BAB II
TEORI PENUNJANG

2.1 Definisi Jaringan Komputer

Jaringan Komputer yaitu sekumpulan komputer beserta perangkat-perangkat lain sebagai pendukung komputer yang saling terhubung satu sama lain dalam satu kesatuan[2]. Media jaringan komputer bisa tanpa kabel dan bisa melalui kabel, hal ini memungkinkan pengguna jaringan komputer dapat saling bertukar informasi, misalnya data atau dokumen, dapat mencetak melalui printer yang sama di dalam satu jaringan yang sama, dapat saling berkomunikasi antara pengguna satu dengan lainnya (*email*, *chatting*), untuk mengakses informasi (*web browsing*).

Di dalam sebuah jaringan komputer ada dua pihak yang saling beinteraksi untuk mencapai tujuan yang sama yaitu pihak client dan pihat *server*. Pihak client adalah pihak yang menerima atau meminta layanan, sedangkan pihak *server* adalah pihak yang mengirim atau mengirimkan layanan. Selain itu dalam sebuah jaringan komputer terdapat puluhan, ribuan, dan bahkan jutaan node. Node merupakan setiap komputer atau perangkat lain yang terhubung dalam suatu jaringan.

2.1.1 Pengelompokan Jaringan Komputer

Berdasarkan jarak dan area kerjanya jaringan komputer dibedakan menjadi tiga kelompok, yaitu :

1. LAN (*Local Area Network*)

   LAN adalah sejumlah komputer yang saling dihubungkan bersama di dalam satu area tertentu yang tidak begitu luas, seperti di dalam satu kantor atau gedung [2].

2. MAN (*Metropolitan Area Network*)

   MAN adalah jaringan yang banyak digunakan untuk menghubungkan simpul yang berada pada jarak 20 – 50 Km, jaringan ini biasa digunakan untuk antar

kota dengan menggunakan poket radio atau fasilitas perusahaan telekomunikasi [2].

3. WAN (*Wide Area Network*)

   Wide Area Network (WAN) merupakan jaringan dari sistem komunikasi data yang masing-masing *node* berlokasi jauh (*Remote Location*) satu dengan yang lainnya. WAN disebut juga dengan nama *Remote Network* / *Long Distance network*. *Node* adalah titik yang dapat menerima *input* data ke dalam *network* atau menghasilkan *output* informasi atau kedua-duanya [2].

2.1.2 Berdasarkan Media Penghantar

Berdasarkan media penghantar, jaringan komputer dapat dibagi menjadi dua jenis, yaitu :

1. *Wire Network*

   Pada jaringan ini, untuk menghubungkan satu komputer dengan komputer lain diperlukan penghubung berupa kabel jaringan. Kabel jaringan berfungsi dalam mengirim informasi dalam bentuk sinyal listrik antar komputer .

2. *Wireless Network*

   Merupakan jaringan dengan medium berupa gelombang elektromagnetik. Pada jaringan ini tidak diperlukan kabel untuk menghubungkan antar komputer karena menggunakan gelombang elektromagnetik yang akan mengirimkan sinyal informasi antar komputer jaringan.

2.1.3 Berdasarkan Fungsi

Berdasarkan fungsinya, jaringan komputer dapat dibagi menjadi dua jenis, yaitu:

1. *Client Server*

   Pada jaringan *client–server* terdapat sebuah komputer yang berfungsi sebagai *server* sedangkan komputer–komputer yang lain berfungsi sebagai *client*. Sesuai dengan namanya maka komputer *server* berfungsi dan bertugas melayani seluruh komputer yang terdapat dalam jaringan tersebut. Komputer–

komputer ini sering disebut juga dengan *workstation*, yaitu komputer dimana pengguna jaringan dapat mengakses dan memanfaatkan pelayanan yang diberikan oleh komputer *server*.

2. *Peer to Peer*

   Peer to peer adalah jaringan komputer dimana setiap komputer bisa menjadi *server* sekaligus *client*. Setiap komputer dapat menerima dan memberikan akses dari atau ke komputer lain [2].

2.1.4 Topologi Jaringan Komputer

Topologi Jaringan adalah suatu cara menghubungkan komputer yang satu dengan yang lainya sehingga membentuk sebuah jaringan[2]. Berikut topologi dasar jaringan diantaranya:

1. *Bus*

   Merupakan sebuah arsitektur jaringan di mana satu set *client* terhubung pada satu kabel utama (*backbone*) yang dinamakan *bus*. Topologi *bus* adalah cara yang paling sederhana untuk menghubungkan banyak client, namun masalah yang paling sering dihadapi adalah pada saat dua client akan mengirimkan data pada saat yang bersamaan pada bus yang sama.

Gambar 2.1. Topologi Bus

Data yang dikirimkan akan langsung menuju terminal yang dituju tanpa harus melewati terminal-terminal dalam jaringan, atau akan di *routing*kan ke *head end controller*. Tidak bekerjanya sebuah komputer tidak akan menghentikan kerja dari jaringan, jaringan akan tak bekerja apabila kabel utamanya dipotong atau putus.

Jaringan ini merupakan jaringan yang banyak digunakan karena hanya dalam beberapa meter kabel dapat dihubungkan ke banyak terminal *client*. Jaringan ini biasanya menggunakan kabel *coaxial* sebagai media transmisinya. Kabel *coaxial* dilihat dari bentuk fisiknya mirip dengan kabel antena. Kabel ini mempunyai kapasitas *bandwidth* 2MB.

Kelebihan dari topologi *bus* adalah, sebagai berikut:

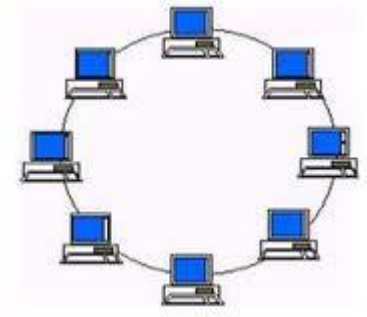
1. Kecepatan pengiriman tinggi.
2. Tidak diperlukan pengendali pusat.
3. Jumlah perangkat yang terhubung dapat dirubah tanpa mengganggu yang lain.

Kekurangan topologi *bus* adalah, sebagai berikut:

1. Jika tingkat traffic tinggi dapat menyebabkan *congestion* .
2. Diperlukan *repeater* untuk memperkuat sinyal.
3. Operasional jaringan LAN tergantung tiap perangkat.

2. *Ring*

Topologi jenis ring menghubungkan satu komputer di dalam suatu loop tertutup. Pada topologi ini data atau message berjalan mengelilingi jaringan dengan satu arah pengiriman ke komputer selanjutnya terus hingga mencapai komputer yang dituju.Waktu yang di butuhkan untuk mencapai terminal tujuan disebut waktu transmisi.



Gambar 2.2. Topologi *Ring*

Di dalam topologi cincin ini terdapat beberapa kekurangan dan kelebihan sebagai berikut:

Keuntungan topologi jaringan tipe cincin:

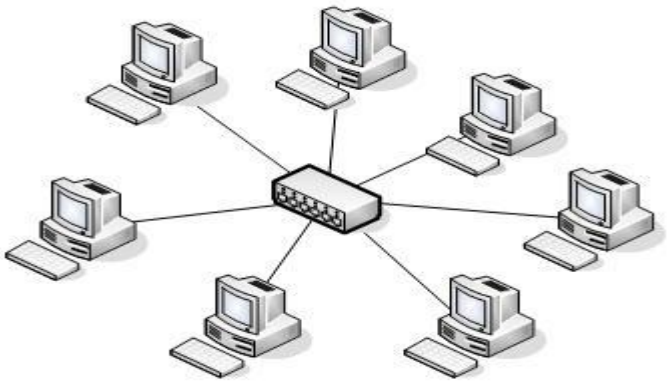
1. Mudah dibuat dan rapi.
2. Performa lebih baik ketimbang *bus* bahkan pada transfer data yang berat sekalipun.
3. tidak membutuhkan *central node* untuk menghubungkan antara satu komputer dengan komputer yang lainnya.

