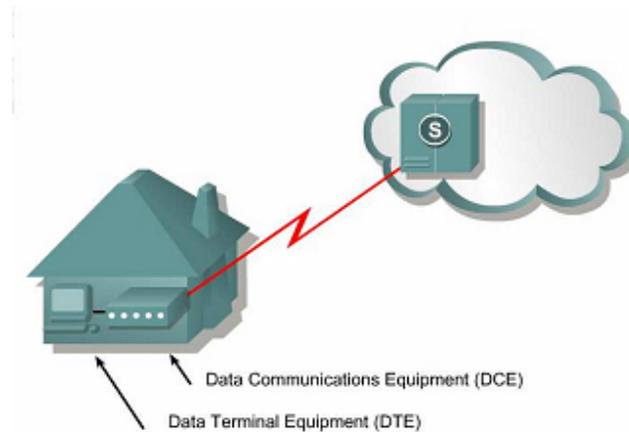
Satu perbedaan utama LAN dengan WAN adalah organisasi harus berlangganan kepada penyedia jaringan dari perusahaan penyedia jaringan yang ada. Sebuah WAN menggunakan jalur data untuk membawa data menuju ke internet dan menghubungkan lokasi–lokasi perusahaan yang terpisah–pisah. Telepon dan layanan data 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

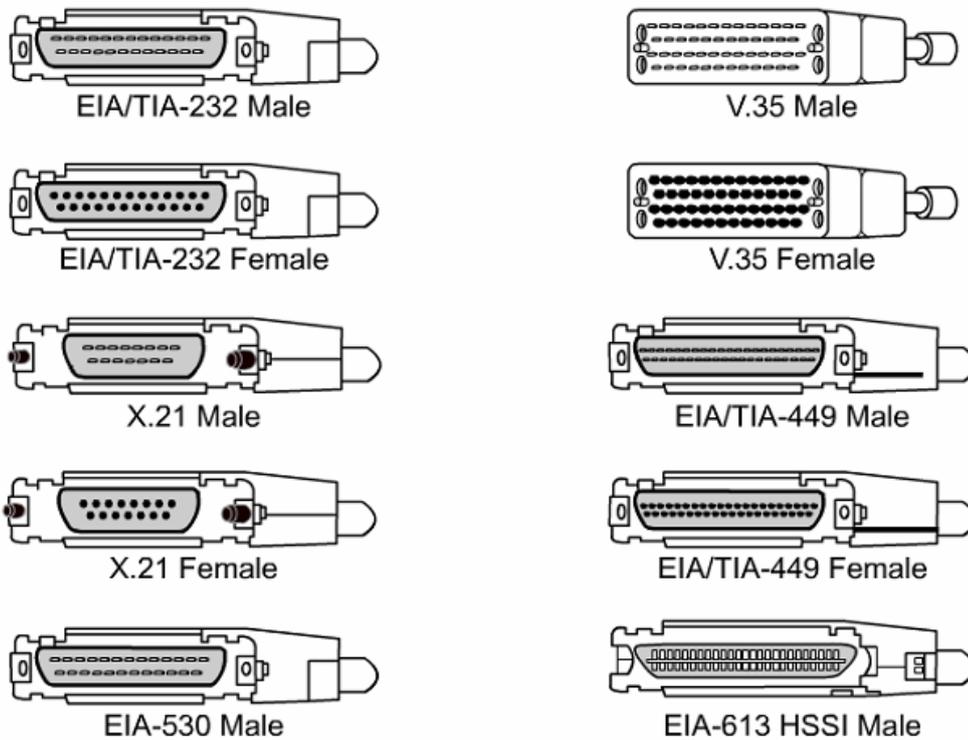
Acronym	Organization
ITU-T (was CCITT)	International Telecommunication Union Telecommunication Standardization Sector, formerly the Consultative Committee for International Telegraph and Telephone
ISO	International Organization for Standardization
IETF	Internet Engineering Task Force
EIA	Electronic Industries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

