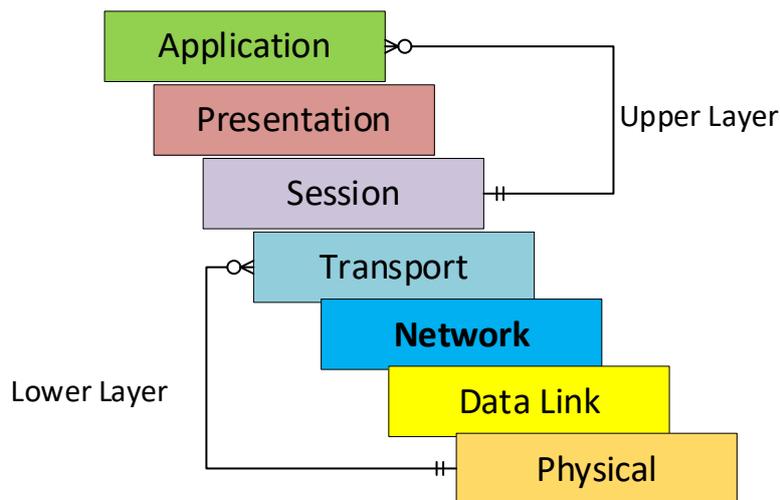


MERANCANG LAPISAN JARINGAN, ALGORITMA ROUTING, ALGORITMA KONTROL KEMACETAN, INTERNETWORK

A. MERANCANG LAPISAN JARINGAN

Lapisan Jaringan (Network Layer)

Lapisan jaringan atau Network Layer adalah merupakan lapisan ketiga dari urutan bawah dalam model lapisan OSI, berada dibawah lapisan transport dan diatas lapisan Data Link. Lapisan ini termasuk kedalam lower layer. Tugas utama lapisan jaringan adalah menyediakan fungsi routing, sehingga paket dapat dikirim keluar dari segment network local ke suatu tujuan yang berbeda pada suatu network lain. IP atau Internet Protokol dan IPX atau Internet Packet eXchange pada umumnya digunakan pada lapisan ini. Perusahaan Novell telah memprogram protocol menjadi beberapa jenis, yaitu: SPX atau Sequence Packet Exchange dan NCP atau Netware Core Protocol. Netware merupakan jenis protocol yang telah dimasukkan kedalam sistem operasi.



Gambar 1. Lapisan OSI

Lapisan ini bertanggung jawab pada sebuah internetwork dan pengalamatan. Pengalamatan yang dilakukan yaitu pengalamatan logis (logical address) yaitu IP Address dan Device utama pada layer ini adalah Router. Pada sebuah router, ketika sebuah paket diterima di sebuah interface router, alamat IP tujuan akan diperiksa. Jika paket tersebut tidak ditujukan untuk router, maka router akan mencari alamat tujuan jaringan pada tabel routing. Setelah sebuah interface untuk keluar dipilih, paket akan dikirim ke interface tersebut untuk diframe dan dikirim pada jaringan. Jika entri untuk jaringan tujuan tidak ditemukan pada tabel routing, router akan memusnahkan paket tersebut.

Jaringan menjelaskan beberapa kumpulan dari piranti terhubung bersama-sama untuk berbagi informasi dan resources dan juga saling berkomunikasi. Secara fisik, jaringan-jaringan di identifikasikan oleh segmen-segmen media transmisi dan juga oleh address-address jaringan. Berikut adalah beberapa address-address yang adalah dalam jaringan :

1. Subnetting Jaringan

Suatu jaringan yang didefinisikan oleh address jaringannya. Address Jaringan dapat mempunyai arti dalam bentuk internal maupun external. Dilihat dari luar jaringan, sebuah address jaringan dapat mengidentifikasikan dalam suatu jaringan dalam satu administrasi. Secara internal, jaringan itu sendiri dapat dibagi kedalam beberapa jaringan, dimana masing-masing mempunyai address jaringannya sendiri-sendiri, hal ini disebut dengan "subnetting".

2. Subnetting Layer Network

Dari luar jaringan ini terdapat sebagai address jaringan yang di manage oleh satu organisasi. Akan tetapi secara internal, jaringan ini mempunyai banyak subnet-subnet. Setiap subnet tidak dapat berkomunikasi satu sama lain, akan tetapi dengan router-router semua komputer dapat melakukan komunikasi satu sama lain antar jaringan. Router-router yang menghubungkan jaringan - jaringan dan segmen jaringan dengan address - address yang berbeda.

3. Address Layer Network

Pada Layer Data Link, address - address mengidentifikasikan masing - masing piranti fisik. Kemampuan untuk melakukan routing antar jaringan tergantung identifikasi jaringan - jaringan. Hal ini bisa dilakukan dengan addressing jaringan, disebut juga Logical Addresses untuk membedakan dari address fisik yang dipakai pada layer Data Link. Logical Addresses mengidentifikasikan kedua segmen address jaringan, dan address piranti itu sendiri, walaupun piranti mempunyai address fisik yang sama.