Kekurangan topologi jaringan tipe cincin:

1. kesalahan pada satu perangkat akan mengganggu kinerja keseluruhan jaringan.
2. memindahkan, mengubah atau mengganti salah satu perangkat akan berpengaruh terhadap seluruh jaringan
3. lebih sulit untuk melakukan konfigurasi ketimbang tipe *star*.

3. Star

Jenis topologi jaringan ini menggunakan satu terminal sebagai terminal sentral yang mengubungkan ke semua terminal *client*. Terminal sentral ini yang mengarahkan setiap data yang dikirimkan ke komputer yang dituju. Jenis jaringan ini apabila ada salah satu terminal *client* tidak berfungsi atau media transmisi putus atau terganggu maka tidak akan mempengaruhi kerja dari jaringan, karena gangguan tersebut hanya mempengaruhi terminal yang bersangkutan.



Gambar 2.3. Topologi *Star*

Kelebihan topologi *star :*

1. Memiliki performa yang lebih baik
2. Mudah melacak adanya kesalahan pada perangkat. Jika terdapat kesalahan pada salah satu perangkat maka kesalahan tersebut dapat diisolasi tanpa menggangu keseluruhan jaringan.
3. Mudah untuk instalasi perangkat baru.

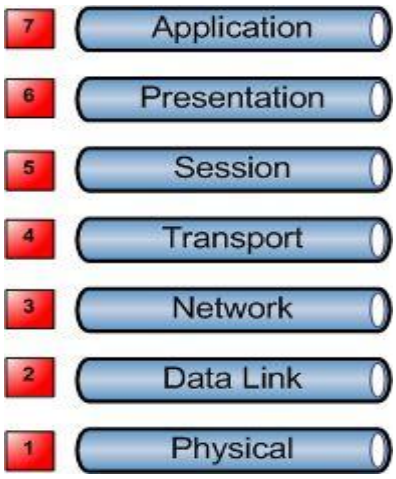
   Kekurangan topologi *star* yaitu sangat bergantung pada hub atau *switch*. Kesalahan pada *hub* akan berakibat pada matinya seluruh jaringan.

2.2 Protokol Jaringan Komputer

Protokol Jaringan adalah perangkat aturan yang digunakan dalam jaringan, Protokol adalah aturan main yang mengatur komunikasi diantara beberapa komputer di dalam sebuah jaringan sehingga komputer-komputer anggota jaringan dan komputer berbeda *platform* dapat saling berkomunikasi. semua jenis-jenis jaringan komputer menggunakan protocol [4]. Aturan-aturan protokol adalah termasuk di dalamnya petunjuk yang berlaku bagi cara-cara atau metode mengakses sebuah jaringan, topologi fisik, tipe-tipe kabel dan kecepatan transfer data.

2.2.1 OSI (Open System Interconnection) Model

Model OSI atau *Open System Interconnection* menggambarkan bagaimana informasi dari suatu perangkat lunak aplikasi di sebuah komputer berpindah melewati sebuah media jaringan ke suatu perangkat lunak aplikasi di komputer lain [2]. Model OSI dibuat untuk mengatasi masalah *internetworking* akibat perbedaan arsitektur dan protokol jaringan.



Gambar 2.4. *Seven layers OSI model*

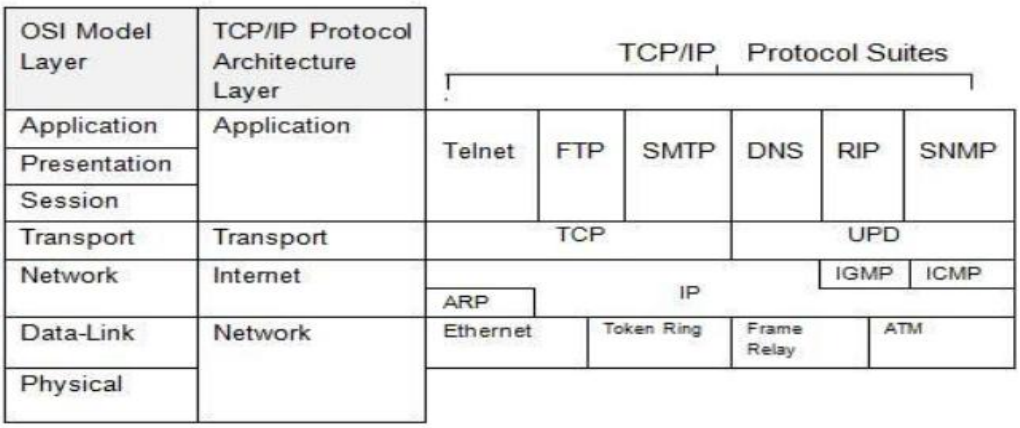
Masing-masing *layer* pada gambar 2.4 dapat dijelaskan sebagai berikut:

1. *Layer Phsical* berfungsi untuk mendefinisikan media transmisi jaringan, sinkronisasi *bit*, arsitektur jaringan. Selain itu, *layer* ini juga mendefinisikan bagaimana *network interface card* berinteraksi dengan media *wire* atau *wireless.*
2. *Layer Data Link* berfungsi untuk menentukan bagaimana *bit-bit* dikelompokan menjadi format yang disebut *frame*. Pada *layer* ini juga terjadi pengalamatan perangkat keras dan menentukan bagaimana perangkat-perangkat jaringan beroprasi. Contoh protokol pada *layer* ini, Ethernet, *Token bus*, *Token ring.*
3. *Layer Network* berfungsi untuk mendefinisikan alamat-alamat IP, membuat *header* untuk paket-paket data, dan melakukan *routing*
4. *Layer Transport* berfungsi untuk memecah data menjadi paket-paket data serta untuk memberikan nomor urut setiap paket sehingga dapat disusun kembali setelah diterima. Contoh protokol yang digunakan pada *layer* ini TCP dan UDP.
5. *Layer Session* berfungsi untuk mendefinisikan bagaimana koneksi dimulai, dipelihara, dan diakhiri. Contoh protokol pada *layer* ini, NetBIOS, ADSP, PAP .

6. *Layer Presentation* berfungsi untuk mentranslasikan data yang hendak ditransmisikan kedalam format yang dimengerti dalam jaringan. Contoh format kompresi, GIF, TIF, JPG.
7. *Layer Aplication* berfungsi sebagai antarmuka dengan *user*. Mengatur bagaimana aplikasi dapat mengakses jaringan. Contoh protokol yang berada pada *layer* ini, FTP, telnet, HTTP, SMTP, POP3, dan NFS.