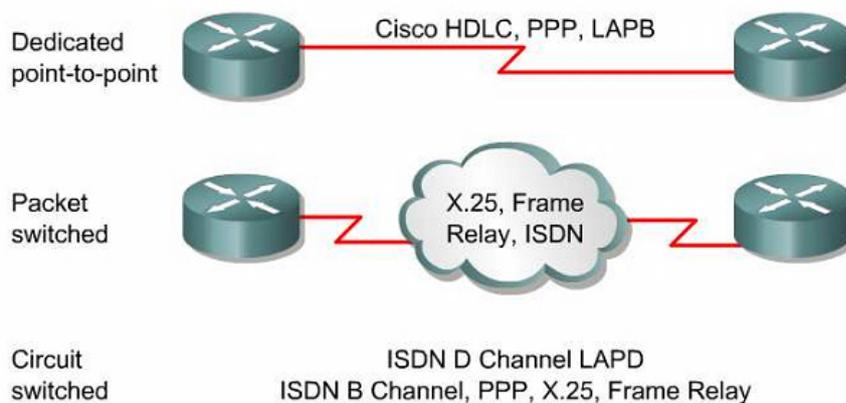
Layer 2

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



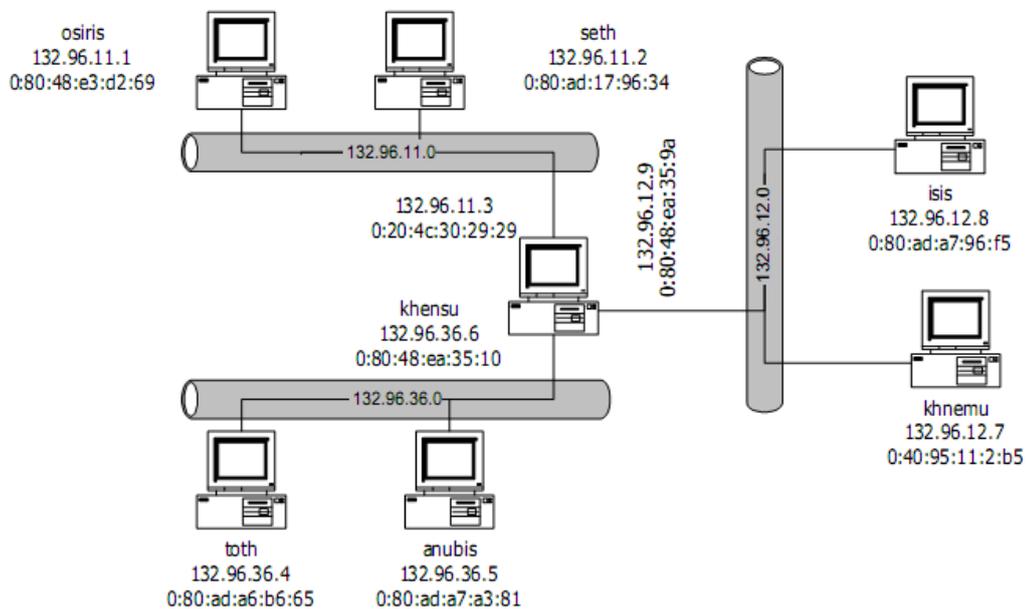
Data link layer menjelaskan bagaimana data dienkapsulasi untuk transmisi ke remote site, dan mekanisme untuk pengiriman yang menghasilkan frame. Ada bermacam-macam teknologi yang digunakan seperti ISDN, Frame Relay atau Asynchronous Transfer Mode (ATM). Protokol ini menggunakan dasar mekanisme framing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



4. Dasar-dasar Routing

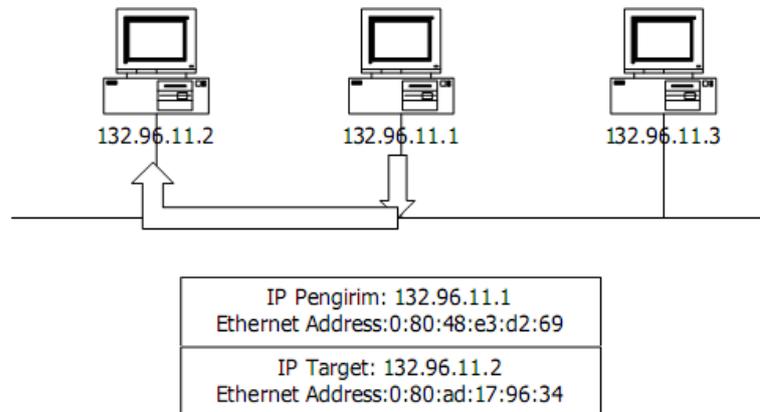
a. Routing Langsung dan Tidak Langsung

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.