Ada beberapa jenis paket yang digunakan dalam lapisan jaringan, yaitu:

1. Data packet digunakan untuk mengangkut data pengguna melalui internetwork, dan protokol yang digunakan untuk mendukung lalu lintas data tersebut disebut routed protokol. Contoh routed protokol adalah IP dan IPX
2. Route Update packet digunakan untuk meng-update router tetangga tentang jaringan yang terhubung dalam internetwork. protokol yang mengirimkan paket update rute disebut protokol routing, contoh RIP, EIGRP dan OSPF. Routing update packets digunakan untuk membantu membangun dan mempertahankan tabel routing pada setiap router. Tabel routing yang digunakan dalam router mencakup informasi berikut
3. Network addresses, spesifik protokol untuk pengalamatan network. Sebuah router harus mempertahankan tabel routing secara individu karena setiap protokol routing melacak jaringan dengan skema pengalamatan yang berbeda.
4. Interface, menunjukkan interface mana yang digunakan oleh paket sebagai jalan keluar untuk menuju ke spesifik network.

5. Metric, merupakan Jarak ke network remote. Umumnya, pada routing protokol yang berbeda menggunakan metode yang berbeda untuk menghitung jarak ini

Lapisan Jaringan mempunyai fungsi sebagai berikut:

1. Menerjemahkan alamat / address logikal di jaringan beserta nama ke bentuk address fisik, yaitu menerjemahkan nama komputer menjadi MAC address.
2. Bertanggung jawab untuk addressing, menetapkan rute pengiriman, penanganan permasalahan jaringan seperti: packet switching, data congestion, dan routing
3. Jika router tidak dapat mengirimkan frame data dalam ukuran yang dikirim kode sumber, network layer menanganinya dengan memecah data ke dalam unit yang lebih kecil.
4. Pada mesin penerima, network layer akan memadukan ulang data yang dipecah sebelumnya

Berikut adalah beberapa komponen dari lapisan jaringan, yaitu:

1. NIC
NIC (Network Interface Card) adalah peralatan yang langsung berhubungan dengan komputer dan didesain agar komputer dapat saling berkomunikasi. NIC juga menyediakan akses ke media fisik jaringan, dimana setiap bit bit data seperti tegangan listrik, arus, gelombang elektromagnetik, besaran fisik lainnya di bentuk dan selanjutnya akan di tentukan oleh NIC. NIC adalah contoh perangkat yang bekerja pada layer pertama atau layer physical.
2. Repeater
Repeater merupakan salah satu contoh aktif hub, repeater merupakan alat yang dapat menerima sinyal kemudian memperkuat dan mengirimkannya kembali sinyal tersebut ke tempat lain sehingga dapat menjangkau area yang lebih luas. Repeater termasuk peralatan yang bekerja pada layer physical.
3. Hub
Merupakan peralatan yang dapat menggandakan frame data yang berasal dari salah satu komputer ke semua port yang ada pada hub tersebut. Hub di pakai pada jaringan topologi star dan bekerja pada layer data link.
4. Bridge
Bridge merupakan peralatan yang dapat menggabungkan beberapa segmen dalam sebuah jaringan. Beda halnya dengan hub, bridge dapat mempelajari MAC Address tujuan. Sehingga apabila data dikirim melalui bridge maka data tersebut akan dikirim ke komputer yang menjadi tujuannya saja. Bridge bekerja pada layer data link.
5. Switch
Switch memiliki beberapa kelebihan yaitu dalam hal forwarding method paket yang akan dilewatkan. Berikut adalah beberapa kelebihan dari switching, yaitu:
 - a. Kemampuan dari sebuah router untuk menerima data pada satu port dari satu jaringan dan mengirim nya keluar port yang lain pada jaringan lainnya.

- b. Memindahkan data antara jaringan-2 terhubung untuk mencapai tujuan akhir

B. ALGORITMA ROUTING

Routing adalah suatu protokol yang digunakan untuk mendapatkan rute dari satu jaringan ke jaringan yang lain. Rute ini, disebut dengan route dan informasi route secara dinamis dapat diberikan ke router yang lain ataupun dapat diberikan secara statis ke router lain. Seorang administrator memilih suatu protokol routing dinamis berdasarkan keadaan topologi jaringannya. Misalnya berapa ukuran dari jaringan, bandwidth yang tersedia, proses power dalam router, merek dan model dari router, dan protokol yang digunakan dalam jaringan.