2.2.2 TCP/IP

Internet protocol suite atau *TCP/IP* (singkatan dari *Transmission Control Protocol*/*Internet Protocol*) adalah standar komunikasi data yang digunakan oleh komunitas internet dalam proses tukar-menukar data dari satu komputer ke komputer lain di dalam jaringan Internet [4]. Protokol ini tidaklah dapat berdiri sendiri, karena memang protokol ini berupa kumpulan protokol (*protocol suite*). Protokol TCP/IP dikembangkan pada akhir dekade 1970-an hingga awal 1980-an sebagai sebuah protokol standar untuk menghubungkan komputer-komputer dan jaringan untuk membentuk sebuah jaringan yang luas (WAN). TCP/IP merupakan sebuah standar jaringan terbuka yang bersifat independen terhadap mekanisme trans*port* jaringan fisik yang digunakan, sehingga dapat digunakan di mana saja. Protokol ini menggunakan skema pengalamatan yang sederhana yang disebut sebagai alamat IP (*IP Address*) yang mengizinkan hingga beberapa ratus juta komputer untuk dapat saling berhubungan satu sama lainnya di Internet. Protokol ini juga bersifat *routable* yang berarti protokol ini cocok untuk menghubungkan sistem-sistem berbeda (seperti Microsoft Windows dan keluarga UNIX) untuk membentuk jaringan yang heterogen.



Gambar 2.5. *TCP/IP* dan OSI model

Masing-masing *layer* pada gambar 2.5 dapat dijelaskan sebagai berikut:

1. *Network interface*

   Sama halnya dengan layer *Data link* dan *Physical layer* Pada OSI yang mengurusi banyak hal yang berhubungan dengan prosedur mekanis dan elektris dalam transmisi bit-bit.

2. Internet

   Berfungsi untuk memberikan layanan dasar pengantaran data. salah satu protokol yang bekerja pada layer ini adlah IP (*internet protokol*) yang diantaranya berfungsi: mentransfer data dari *Network access layer* ke trans*port* layer dan sebaliknya menangani datagaram termasuk fragmentasi dan defragmentasi menangani skema pengalamatan yang diguankan dalam pertukaran data- menangani proses routing

3. *Transport*

   Sama seperti pada model protokol OSI yaitu berfungsi menghubungkan antara aplication layer dan internet layer contohnya : UDP, TCP, SNMP (*apliccation*) menggunakan UDP, Telnet, FTP, SMTP (*apliccation*) menggunakan TCP

4. *Application*

   Adalah seperti seperti gabungan dari layer application, presentation dan session pada protokol model OSI,pada model protokol tcp/ip maka aplikasi

yang dibuat dan berhubungan langsung dengan pemakai akan diletakkan di sini.contohnya : FTP, SMTP, HTTP, SNMP, RPC, DNS.

2.3 IP (*Internet Protocol*)

IP *address* digunakan sebagai alamat dalam hubungan antar host di internet sehingga merupakan sebuah sistem komunikasi yang *universal* karena merupakan metode pengalamatan yang telah diterima di seluruh dunia. Dengan menentukan IP *address* berarti kita telah memberikan identitas yang *universal* bagi setiap *interface* komputer. Jika suatu komputer memiliki lebih dari satu *interface* (misalkan menggunakan dua ethernet) maka kita harus memberi dua IP *address* untuk komputer tersebut masing-masing untuk setiap interfacenya [4].

IP *address* versi 4 dapat dipisahkan menjadi 2 bagian, yakni bagian *network* (*net* ID) dan bagian *host* (*host* ID). *Network* ID berperan dalam identifikasi suatu *network* dari *network* yang lain, sedangkan *host* ID berperan untuk identifikasi *host* dalam suatu *network*. Jadi, seluruh *host* yang tersambung dalam jaringan yang sama memiliki network ID yang sama. Sebagian dari bit-bit bagian awal dari IP *Address* merupakan *network* bit/*network number*, sedangkan sisanya untuk *host*. Garis pemisah antara bagian *network* dan *host* tidak tetap, bergantung kepada kelas *network.*

Perbedaan tiap kelas adalah pada ukuran dan jumlahnya. Contohnya IP kelas A dipakai oleh sedikit jaringan namun jumlah *host* yang dapat ditampung oleh tiap jaringan sangat besar. Kelas D dan E tidak digunakan secara umum, kelas D digunakan bagi jaringan *multicast* dan kelas E untuk keprluan eksperimental. Perangkat lunak *Internet Protokol* menentukan pembagian jenis kelas ini dengan menguji beberapa bit pertama dari IP *Address*. Secara umum IP *Address* itu sendiri dikelompokan dalam beberapa kelas, antara lain :

1. Kelas A

   Bit pertama IP *address* kelas A adalah 0, dengan panjang network ID 8 bit dan panjang *host* ID 24 bit. Jadi byte pertama IP *address* kelas A mempunyai range dari 0-127. Jadi pada kelas A terdapat 127 *network* dengan tiap *network*

dapat menampung sekitar 16 juta *host*. IP *address* kelas A diberikan untuk jaringan dengan jumlah *host* yang sangat besar.

2. Kelas B

   Dua bit IP *address* kelas B selalu di*set* 10 sehingga byte pertamanya selalu bernilai antara 128-191. *Network* ID adalah 16 bit pertama dan 16 bit sisanya adalah *host* ID sehingga kalau ada komputer mempunyai IP *address* 167.205.26.161, *network* ID = 167.205 dan *host* ID = 26.161. Pada IP *address* kelas B ini mempunyai *range* IP dari 128.0.xxx.xxx sampai 191.155.xxx.xxx, yakni berjumlah 65.255 *network* dengan jumlah *host* tiap *network* 216 *host* atau sekitar 65 ribu *host.*

3. Kelas C

   Alamat IP kelas C mulanya digunakan untuk jaringan berukuran kecil seperti LAN. Tiga bit pertama IP *address* kelas C selalu di*set* 111. *Network* ID terdiri dari 24 bit dan *host* ID 8 bit sisanya sehingga dapat terbentuk sekitar 2 juta *network* dengan masing-masing *network* memiliki 28 *host* atau sekitar 256 *host*.

4. Kelas D

   Alamat IP kelas D disediakan hanya untuk alamat-alamat *IP multicast*, sehingga berbeda dengan tiga kelas di atas. Empat *bit* pertama di dalam IP kelas D selalu di*set* ke bilangan biner 1110. 28 *bit* sisanya digunakan sebagai alamat yang dapat digunakan untuk mengenali *host*.

5. Kelas E

   Alamat IP kelas E tidak diperuntukan untuk keperluan umum. Empat bit pertama selalu di *set* kepada bilangan biner 1111. 28 bit sisanya digunakan sebagai alamat yang dapat digunakan untuk mengenali *host*. Secara garis besar pembagian kelas.

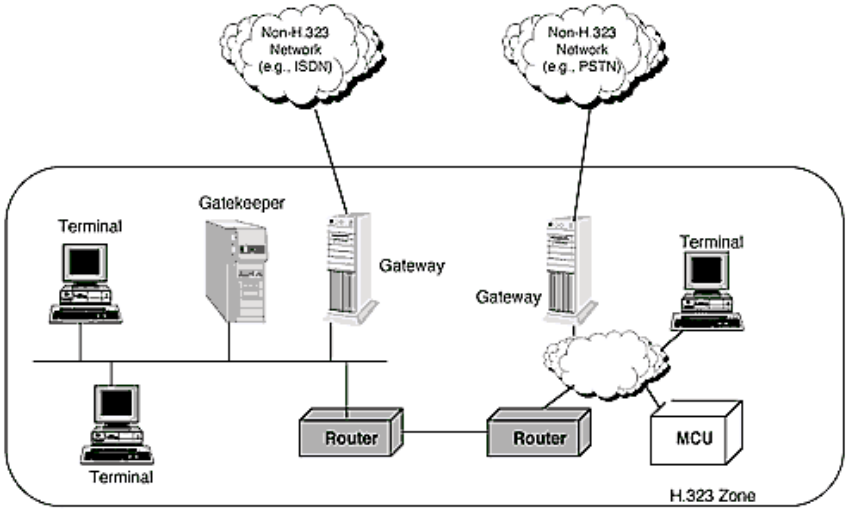
2.4 Protokol H.323

Protokol H.323 adalah salah satu dari Protokol untuk teknologi jaraingan komputer yang merupakan protokol yang digunakan dalam proses transmisi multimedia dan penerapannya ditemukan secara luas untuk lalulintas jarak jauh, seperti layanan *Lokal Area Network* (LAN) [3]. Teknologi Protokol H.323 sendiri merupakan suatu standart ITU-T *(International Telecomunications Union - Telecomunications)* atau bisa di istilahkan standar yang menentukan komponen protokol, dan prosedur yang menyediakan layanan komunikasi multimedia, yaitu komunikasi *audio*, *video* dan data *real-time* , melalui jaringan berbasis paket *(packet-based network).* Jaringan tersebut antara lain *Internet Protocol* (IP), *Internet Packet eXchange* (IPX), *Local Area Network* (LAN), *Enterpraise* Network (EN), *Metropolitan Area Network* (MAN) dan *Wide Area Network* (WAN).