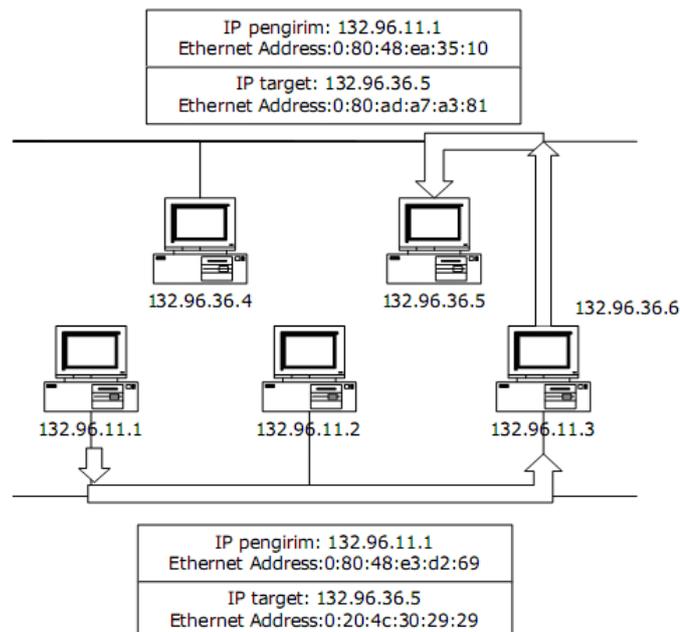


Gambar diatas memperlihatkan jaringan TCP/IP yang menggunakan teknologi Ethernet. Pada jaringan tersebut host osiris mengirimkan data ke host seth, alamat tujuan datagram adalah ip address host seth dan alamat sumber datagram adalah ip address host osiris. Frame yang dikirimkan oleh host osiris juga 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 merupakan 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

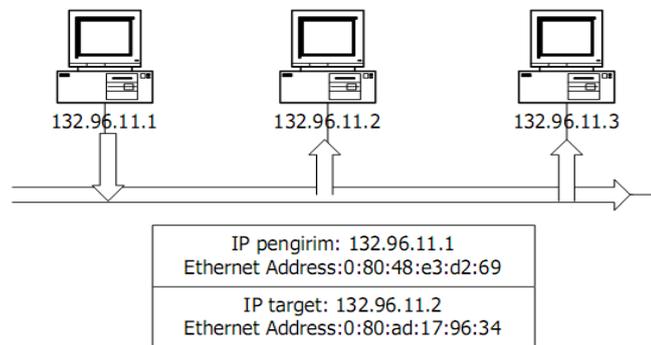
Agar dapat mengirimkan datagram ke host B, host A perlu mengisi cache ARP dengan entri host B. Karena cache ARP tidak dapat digunakan untuk menerjemahkan IP address host BB menjadi alamat Ethernet, maka host A harus melakukan dua hal yaitu:

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.

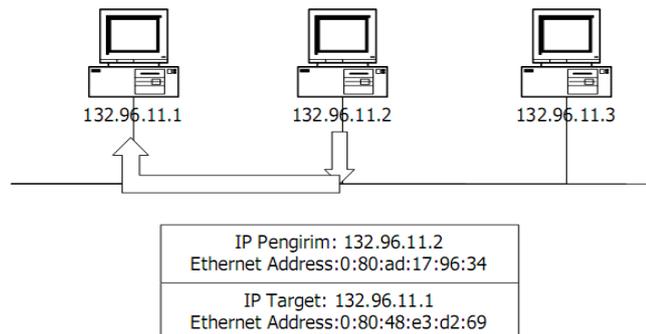
Menempatkan datagram IP yang hendak dikirim dalam antrian.

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.

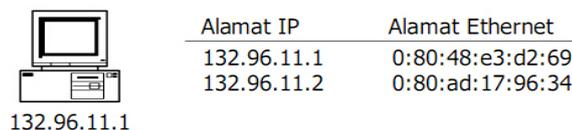
Konsep Dasar Jaringan WAN



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

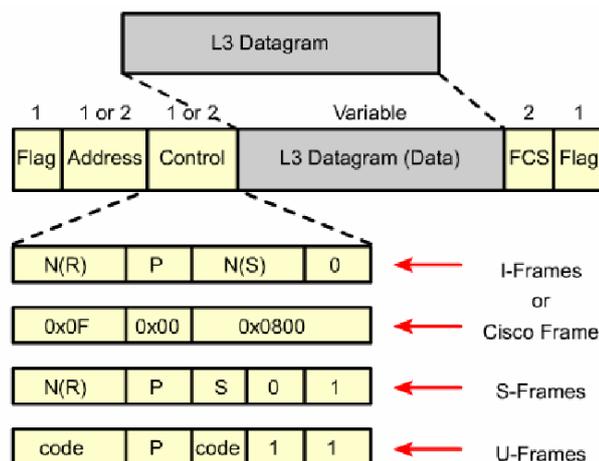
Konsep Dasar Jaringan WAN

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.