Routing adalah proses dimana suatu router mem-forward paket ke jaringan yang dituju. Suatu router membuat keputusan berdasarkan IP address yang dituju oleh paket. Semua router menggunakan IP address tujuan untuk mengirim paket. Agar keputusan routing tersebut benar, router harus belajar bagaimana untuk mencapai tujuan. Ketika router menggunakan routing dinamis, informasi ini dipelajari dari router yang lain. Ketika menggunakan routing statis, seorang network administrator mengkonfigurasi informasi tentang jaringan yang ingin dituju secara manual. Jika routing yang digunakan adalah statis, maka konfigurasinya harus dilakukan secara manual, administrator jaringan harus memasukkan atau menghapus rute statis jika terjadi perubahan topologi. Pada jaringan skala besar, jika tetap menggunakan routing statis, maka akan sangat membuang waktu administrator jaringan untuk melakukan update table routing. Karena itu routing statis hanya mungkin dilakukan untuk jaringan skala kecil. Sedangkan routing dinamis bisa diterapkan di jaringan skala besar dan membutuhkan kemampuan lebih dari administrator

Untuk dapat melakukan perutean, suatu router, atau entitas apapun yang membangun routing, melakukan beberapa langkah berikut ini :

1. Mengetahui Alamat tujuan – Ke tujuan (alamat) mana sesuatu yang dirutekan dikirim?
2. Mengenali sumber-sumber informasi perutean – Dari sumber-sumber (router-router lain) mana saja suatu router dapat mempelajari jalur-jalur menuju tujuan?
3. Menemukan rute-rute – Jalur-jalur atau rute-rute mana saja yang mungkin dapat dilalui untuk mencapai alamat tujuan?
4. Memilih jalur atau rute – Memilih jalur atau rute terbaik untuk menuju alamat tujuan yang dimaksud.
5. Memelihara dan memverifikasi informasi routing – Apakah jalur-jalur ke tujuan yang telah diketahui masih berlaku dan benar?

Pada suatu sistem jaringan komputer, router mempelajari informasi routing dari sumber-sumber routing-nya yang terletak di dalam tabel routing (routing table). Router akan berpedoman pada tabel ini untuk menyatakan port mana yang digunakan mem-forward paket-paket yang ditujukan kepadanya.

1. Jika jaringan tujuan terhubung langsung dengan router, maka router sudah mengetahui port mana yang digunakan untuk mem-forward paket.
2. Jika jaringan tujuan tidak terhubung langsung dengan router, maka router harus mempelajari rute terbaik untuk mem-forward paket ke tujuan.

Static Routing dan Dynamic Routing

Secara umum mekanisme koordinasi routing dapat dipelajari oleh router dalam dua metode, yaitu :

1. Dimasukkan secara manual oleh administrator jaringan, disebut Static Routes
2. Dikumpulkan melalui proses-proses dinamis yang berjalan di jaringan, disebut sebagai Dynamic Routes.

Static Routing

Routing statik (static route) adalah pengaturan routing paling sederhana yang dapat dilakukan pada jaringan komputer. Static route adalah rute-rute ke host atau jaringan tujuan yang dimasukkan secara manual oleh administrator jaringan ke route table suatu router. Static route mendefinisikan alamat IP hop router berikutnya dan interface lokal yang digunakan untuk mem-forward paket ke tujuan tertentu (hop router berikutnya). Static route memiliki keunggulan untuk menghemat bandwidth jaringan karena static route tidak membangkitkan trafik route update untuk memberikan informasi perubahan rute yang berlaku (sah) saat ini ke router-router lain. Penggunaan routing statik dalam sebuah jaringan yang kecil tentu bukanlah suatu masalah, hanya beberapa entri yang perlu diisikan pada forwarding table di setiap router.

Namun tentu dapat dibayangkan bagaimana jika harus melengkapi forwarding table di setiap router yang jumlahnya tidak sedikit dalam jaringan yang besar. Apalagi jika untuk mengisi entri-entri di seluruh router di Internet yang jumlahnya banyak sekali dan terus bertambah setiap hari. Jadi penggunaan static route cenderung membutuhkan waktu ekstra ketika manajemen jaringan. Hal ini disebabkan karena system administrator harus secara manual meng-update route table setiap terjadi perubahan konfigurasi jaringan.

Dynamic Routing

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

Routing dinamik yang populer saat ini mengacu pada dua tipe algoritma yang dikenalkan oleh Bellman Ford dengan algoritma distance vektornya dan oleh

Dijkstra dengan algoritma link statenya. Cisco kemudian mengembangkan protocol untuk perangkat routernya yang merupakan gabungan dari kedua algoritma tersebut yang diberi nama protocol EIGRP