Teknologi Protokol H.323 bisa diterapakan pada berbagai layanan aplikasi komuikasi yatu meliputi suara saja *(IP Telephony)*, suara dan gambar *(Video Telephony)*, suara dan data, dan juga suara, gambar dan data. H.323 juga bisa diterapkan dalam *point-to-point* dan juga bisa digunakan dalam aplikasi multipoint conference. Standart H.323 terdiri dari empat buah komponen yang telah disatukan kedalam suatu jaringan dan akan memberikan layanan komunikasi point-to-point dan multipoint conference, Adapun komponen jaringan H.323 itu terdiri beberapa item yaitu terminal, *gateway, gatekeeper dan Multipoint Control Unit* (MCU). Standar kumpulan beberapa komponen, protokol dan prosedur dalam membangun komunikasi multimedia yang menerangkan set suara, *video* dan standar konferensi data. Beberapa protokol tersebut diantaranya:

1. H.26x codecs Rekomendasi mengenai proses digitalisasi sinyal *video* analog.
2. H.225.0 Jika *gatekeeper* terdapat dalam suatu *network* maka H.225.0 mengatur proses registrasi terminal ke *gatekeeper* tersebut dan mengatur pula proses admisi di jaringan tersebut.
3. H.245 Protokol ini berfungsi untuk membangun kanal logikal yang akan menjadi kanal transmisi media.

4. Q.931Q.931 digunakan bersama H.225.0 untuk membangun hubungan H.323.
5. RTP (*Real time Transport Protocol*) adalah protokol yang digunakan untuk mengkompensasi *jitter* dan *desequencing* yang terjadi pada jaringan IP.
6. RTCP (*Real time Transport Control Protocol*) digunakan untuk mengirimkan paket kontrol setiap terminal yang berpartisipasi pada percakapan yang digunakan sebagai informasi untuk kualitas transmisi jaringan.



Gambar 2.6 Arsitektur H.323

.

2.5 Perangkat-Perangkat Jaringan

Perangkat-perangkat yang terdapat dalam jaringan computer di antaranya adalah :

1. *Hub*

   Hub adalah perangkat jaringan yang paling sederhana. Pada hub, data diteruskan ke semua *port*, terlepas dari apakah data dimaksudkan untuk sistem yang terhubung ke *port*. Selain *port* untuk penghubung komputer, bahkan hub pada umumnya memiliki *port* yang ditunjuk sebagai *port uplink* yang memungkinkan hub terhubung ke hub untuk membuat jaringan yang lebih besar.

2. *Switch*

   Seperti *router*, *switch* adalah perangkat cerdas yang memetakan alamat IP dengan alamat MAC dari LAN *cards*. Berbeda dengan hub, *switch* tidak menyampaikan data ke semua komputer, namun hanya mengirimkan paket data ke komputer yang ditujukan. Switch digunakan dalam LAN, MAN dan WAN. Dalam sebuah jaringan Ethernet, komputer secara langsung terhubung dengan *switch* melalui kabel *twisted pair*.Dalam jaringan, *switch* menggunakan tiga metode untuk mengirimkan data yaitu *store and forward*, *cut through and fragment free*.

3. *Router*

   Router adalah perangkat komunikasi yang digunakan untuk menghubungkan dua jaringan yang berbeda. Fungsi utama dari *router* adalah untuk pemilahan dan distribusi dari paket data untuk berbagai tujuan mereka berdasarkan alamat IP paket data tersebut.

4. Modem

   Modem adalah salah satu perangkat jaringan komputer yang merupakan perangkat komunikasi yang digunakan untuk menyediakan konektivitas dengan internet. Modem bekerja dalam dua cara yaitu modulasi dan demodulasiyang berfungsi mengubah data digital ke analog dan data analog ke digital.

5. LAN *Card*

   LAN *Card* atau *network adapters* merupakan blok bangunan dari sebuah jaringan komputer. Komputer tidak dapat berkomunikasi tanpa terinstal dan terkonfigurasi dengan Lan *card*. Setiap LAN *card* disediakan dengan sebuah alamat IP yang unik, *subnet mask*, *gateway* dan DNS (jika ada). Setiap kartu LAN disediakan dengan sebuah alamat IP yang unik, *subnet mask*, *gateway* dan DNS (jika ada). Kartu LAN dimasukkan ke dalam *expansion slot* di dalam komputer.

2.6 Performansi Jaringan

Performansi Jaringan merupakan salah satu hal penting yang harus dilakukan dalam mengelola suatu jaringan Performansi jaringan ini dapat memberikan informasi mengenai operasi jaringan yang dimiliki dan untuk memberikan informasi mengenai kejanggalan / perubahan jaringan yang aneh. Dengan adanya performansi tersebut, masalah yang terjadi dapat segera dianalisa penyebabnya dan dapat diselesaikan sesuai dengan prosedur yang ada. Pada bagian ini akan dijelaskan dan memperkenalkan istilah yang dibutuhkan untuk bab-bab selanjutnya.

Salah satu karakteristik yang mengukur kinerja jaringan *bandwidth*. Namun, istilah dapat digunakan dalam dua konteks yang berbeda dengan dua nilai pengukuran yang berbeda yaitu *bandwidth* dalam hertz dan *bandwidth* dalam bit per detik.

1. *Bandwidth* dalam Hertz

   Bandwidth dalam hertz adalah rentang frekuensi yang terkandung dalam sinyal komposit atau rentang frekuensi saluran dapat melewati. Sebagai contoh, mengatakan *bandwidth* dari saluran telepon pelanggan adalah 4 kHz.

2. *Bandwidth* dalam Bit per Detik.

   Istilah *bandwidth* bisa juga merujuk kepada jumlah bit per detik sehingga saluran, link, atau bahkan jaringan dapat mengirimkan. Misalnya *bandwidth* yang cepat jaringan ethernet (atau link dalam jaringan ini) maksimal 100 mbps. Ini berarti bahwa jaringan ini dapat mengirim 100 mbps.