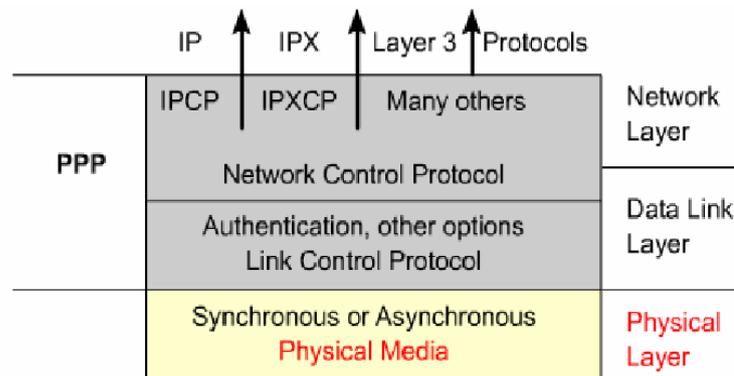


HDLC dapat digunakan untuk protokol point-to-point yang dapat digunakan pada leased line diantara dua perangkat dengan merk sejenis. Ketika berkomunikasi dengan perangkat dengan merk yang berbera maka dapat menggunakan PPP.

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:

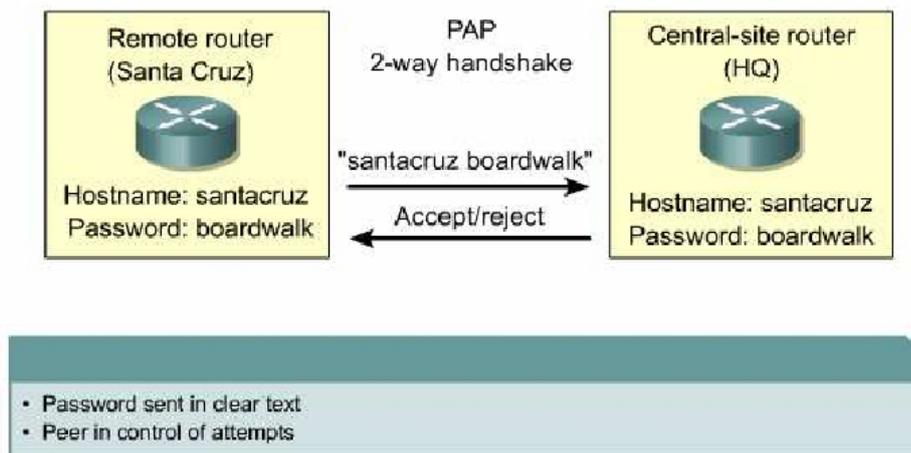
- Fase Pembangunan Jalur, pada fase ini perangkat PPP mengirim LCP frame untuk mengkonfigurasi dan mengetes jalur data. Frame LCP berisi configuration option field yang memungkinkan perangkat untuk menegosiasikan pilihan yang digunakan seperti maksimum transmission unit (MTU), kompresi dari beberapa 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.

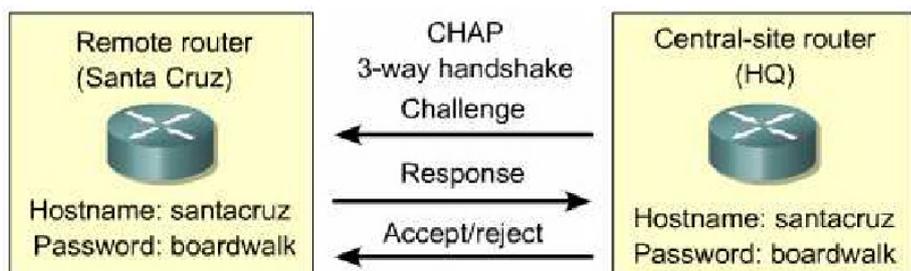
PAP menyediakan metode sederhana untuk meremote node untuk mengidentifikasi pembangunan, menggunakan two way handshake. Setelah jalur PPP dibangun, username/password secara terus menerus dikirim dari node tujuan melalui jalur sampai

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 Diggest 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 melewatkan 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.