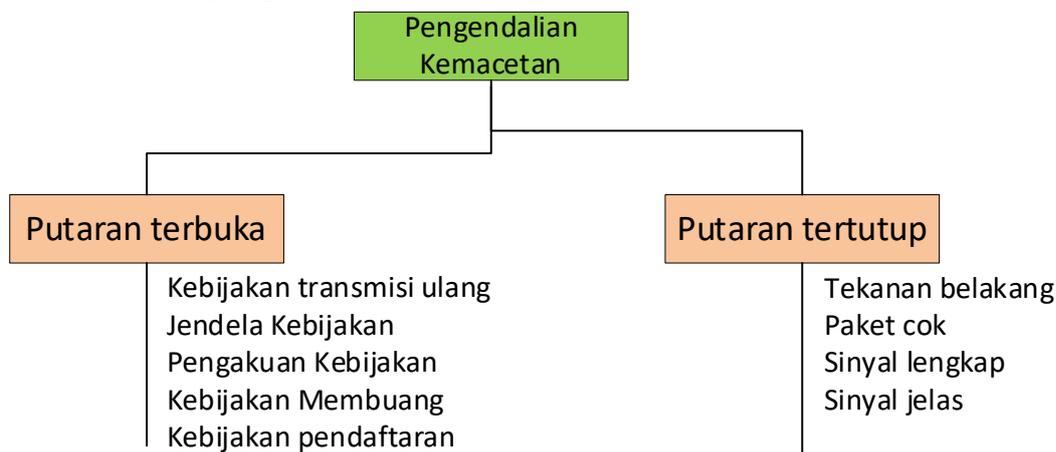
Algoritma Distance Vector

Protokol distance vector bekerja dengan memberikan router-router kemampuan untuk mempublikasikan semua rute-rute yang diketahui (router bersangkutan) keluar ke seluruh interface yang dimilikinya. Router yang secara fisik berada pada jaringan yang sama dinamakan neighbor. Jika router-router mempublikasikan rute-rute yang diketahuinya melalui seluruh interface-nya, dan seluruh neighbor menerima routing update, maka setiap router akan juga mengetahui rute-rute yang dapat dilalui ke seluruh subnet suatu jaringan.

C. ALGORITMA KONTROL KEMACETAN

1. Pengendalian Kemacetan

Pengendalian kemacetan mengacu pada teknik dan mekanisme yang baik dapat mencegah kemacetan, sebelum itu terjadi, atau menghapus kemacetan setelah terjadi. Secara umum, kita dapat mekanisme pengendalian kemacetan kedalam dua kategori besar yaitu putaran terbuka pengendalian kemacetan (pencegahan) dan putaran tertutup pengendalian kemacetan (pengangkatan) seperti yang ditunjukkan pada Gambar 1.



Gambar 2. Pengendalian Kemacetan

a. Open-Loop Congestion Control (Putaran terbuka pengendalian kemacetan)

Dalam pengendalian kemacetan terbuka, kebijakan yang diterapkan adalah untuk mencegah sebelum terjadi kemacetan. Dalam mekanisme ini, pengendalian kemacetan ditangani oleh sumber yang baik atau tujuan.

1) Retransmission Policy (Kebijakan retransmisi)

Retransmisi kadang-kadang tidak dapat dihindari. Jika pengirim merasa bahwa paket yang dikirim hilang atau rusak, paket perlu dipancarkan kembali. Retransmisi secara umum dapat meningkatkan kemacetan pada jaringan. Namun, kebijakan penyiaran baik dapat mencegah kemacetan. Kebijakan retransmisi dan waktu retransmisi harus dirancang untuk mengoptimalkan efisiensi dan pada saat yang sama mencegah kemacetan. Sebagai contoh, kebijakan penyiaran yang digunakan oleh TCP (dijelaskan kemudian) dirancang untuk mencegah atau meringankan kemacetan.

2) Window Policy (Jendela Kebijakan)

Jenis jendela pengirim juga dapat mempengaruhi kemacetan. Jendela pengulangan selektif lebih baik dari jendela-Go Back-N untuk pengendalian kemacetan. Di N-Go Back jendela, ketika waktu untuk kali paket keluar, mungkin beberapa paket membenci, meskipun kemungkinan beberapa telah tiba aman dan suara pada penerima. duplikasi ini mungkin membuat kemacetan parah. Jendela Ulangi Selektif, di sisi lain, mencoba untuk mengirim paket khusus yang telah hilang atau rusak

3) Acknowledgment Policy (Pengakuan Kebijakan)

Kebijakan pengakuan yang dikenakan oleh penerima juga dapat mempengaruhi kemacetan. Jika penerima tidak mengakui setiap paket yang diterima, hal itu mungkin memperlambat pengirim dan membantu mencegah kemacetan. Beberapa pendekatan yang digunakan dalam kasus ini. penerima mungkin mengirimkan pemberitahuan hanya jika memiliki paket untuk dikirim atau waktu khusus berakhir. Penerima dapat memutuskan untuk mengakui hanya paket N pada suatu waktu. Kita perlu tahu bahwa pengakuan juga merupakan bagian dari beban dalam jaringan. Mengirim lebih sedikit pengakuan berarti memaksakan beban sedikit pada jaringan.

4) Discarding Policy (Kebijakan membuang)

Kebijakan membuang baik oleh arah dapat mencegah kemacetan dan pada saat yang sama tidak dapat membahayakan integritas transmisi. Misalnya, dalam transmisi audio, jika kebijakan tersebut adalah untuk membuang paket kurang sensitif ketika kemacetan yang mungkin terjadi, yang kualitas suara masih ada dan kemacetan dicegah atau dikurangi.