3. *Throughput*

   Throughput adalah ukuran dari seberapa cepat kita benar-benar dapat mengirim data melalui jaringan[5]. Meskipun *bandwidth* dalam bit per detik dan *throughput* tampak sama, Tetapi mereka berbeda. Sebuah link mungkin memiliki *bandwidth* B bps, tapi kita hanya bisa mengirim T bps melalui link ini dengan T selalu kurang dari B. Dengan kata lain, *bandwidth* merupakan potensi pengukuran link, throughput adalah pengukuran sebenarnya seberapa cepat kita dapat mengirim data. Sebagai contoh, kita mungkin memiliki link

dengan *bandwidth* 1 Mbps, tetapi perangkat yang terhubung ke ujung link mungkin hanya menangani 200 kbps. Ini berarti bahwa tidak bisa mengirim lebih dari 200 kbps melalui link ini. Bayangkan sebuah jalan raya yang dirancang untuk mengirimkan 1.000 mobil per menit dari satu titik ke titik lain. Namun, jika terjadi *congestion* di jalan, angka ini dapat dikurangi menjadi 100 mobil per menit. *Bandwidth* adalah 1000 mobil per menit, throughput adalah 100 mobil per menit.

$$Throughput = \frac{Paket\ Data\ Yang\ Diterima}{Lama\ Pengamatan} \qquad (2.1)$$

4. *Latency (delay)*

   Delay adalah waktu tunda suatu paket yang diakibatkan oleh proses transmisi dari satu titik ke titik lain yang menjadi tujuannya.

$$Delay = \frac{\text{Total Paket}}{Total\ Delay} \qquad (2.2)$$

   Delay dalam jaringan TCP/IP dapat digolongkan sebagai berikut :.

   a. Queuing Delay

      Delayini disebabkan oleh waktu proses yang diperlukan oleh router didalam menangani antrian transmisi paket di sepanjang jaringan. Umumnya delay ini sangat kecil , kurang lebih 100micro second.

   b. Delay Propagasi

      Proses perjalanan informasi selama didalam media transmisi, misalnya SDH, coax atau tembaga, menyebabkan delay yang disebut dengan delay propagasi.

   c. Transmission Delay

      Transmission Delay adalah waktu yang diperlukan sebuah paket data untuk melintasi suatu media. Transmission delay ditentukan oleh kecepatan media dan besar paket data.

Menurut versi TIPHON (Joesman 2008), besarnya delay dapat diklasifikasikan sebagai berikut:

Tabel 2.1 Klasifikasi *Delay* TIPHON

Kategori	Besar *Delay*
Sangat Bagus	< 150 ms
Bagus	150 s/d 300 ms
Sedang	300 s/d 450 ms
Jelek	> 450 ms

5. *Jitter*

Masalah kinerja lain yang juga terkait penundaan adalah *jitter*. bisa dikatakann bahwa jitter adalah masalah jika paket data yang berbeda menghadapi penundaan yang berbeda dan aplikasi menggunakan data pada tempat penerima sensitif terhadap waktu (data *audio* dan *video*) misalnya jika *delay* untuk paket pertama adalah 20 ms, untuk kedua adalah 45 ms, dan ketiga adalah 40 ms, maka aplikasi *real-time* yang menggunakan paket bertahan dari *jitter*.

$$Jitter = \frac{Total\ Variasi\ \ Delay}{Total\ \ Paket\ \ Diterima} \qquad (2.3)$$

2.2 Klasifikasi *Jitter* TIPHON

Kategori	Besar *Jitter*
Sangat Bagus	0 ms
Bagus	0 s/d 75 ms
Sedang	75 s/d 125 ms
Jelek	125 s/d 225 ms

2.7 *Congestion*

Suatu hal yang penting dalam jaringan *packet-switched* adalah *congestion* . *Congestion* dalam jaringan dapat terjadi jika beban pada jaringan-jumlah paket yang dikirim ke jaringan adalah lebih besar dari kapasitas jaringan-jumlah paket jaringan yang dapat menangani. Kontrol *congestion* mengacu pada mekanisme dan teknik untuk mengendalikan *congestion* dan menjaga load di bawah kapasitas. Kita mungkin bertanya mengapa ada *congestion* pada jaringan. *Congestion* terjadi di setiap sistem yang melibatkan menunggu. Misalnya, *congestion* yang terjadi di jalan bebas hambatan karena setiap abnonnality dalam aliran, seperti kecelakaan pada jam sibuk, menciptakan penyumbatan. *Congestion* dalam jaringan atau *internetwork* terjadi karena *router* dan *switch* memiliki antrian-buffer yang memegang paket sebelum dan sesudah pengolahan. *Router* A, misalnya, memiliki antrian input dan output antrian untuk setiap antarmuka. Ketika sebuah paket tiba di antarmuka yang datang, itu mengalami tiga langkah sebagai berikut :

1. Paket yang diletakkan pada akhir antrian masukan sambil menunggu untuk diperiksa.
2. Modul pengolahan *router* menghapus paket dari antrian Input setelahmencapai antrean paling depan dan menggunakan tabel routing dan destinasialamat untuk menemukan rute.
3. Paket akan dimasukkan ke dalam antrian *output* yang sesuai dan menunggu giliran untuk dikirim.

Kontrol *congestion* mengacu pada teknik dan mekanisme yang baik dapat mencegah *congestion* , sebelum hal itu terjadi, atau menghapus *congestion* , setelah itu terjadi. Secara umum, kita bisa membagi mekanisme kontrol *congestion* menjadi dua kategori besar *open-loop congestion control* (*prevention*) *and closed-loop congestion control* (*removal*).

1. *Open loop Congestion Control*

Dalam *Open-loop Congestion Control*, kebijakan yang diterapkan untuk mencegah kemacetan sebelum terjadi. Dalam mekanisme ini, kontrol kongesti ditangani baik oleh sumber atau tujuan.

2. *Closed loop Congestion Control*

   Mekanisme *Closed-loop Congestion Control* mencoba untuk mengurangi kemacetan setelah terjadi. Beberapa mekanisme telah digunakan oleh protokol yang berbeda.

2.8 *Quality of Service* (QoS)

Quality of Service (QoS) didefinisikan sebagai sebuah mekanisme atau cara yang memungkinkan layanan dapat beroperasi sesuai dengan karakteristiknya masing masing dalam jaringan IP [5]. QoS bertujuan untuk menyediakan kualitas yang berbeda-beda dan memberikan prioritas untuk beragam kebutuhan akan layanan di dalam jaringan IP. Secara umum model layanan untuk memberikan fungsi QoS adalah *Best effort Service*, *Integrated Service* (IntServ) dan *Differentiated Service* (DiffServ). Parameter-parameter yang lazim dijadikan referensi umum untuk mengamati unjuk kerja jaringan, diantaranya adalah *delay* dan *jitter*. *Best-effort* service digunakan untuk melakukan semua usaha agar dapat mengirimkan sebuah paket ke suatu tujuan.

2.8.1 *Best Effort*

Sesuai dengan namanya, model QoS *Best-Effort* merupakan model servis yang dihantarkan kepada penggunanya akan dilakukan sebisa mungkin dan sebaikbaiknya tanpa ada jaminan apa-apa. Jika ada sebuah data yang ingin dikirim, maka data tersebut akan di kirim segera begitu media perantaranya siap dan tersedia. Data yang dikirim juga tidak dibatasi, tidak diklasifikasikan, tidak perlu mendapatkan ijin dari perangkat manapun, tidak diberi *policy*, semuanya hanya berdasarkan siapa yang datang terlebih dahulu ke perangkat *gateway* [5].

Dengan kata lain model *Best-Effort* ini tidak memberikan jaminan apa-apa terhadap *reliabilitas*, performa, *bandwidth*, kelancaran data dalam jaringan, *delay*, dan banyak lagi parameter komunikasi data yang tidak dijamin. Data akan dihantarkan sebisa mungkin untuk sampai ke tujuannya. Jika hilang ditengah jalan atau tertunda dengan waktu yang cukup lama di dalam perjalanannya, maka tidak ada pihak maupun perangkat yang bertanggung jawab.