5) Admission Policy (Kebijakan Pendaftaran)

Suatu kebijakan masuk, yang merupakan kualitas mekanisme-service, juga bisa mencegah kemacetan di jaringan virtual-circuit. Tombol dalam aliran pertama diperiksa dulu kebutuhan sumber daya aliran sebelum mengakui ke jaringan. arah A dapat menyangkal membangun virtual sirkuit koneksi jika ada kemacetan dalam jaringan atau jika ada kemungkinan masa depan kemacetan.

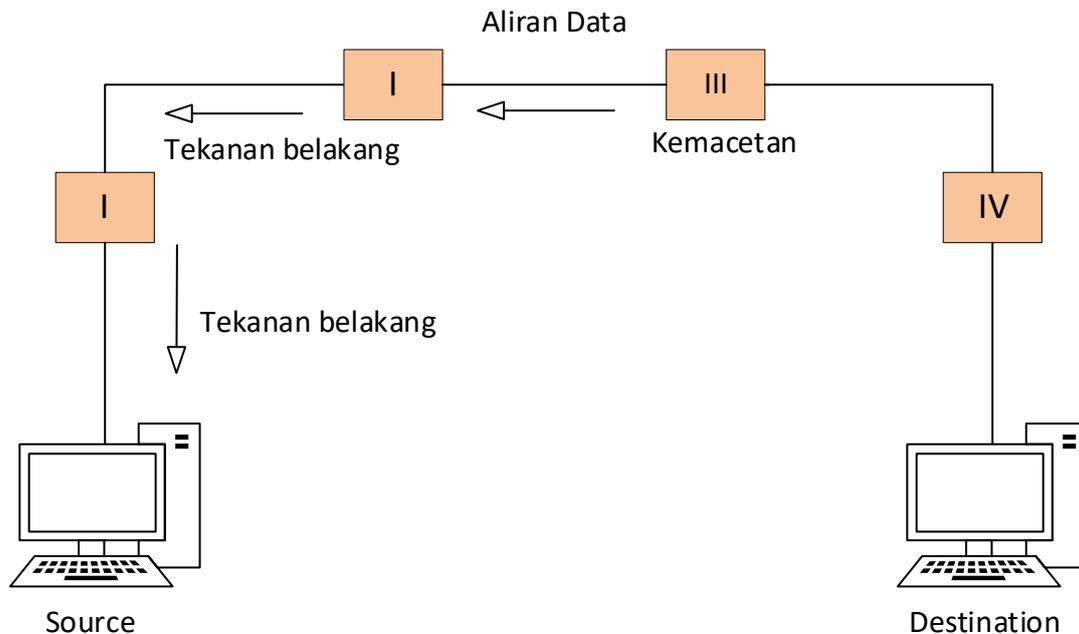
b. Closed-Loop Congestion Control (Putaran tertutup pengendalian kemacetan)

Mekanisme pengendalian kemacetan putaran tertutup mencoba untuk mengurangi kemacetan setelah terjadi . Beberapa mekanisme telah digunakan oleh protokol yang berbeda. Kita menjelaskan beberapa di sini.

1) Backpressure (tekanan belakang)

Teknik tekanan belakang mengacu pada mekanisme pengendalian kemacetan di mana simpul padat berhenti menerima data dari node hulu langsung atau node. Ini dapat menyebabkan node atau node hulu atau menjadi sesak, dan mereka, pada gilirannya, menolak data dari node hulu atau node. Dan seterusnya. Tekanan belakang adalah node-ke-node pengendalian kemacetan yang dimulai dengan node dan menjalar, dalam arah yang berlawanan dari aliran data ke sumbernya. Teknik tekanan belakang dapat diterapkan hanya untuk virtual circuit jaringan, di mana setiap node node hulu tahu dari mana aliran data coming.

Metode Back Pressure untuk mengurangi kemacetan



Gambar 3. Metode Back Pressure

Node III dalam gambar memiliki data masuk lebih dari itu bisa menangani. Ini tetes beberapa paket dalam penyangah masuk dan menginformasikan node II untuk memperlambat. Node II, pada gilirannya, mungkin sesak karena memperlambat aliran data keluar. Jika node II padat, menginformasikan node I untuk memperlambat, yang pada gilirannya dapat menciptakan kemacetan. Jika demikian, node I menginformasikan sumber data untuk memperlambat. Ini, dalam waktu mengurangi kemacetan. Catatan sebuah tekanan bahwa pada node III dipindahkan mundur ke sumber untuk menghapus kemacetan.