Model *Best-Effort* ini sangat cocok digunakan dalam jaringan dengan koneksi lokal (LAN) atau jaringan dengan koneksi WAN yang berkecepatan sangat tinggi. Model ini sangat tepat jika digunakan dalam jaringan yang melewatkan aplikasi dan data yang bermacam-macam dengan tingkat prioritas yang sama. Jadi semua aplikasi didalamnya memiliki kualitas yang sama. Contohnya misalnya penggunaan internet di rumah atau perkantoran yang digunakan untuk *browsing*, *emai*l, *chatting*, banyak aplikasi lain.

Jenis QoS ini tidak cocok digunakan untuk melayani aplikasi-aplikasi bisnis yang kritis dan penting, karea aplikasi tersebut biasanya membutuhkan perlakuan istimewa untuk dapat berjalan dengan baik.

2.8.2 *Integrated Service* (IntServ)

IntServ Model atau disingkat IntServ merupakan sebuah model QoS yang bekerja untuk memenuhi berbagai macam kebutuhan QoS berbagai perangkat dan berbagai aplikasi dalam sebuah jaringan. Dalam model *IntServ* ini, para pengguna atau aplikasi dalam sebuah jaringan akan melakukan *request* terlebih dahulu mengenai servis dan QoS jenis apa yang mereka dapatkan, sebelum mereka mengirimkan data. *Request* tersebut biasanya dilakukan dengan menggunakan sinyal-sinyal yang jelas dalam proses komunikasinya [5].

Dalam *request* tersebut, pengguna jaringan atau sebuah aplikasi akan mengirimkan informasi mengenai profile *traffic* mereka ke perangkat QoS. Profile *traffic* tersebut akan menentukan hak-hak apa yang akan mereka dapatkan seperti misalnya berapa *bandwidth* dan delay yang akan mereka terima dan gunakan.

Setelah mendapatkan konfirmasi dari perangkat QoS dalam jaringannya, maka pengguna dan aplikasi tersebut baru diijinkan untuk melakukan transaksi pengiriman dan penerimaan data. Transaksi data akan dilakukan dalam batasan-batasan yang telah diberikan oleh perangkat QoS tersebut tanpa kecuali.

Sebuah perangkat QoS biasanya akan bertindak sebagai pengontrol hak-hak yang akan diterima oleh pengguna. Sedangkan pengguna jaringan dan aplikasi didalamnya bertugas untuk mengirimkan profile nya untuk dapat diproses dalam perangkat QoS. Setelah hak-hak pengguna jaringan jelas, perangkat QoS akan memenuhi komitmen yang telah dijanjikannya dengan cara mempertahankan status semua pengguna dan kemudian melakukan proses-proses QoS untuk memenuhinya. Proses-proses tersebut adalah *Packet Classification*, *Policing*, *Queing*, dan banyak lagi yang akan dibahas selanjutnya.

2.8.2.1 RSVP (*Resource Reservation Protocol*)

Pada kebanyakan perangkat jaringan yang mampu menjalankan QoS model IntServ ini, dilengkapi sebuah system sinyaling yang bertugas untuk mengirimkan profile dan request mereka ke perangkat QoS. Sistem sinyaling tersebut sering disebut dengan istilah *Resource Reservation Protocol* (RSVP).

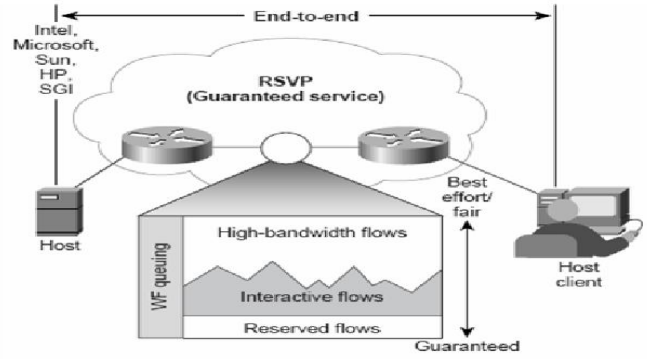
RSVP merupakan protokol signaling khusus untuk keperluan QoS. Protokol ini menggunakan info dari routing protocol untuk menentukan jalur terbaik menuju ke suatu lokasi. Meskipun RSVP sangat cocok digunakan untuk keperluan pengaturan QoS pada aplikasi real-time seperti IP *Telephony*, NetMeeting, IPTV *streaming*, dan banyak lagi, namun penggunaan RSVP sangatlah terbatas.

Penggunaan RSVP sangat terbatas dikarenakan semua perangkat yang berada dalam jaringan yang mendukung QoS jenis ini harus mendukung system sinyaling RSVP. Servis jenis ini sangat cocok untuk memberikan kualitas yang baik pada aplikasi-aplikasi real-time seperti *video converence*.

2.8.2.2 Cara Kerja RSVP

RSVP merupakan protokol pemesanan *resource* yang dipakai untuk integrated service. Protokol RSVP dipakai oleh host untuk meminta QoS dari jaringan untuk dipakai oleh aplikasi tertentu. RSVP juga dipakai oleh router untuk mengantar permintaan QoS ke semua node sepanjang jalur aliran data dan dipakai untuk membangun dan memelihara kondisi RSVP didesain untuk beroperasi dengan protokol peroutingan *unicast* dan *multicast*, sehingga RSVP bukan protokol perutingan. Proses RSVP memeriksa database perutingan lokal untuk mendapatkan route.

Protokol RSVP digunakan oleh router untuk mengirim permintaan QoS pada semua router lain. Tanggapan terhadap permintaan ini adalah pemesanan sumber daya (*resource reservation*) pada jalur yang akan digunakan oleh aplikasi. RSVP memungkinkan router memesan bandwidth yang cukup pada interface untuk meningkatkan performansi dan kualitas dari jaringan.



Gambar 2.7 Arsitektur RSVP

Message RSVP akan dipertukarkan oleh sender dan *receiver* dalam proses *resource reservation*. Ada beberapa macam message RSVP, tetapi message yang dianggap paling utama yaitu *Resv Message* dan *Path Message*. Sender akan mengirim Path Message ke receiver, dan receiver akan mengirim *Resv Message* ke sender dengan membalikkan jalur yang didefinisikan pada *Path Message* sebelumnya. RSVP merupakan protokol yang bersifat connection-oriented dimana terdapat tiga fase dalam mengadakan reservasi.

2.8.2.3 Masalah dengan *IntServ*

Setidaknya ada dua masalah dengan Integrated Services yang dapat mencegah implementasi maksimal di Internet: *Scalability* dan *Service-Type Limitation*.

1. *Scalability*

   Model pelayanan mengharuskan setiap *router* menyimpan informasi untuk setiap paket data . Karena internet berkembang setiap hari, ini adalah masalah serius.

2. *Service-Type Limitation*

   Model layanan *Intserv* hanya menyediakan dua jenis layanan, dijamin dan *control load* . Mereka menentang model ini berpendapat bahwa aplikasi mungkin membutuhkan lebih dari kedua jenis layanan.

2.8.3 *Differentiated Service* (DiffServ)

Model QoS ini merupakan model yang sudah lama ada dalam standarisasi QoS dari organisasi IETF. Model QoS ini bekerja dengan cara melakukan klasifikasi terlebih dahulu terhadap semua paket yang masuk kedalam sebuah jaringan [5]. Pengklasifikasian ini dilakukan dengan cara menyisipkan sebuah informasi tambahan yang khusus untuk keperluan pengaturan QoS dalam *header* IP pada setiap paket.

Setelah paket diklasifikasikan pada perangkat-perangkat jaringan terdekatnya, jaringan akan menggunakan klasifikasi ini untuk menentukan bagaimana *traffic* data ini diperlakukan, seperti misalnya perlakuan *queuing*, *shaping* dan policing nya. Setelah melalui semua proses tersebut, maka akan didapat sebuah aliran data yang sesuai dengan apa yang dikomitmenkan kepada penggunanya.