2) Choke Packet (paket cok)

Paket cok adalah paket dikirim oleh sebuah node sumber untuk menginformasikan kemacetan. Perhatikan perbedaan antara tekanan belakang dan metode paket cok. Dalam tekanan belakang , peringatan ini dari satu node ke node hulu, meskipun peringatan akhirnya mencapai stasiun sumber. Dalam metode paket cok, peringatan ini dari arah yang telah mengalami kemacetan ke stasiun sumber langsung. Tingkat menengah node melalui paket bepergian tidak peringatan. Kita telah melihat contoh dari jenis pengaturan dalam ICMP. Ketika suatu arah di Internet membanjiri dengan datagram IP, mungkin membuang beberapa dari mereka, tetapi menginformasikan sumber tuan rumah, menggunakan sumber memuaskan pesan ICMP. Pesan peringatan pergi langsung ke stasiun sumber, arah menengah, dan tidak mengambil tindakan apapun.

3) Implicit Signaling (sinyal lengkap)

Dalam sinyal lengkap, tidak ada komunikasi antara node tersumbat atau node dan sumbernya. Sumber itu menduga bahwa ada kemacetan di suatu tempat di jaringan dari gejala lainnya. Sebagai contoh, ketika sumber mengirim beberapa paket dan ada tidak ada pengakuan untuk sementara waktu, satu asumsi adalah bahwa jaringan padat. keterlambatan dalam menerima pengakuan adalah diartikan sebagai kemacetan dalam jaringan, sedangkan sumber harus memperlambat. Kita akan melihat jenis sinyal ketika kita membahas TCP pengendalian kemacetan dalam bab ini.

4) Explicit Signaling (sinyal jelas)

Simpul yang mengalami kemacetan secara jelas dapat mengirim sinyal ke sumber atau tujuan. Metode sinyal jelas, bagaimanapun adalah berbeda dari metode paket cok. Dalam metode paket cok, sebuah paket yang terpisah digunakan untuk tujuan ini dalam Metode sinyal jelas, sinyal yang termasuk dalam paket yang membawa data. Sinyal jelas, seperti yang akan kita lihat dalam pengendalian kemacetan di bingkai beranting, dapat terjadi baik di depan atau arah belakang. Sinyal Mundur Sedikit dapat diatur dalam paket bergerak dalam arah berlawanan untuk kemacetan. Bit ini dapat memperingatkan sumber yang ada kemacetan dan bahwa perlu untuk memperlambat untuk menghindari pembuangan paket. Sinyal bagian depan Sedikit dapat diatur dalam paket bergerak dalam arah kemacetan. Bit ini dapat memperingatkan tujuan bahwa ada kemacetan. Penerima dalam hal ini dapat menggunakan kebijakan, seperti memperlambat pengakuan, untuk meringankan kemacetan.

2. Kemacetan TCP (Example)

Kita sekarang menunjukkan bagaimana TCP menggunakan kontrol kongesti untuk menghindari kemacetan atau mengurangi kemacetan pada jaringan.

a. Kontrol Kemacetan di TCP

Kita sekarang menunjukkan bagaimana TCP menggunakan pengendalian kemacetan untuk menghindari kemacetan atau mengurangi kemacetan pada jaringan

b. Jendela Kemacetan

Kita mengatakan bahwa ukuran jendela pengirim ditentukan oleh faedah ruang penyangah dapat di terima ($rwnd$). Dengan kata lain, kita berasumsi bahwa hanya penerima yang dapat mendikte pengirim ukuran jendela pengirim. Kita benar-benar diabaikan entitas lain di sini-jaringan. Jika jaringan tidak bisa mengirimkan data secepat mereka dibuat oleh pengirim, maka harus memberitahu pengirim untuk memperlambat. Dengan kata lain, di samping penerima, jaringan adalah entitas kedua yang menentukan ukuran jendela pengirim. Hari ini, ukuran jendela pengirim ditentukan tidak hanya oleh penerima tetapi juga oleh kemacetan dalam jaringan. Pengirim memiliki dua potongan informasi: ukuran jendela penerima-diiklankan dan kemacetan ukuran jendela. Ukuran sebenarnya dari jendela adalah minimum dua. Ukuran sebenarnya jendela = minimum ($rwnd$, $cwnd$).

c. Kebijakan Kemacetan

Kebijakan umum TCP untuk penanganan kemacetan didasarkan pada tiga fase: start lambat, penghindaran kemacetan, dan deteksi kemacetan. Pada fase lambat-start, pengirim mulai dengan tingkat penuluran sangat lambat, tetapi meningkatkan laju cepat untuk mencapai ambang pintu. Ketika ambang batas tersebut tercapai, kecepatan data dikurangi untuk menghindari kemacetan. Akhirnya jika kemacetan terdeteksi, pengirim akan kembali ke awal lambat atau menghindari kemacetan fase didasarkan pada bagaimana kemacetan terdeteksi. mulai lambat: Eksponensial Meningkatkan Salah satu algoritma yang digunakan dalam TCP pengendalian kemacetan ini disebut mulai lambat. Algoritma ini didasarkan pada gagasan bahwa ukuran kemacetan jendela ($cwnd$) dimulai dengan satu ukuran segmen maksimum (MSS). MSS ini ditentukan selama pembentukan koneksi dengan menggunakan pilihan dari nama yang sama. ukuran jendela akan bertambah satu setiap kali MSS pengakuan diterima. Sebagai nama menyiratkan, jendela mulai perlahan, tetapi tumbuh secara eksponensial. Untuk menampilkan ide, mari kita lihat Gambar 24.8. Perhatikan bahwa kita telah menggunakan tiga penyederhanaan untuk membuat diskusi lebih dimengerti. Kita telah menggunakan nomor segmen bukan darinomor byte (seolah-olah setiap segmen hanya berisi 1 byte). Kita telah mengasumsikan bahwa $rwnd$ jauh lebih tinggi daripada $cwnd$, sehingga ukuran jendela pengirim selalu sama $cwnd$. Kita telah mengasumsikan bahwa setiap segmen diakui secara individual. Pengirim dimulai dengan $cwnd = 1MSS$. Ini berarti bahwa pengirim dapat mengirim hanya satu segmen. Setelah menerima pengakuan untuk segmen 1, ukuran jendela kemacetan meningkat sebesar

1, yang berarti cwnd yang sekarang 2. Sekarang dua segmen lebih dapat dikirim. Ketika setiap pengakuan diterima, ukuran jendela yang meningkat sebesar 1 MSS. Ketika semua tujuh segmen diakui, cwnd = 8.

d. Menghindari Kemacetan

Untuk menghindari kemacetan, protokol Frame Relay menggunakan 2 bit dalam bingkai secara eksplisit memperingatkan sumber dan tujuan adanya kemacetan. BECN Pemberitahuan mundur kongesti eksplisit (BECN) sedikit memperingatkan pengirim kongesti dalam jaringan. Orang mungkin bertanya bagaimana hal ini dilakukan karena bingkai perjalanan jauh dari pengirim. Bahkan, ada dua metode: Switch dapat menggunakan respon frame dari penerima (full-duplex mode), atau tombol dapat menggunakan standar konektortion (DLCI = 1023) untuk mengirim frame khusus untuk tujuan tertentu. Pengirim dapat merespon peringatan ini hanya dengan mengurangi tingkat data.

c. INTERNETWORK

Internet merupakan kepanjangan dari interconnected networking, yang mempunyai arti hubungan komputer dengan berbagai tipe yang membentuk system jaringan yang mencakup seluruh dunia (jaringan komputer global) dengan melalui jalur telekomunikasi seperti telepon, radio link, satelit dan lainnya. Istilah INTERNET berasal dari bahasa Latin inter, yang berarti "antara". Internet adalah sebuah dunia maya jaringan computer (interkoneksi) yang terbentuk dari miliaran komputer di dunia. Internet merupakan hubungan antar berbagai jenis komputer dan jaringan di dunia yang berbeda system operasi maupun aplikasinya di mana hubungan tersebut memanfaatkan kemajuan media komunikasi (telepon dan satelit) yang menggunakan protokol standar dalam berkomunikasi.

FUNGSI INTERNET

Internet awal mulanya yaitu sesuatu proyek yang diciptakan untuk keperluan pribadi sesuatu negara. tetapi sekarang ini telah jadi halayak umum. seluruh orang telah bisa menggunakan internet dengan umum. nyaris seluruh orang juga telah bisa mengoperasikan internet. Adapula saat ini internet yang telah bisa di nikmati dengan gratis yang disediakan oleh umum.

Quarterman dan **Mitchell** membagi kegunaan internet dalam empat kategori, yaitu:

1. Internet sebagai media komunikasi, merupakan fungsi internet yang paling banyak digunakan dimana setiap pengguna internet dapat berkomunikasi dengan pengguna lainnya dari seluruh dunia.
2. Media pertukaran data, dengan menggunakan email, newsgroup, ftp dan www (world wide web – jaringan situs-situs web) para pengguna internet di seluruh dunia dapat saling bertukar informasi dengan cepat dan murah.
3. Media untuk mencari informasi atau data, perkembangan internet yang pesat, menjadikan www sebagai salah satu sumber informasi yang penting dan akurat.
4. Fungsi komunitas, internet membentuk masyarakat baru yang beranggotakan para pengguna internet dari seluruh dunia. Dalam komunitas ini pengguna internet dapat berkomunikasi, mencari informasi, berbelanja, melakukan transaksi bisnis, dan sebagainya. Karena sifat internet yang mirip dengan dunia kita sehari-hari maka internet sering di sebut sebagai cyberspace atau virtual world (dunia maya).

FASILITAS INTERNET

Internet sebenarnya mengacu kepada istilah untuk menyebut sebuah jaringan, bukannya suatu aplikasi tertentu. Karena-nya, internet tidaklah memiliki manfaat apa-apa tanpa adanya aplikasi yang sesuai. Internet menyediakan beragam aplikasi yang dapat digunakan untuk berbagai keperluan. Setiap aplikasi berjalan diatas sebuah protokol tertentu. Istilah "protokol" di internet mengacu pada satu set aturan yang mengatur bagaimana sebuah aplikasi ber-komunikasi dalam suatu jaringan. Sedangkan software aplikasi yang berjalan diatas sebuah protokol disebut sebagai aplikasi client. Di bagian ini, kita akan berkenalan secara sepintas dengan aplikasi-aplikasi yang paling sering dimanfaatkan oleh pengguna internet.