Informasi untuk proses klasifikasi pada *field* IP header atau dengan kata lain proses klasifikasi pada layer 3 standar OSI ada dua jenis, yaitu IP *Precedence* dan *Differential Service Code Po*int (DSCP). Informasi klasifikasi ini ditentukan

dalam tiga atau enam bit pertama dari *field Type of Service* (ToS) pada header paket IP.

Klasifikasi ini juga dapat dibawa dalam frame layer 2 dalam *field Class of Service* (CoS) yang dibawa dalam frame ISL maupun 802.1Q. Tidak seperti IntServ, model QoS DiffServ ini tidak membutuhkan kemampuan QoS pada sisi pengguna dan aplikasi-aplikasi yang bekerja di dalamnya.

Metode ini merupakan metode yang paling banyak dan luas digunakan. Selain lebih mudah, lebih ringan dan lebih umum penggunaannya, implementasinya juga tidaklah terlalu sulit. Semua perangkat jaringan yang dapat bekerja berdasarkan standar TCP/IP bisa digunakan untuk melewatkan informasi QoS ini. Jadi yang perlu memiliki kemampuan pemrosesan QoS mungkin saja hanya sisi penerima dan pengirimnya saja. Tentu sistem ini jauh lebih fleksibel dan mudah diterapkan. Selanjutnya pada artikel ini hanya akan dibahas teknik-teknik QoS berdasarkan sistem *DiffServ* ini.

QoS model *DiffServ* merupakan jenis yang paling banyak digunakan. Implementasinya tidak terlalu sulit hanya saja akan sedikit rumit secara teorinya. Model QoS ini menggunakan system penandaan atau marking untuk melakukan pengolahan traffic menjadi tercapai apa yang diinginkan. Setelah paket-paket data berhasil di tandai, serangkaian proses lain akan terjadi.

Berikut ini adalah proses-proses yang akan dilewati oleh paket-paket tersebut untuk mencapai tujuannya:

Model QoS ini merupakan model yang sudah lama ada dalam standarisasi QoS dari organisasi IETF. Model QoS ini bekerja dengan cara melakukan klasifikasi terlebih dahulu terhadap semua paket yang masuk kedalam sebuah jaringan. Pengklasifikasian ini dilakukan dengan cara menyisipkan sebuah informasi tambahan yang khusus untuk keperluan pengaturan QoS dalam *header* IP pada setiap paket.

Setelah paket diklasifikasikan pada perangkat-perangkat jaringan terdekatnya, jaringan akan menggunakan klasifikasi ini untuk menentukan bagaimana traffic data ini diperlakukan, seperti misalnya perlakuan queuing,

shaping dan *policing* nya. Setelah melalui semua proses tersebut, maka akan didapat sebuah aliran data yang sesuai dengan apa yang dikomitmenkan kepada penggunanya.

Informasi untuk proses klasifikasi pada *field* IP header atau dengan kata lain proses klasifikasi pada layer 3 standar OSI ada dua jenis, yaitu IP *Precedence* dan *Differential Service Code Point* (DSCP). Informasi klasifikasi ini ditentukan dalam tiga atau enam bit pertama dari *field Type of Service* (ToS) pada header paket IP.

Klasifikasi ini juga dapat dibawa dalam frame layer 2 dalam *field Class of Service* (CoS) yang dibawa dalam frame ISL maupun 802.1Q. Tidak seperti *IntServ*, model QoS *DiffServ* ini tidak membutuhkan kemampuan QoS pada sisi pengguna dan aplikasi-aplikasi yang bekerja di dalamnya.

Metode ini merupakan metode yang paling banyak dan luas digunakan. Selain lebih mudah, lebih ringan dan lebih umum penggunaannya, implementasinya juga tidaklah terlalu sulit. Semua perangkat jaringan yang dapat bekerja berdasarkan standar TCP/IP bisa digunakan untuk melewatkan informasi QoS ini. Jadi yang perlu memiliki kemampuan pemrosesan QoS mungkin saja hanya sisi penerima dan pengirimnya saja.

2.9 *Buffer*

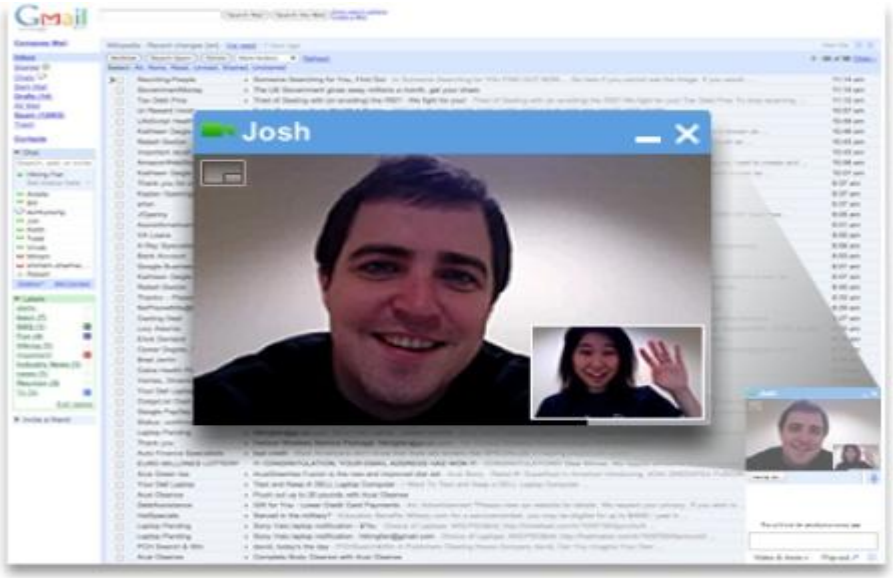
Buffer adalah area memori yang menyimpan data ketika mereka sedang dipindahkan antara dua device atau antara device dan aplikasi. Buffering dilakukan untuk tiga buah alasan. Alasan pertama adalah untuk men-cope dengan kesalahan yang terjadi karena perbedaan kecepatan antara produsen dengan konsumen dari sebuah stream data. Sebagai contoh,sebuah file sedang diterima melalui modem dan ditujukan ke media penyimpanan di hard disk. Kecepatan modem tersebut kira-kira hanyalah 1/1000 daripada hardisk. Jadi buffer dibuat di dalam memori utama untuk mengumpulkan jumlah byte yang diterima dari modem. Ketika keseluruhan data di buffer sudah sampai, buffer tersebut dapat ditulis ke disk dengan operasi tunggal. Karena penulisan disk tidak terjadi dengan