WORLD WIDE WEB (www)

Dewasa ini, WWW atau yang sering disebut sebagai "web" saja adalah merupakan aplikasi internet yang paling populer. Demikian populernya hingga banyak orang yang keliru mengidentikkan web dengan internet. Secara teknis, web adalah sebuah sistem dimana informasi dalam bentuk teks, gambar, suara, dan lain-lain yang tersimpan dalam sebuah internet webserver dipresentasikan dalam bentuk hypertext. Informasi di web dalam bentuk teks umumnya ditulis dalam format HTML (Hypertext

Markup Language). Untuk membuat Hypertext, dikembangkan sebuah bahasa pemrograman khusus yang memungkinkan pengikatan alamat WWW atau file dalam sebuah dokumen. Sesuai dengan fungsinya, bahasa pemrograman ini disebut Hypertext Mark up Language (HTML). File ini biasanya berextension *.html. Agar file yang berisi Hypertext ini bisa dikirimkan, diperlukan protokol pengiriman data yang spesifik yang disebut HyperText Transfer Protocol (HTTP). Untuk menemukan setiap hubungan Hypertext digunakan Uniform Resource Locator (URL). Karena itu, halaman WWW juga disebut dokumen URL.

ELECTRONIC MAIL [EMAIL]

Email atau kalau dalam istilah Indonesia, surat elektronik, adalah aplikasi yang memungkinkan para pengguna internet untuk saling berkirim pesan melalui alamat elektronik di internet. Para pengguna email memiliki sebuah mailbox (kotak surat) elektronik yang tersimpan dalam suatu mailserver. Suatu Mailbox memiliki sebuah alamat sebagai pengenal agar dapat berhubungan dengan mailbox lainnya, baik dalam bentuk penerimaan maupun pengiriman pesan.

TELNET

Telnet adalah program yang memungkinkan komputer kita menjadi terminal dari komputer lain di INTERNET. Telnet memungkinkan kita untuk masuk (log-in) sebagai pemakai komputer jarak jauh dan menjalankan program komputer layanan yang ada dikomputer tersebut.

FILE TRANSFER PROTOCOL [FTP]

Fasilitas ini memungkinkan para pengguna internet untuk melakukan pengiriman (upload) atau menyalin (download) sebuah file antara komputer lokal dengan komputer lain yang terhubung dalam jaringan internet. Protokol standar yang digunakan untuk keperluan ini disebut sebagai File Transfer Protocol (FTP) FTP umumnya dimanfaatkan sebagai sarana pendukung untuk kepentingan pertukaran maupun penyebaran sebuah file melalui jaringan internet. FTP juga dimanfaatkan untuk melakukan proses upload suatu halaman web ke webserver agar dapat diakses oleh pengguna internet lainnya.

GOPHER

Internet menyediakan banyak informasi yang dapat diakses

penggunanya lewat sistem menu. Seorang pengguna INTERNET dihadapkan pada sebuah menu yang bercabang-cabang. Untuk menuju ke informasi atau data yang dituju, seorang pengguna menyeleksi pilihan-pilihan yang disediakan hingga masuk ke topik yang diinginkan. Fasilitas demikian disebut Gopher. Gopher menyediakan pengaksesan informasi hanya berupa teks.

CHAT GROUPS / INTERNET RELAY CHAT (IRC)

Salah satu layanan komunikasi langsung di internet adalah internet relay chat (IRC). Layanan ini memungkinkan para pengakses internet melakukan chatting atau percakapan dengan pengakses internet lainnya dalam sebuah ruang chatting yang sama.

INTERNET PHONE/CONFERENCE

Fasilitas untuk melakukan percakapan jarak jauh via INTERNET. Untuk itu diperlukan aplikasi khusus dan dukungan hardware multimedia.

WAIS SERVER

WAIS (Wide Area Information Service) menyediakan cara lain untuk menemukan informasi yang tersebar dalam INTERNET. WAIS mampu mengakses segala database yang besar (seperti dokumen, file berisi gambar, video dan suara).

MAILING LIST

Kelompok diskusi. Fasilitas ini dibangun menggunakan teknik yang sama dengan proses penyebaran surat elektronik. Dengan menggunakan fasilitas ini, sebuah berita/file dapat didistribusikan ke banyak pengguna sekaligus. Bahkan penggunanya dapat melakukan diskusi, seminar, ceramah, konferensi secara elektronik tanpa terikat dimensi ruang dan waktu. Diskusi dapat berlangsung setiap hari tanpa henti. Hasil yang diperoleh akan jauh lebih efektif daripada penyelenggaraan seminar/konferensi konvensional.