instan dan modem masih memerlukan tempat untuk menyimpan data yang berdatangan, maka dipakai 2 buah buffer. Setelah modem memenuhi buffer pertama, akan terjadi request untuk menulis di disk. Modem kemudian mulai memenuhi buffer kedua sementara buffer pertama dipakai untuk penulisan ke disk. Pada saat modem sudah memenuhi buffer kedua, penulisan ke disk dari buffer pertama seharusnya sudah selesai, jadi modem akan berganti kembali memenuhi buffer pertama dan buffer kedua dipakai untuk menulis. Metode double buffering ini membuat pasangan ganda antara produsen dan konsumen sekaligus mengurangi kebutuhan waktu di antara mereka. Alasan kedua dari buffering adalah untuk menyesuaikan device-device yang mempunyai perbedaan dalam ukuran transfer data. Hal ini sangat umum terjadi pada jaringan komputer, dimana buffer dipakai secara luas untuk fragmentasi dan pengaturan kembali pesan-pesan yang diterima. Pada bagian pengirim, sebuah pesan yang besar akan dipecah ke paket-paket kecil. Paket-paket tersebut dikirim melalui jaringan, dan penerima akan meletakkan mereka di dalam *buffer* untuk disusun kembali. Alasan ketiga untuk buffering adalah untuk mendukung *copy* semantics untuk aplikasi I/O. Sebuah contoh akan menjelaskan pa arti dari *copy* semantics. Jika ada sebuah aplikasi yang mempunyai buffer data yang ingin dituliskan ke disk. Aplikasi tersebut akan memanggil sistem penulisan, menyediakan pointer ke buffer, dan sebuah integer untuk menunjukkan ukuran bytes yang ingin ditulis. Setelah pemanggilan tersebut, apakah yang akan terjadi jika aplikasi tersebut mengubah isi dari buffer, dengan *copy* semantics, keutuhan data yang ingin ditulis sama dengan data waktu aplikasi ini memanggil sistem untuk menulis, tidak tergantung dengan perubahan yang terjadi pada buffer. Sebuah cara sederhana untuk sistem operasi untuk menjamin *copy* semantics adalah membiarkan sistem penulisan untuk mengkopi data aplikasi ke dalam buffer kernel sebelum mengembalikan kontrol kepada aplikasi. Jadi penulisan ke disk dilakukan pada buffer kernel, sehingga perubahan yang terjadi pada buffer aplikasi tidak akan membawa dampak apa-apa. Meng*copy* data antara buffer kernel data aplikasi merupakan sesuatu yang umum pada sistem operasi, kecuali overhead yang terjadi karena

operasi ini karena clean semantics. Kita dapat memperoleh efek yang sama yang lebih fisien dengan memanfaatkan virtual-memori mapping dan proteksi *copy*-on-wire dengan pintar.

2.10 *Video Conference*

Video conference adalah seperangkat teknologi telekomunikasi interaktif yang memungkinkankan dua pihak atau lebih di lokasi berbeda dapat berinteraksi melalui pengiriman dua arah *audio* dan *video* secara bersamaan [1]. Teknologi inti yang digunakan dalam konferensi *video* adalah sistem kompresi digital *audio* dan *video* *streaming* secara nyata. *Hardware* atau *software* yang melakukan kompresi disebut *codec*. Angka kompresi dapat dicapai hingga 1:500. Digital yang dihasilkan aliran 1s dan 0s dibagi menjadi paket label, yang kemudian dikirimkan melalui jaringan digital (biasanya ISDN atau IP). Penggunaan modem *audio* dalam saluran pengiriman memungkinkan penggunaan Plain *Old Telephone System* atau POTS, dalam beberapa aplikasi kecepatan rendah, seperti *video* telephony, karena POTS mengubah getaran digital ke atau dari gelombang analog dalam rentang spektrum *audio*.



Gambar 2.8 *Video Converence Point to Point*

Gambar 2.9 *Video Converence Multipoint*

Komponen lain yang dibutuhkan untuk sistem konferensi *video* meliputi:

1. *Video input*: kamera *video* atau webcam
2. *Video output*: monitor komputer, televisi atau proyektor
3. *Audio input*: mikrofon
4. *Audio output*: biasanya pengeras suara yang berkaitan dengan perangkat layar atau telepon
5. Data transfer: jaringan telepon analog atau digital, LAN atau Internet

2.10.1 Fitur *Video Conference*

Fitur mendasar dari sistem konferensi *video* profesional adalah *Acoustic Echo Cancellation* atau AEC. Echo dapat didefinisikan sebagai sumber gelombang interferensi yang direfleksikan dengan gelombang baru yang diciptakan oleh sumber. AEC adalah suatu algoritma yang mampu mendeteksi ketika suara atau ucapan masuk kembali ke *audio input* dari *codec* konferensi

video , yang berasal dari keluaran *audio* dari sistem yang sama setelah beberapa waktu. Apabila tidak diperiksa, dapat menyebabkan beberapa masalah seperti:

1. Mendengar kembali suara sendiri (biasanya tertunda secara signifikan).
2. Kuat gema, membuat saluran suara menjadi tidak berguna karena sulit untuk memahami.

Video conference dibagi menjadi dua jenis, *Point to Point* (satu ke satu) maupun *Multipoint* (satu ke banyak). Konferensi *video* bersama antara tiga tempat jauh atau lebih dimungkinkan melalui *Multipoint Control Unit* atau MCU. MCU merupakan jembatan yang menghubungkan panggilan dari beberapa sumber dalam cara yang mirip dengan panggilan *audio* konferensi. Semua pihak memanggil unit MCU, atau unit MCU juga dapat menghubungi pihak-pihak yang akan berpartisipasi, secara berurutan. Ada jembatan MCU untuk IP dan ISDN berbasis konferensi *video* . Ada MCU yang murni perangkat lunak, dan yang lain merupakan kombinasi dari perangkat keras dan perangkat lunak. Sebuah MCU dikarakterisasi berdasarkan jumlah panggilan simultan yang dapat ditangani, kemampuan MCU untuk melakukan perubahan protokol dan tarif data serta fitur-fitur lain. MCU dapat berdiri sendiri sebagai perangkat keras atau dapat dimasukkan ke dalam unit konferensi *video* terdedikasi. Beberapa sistem mampu melakukan konferensi *multipoin* tanpa MCU. Hal ini menggunakan teknik standar H.323 yang dikenal sebagai *decentralized multipoint*, dimana setiap stasiun dalam panggilan multipoin bertukar *video* dan *audio* secara langsung dengan stasiun lain tanpa pusat pengaturan. Keuntungan dari teknik tanpa MCU adalah *video* dan *audio* secara umum memiliki kualitas yang lebih tinggi karena tidak harus disampaikan melalui titik pusat. Selain itu, pengguna dapat membuat panggilan multipoin ad-hoc tanpa memerdulikan ketersediaan atau kontrol dari MCU.

Dampak pada bidang-bidang kehidupan antara lain :

2. Pendidikan

   Konferensi *video* memberikan kesempatan kepada siswa untuk belajar dengan berpartisipasi dalam bentuk komunikasi dua arah. Selain itu, guru dan dosen dari seluruh dunia dapat dibawa ke kelas di daerah terpencil. Siswa dari

beragam komunitas dan latar belakang dapat datang bersama untuk belajar tentang satu sama lain. Siswa mampu mengeksplorasi, berkomunikasi, menganalisis, dan berbagi informasi dan ide dengan satu sama lain.

Melalui konferensi *video* siswa dapat mengunjungi bagian lain dari dunia untuk berbicara dengan orang lain, mengunjungi kebun binatang, museum dan sebagainya, untuk belajar. Sekolah kecil dapat menggunakan teknologi konferensi *video* untuk menyatukan sumber daya dan mengajar kursus (seperti bahasa asing) yang tidak dapat ditawarkan.

3. Bisnis

   Konferensi *video* dapat memungkinkan individu di tempat-tempat jauh untuk mengadakan rapat dalam waktu singkat. Waktu dan uang yang dulu dikeluarkan dalam perjalanan dapat digunakan untuk pertemuan singkat. Teknologi seperti VoIP dapat digunakan dalam hubungan dengan konferensi *video* untuk mengaktifkan pertemuan bisnis tatap muka biaya rendah tanpa meninggalkan meja, terutama untuk bisnis dengan kantor tersebar luas. Teknologi ini juga digunakan untuk telecommuting, di mana karyawan bekerja dari rumah.

4. Obat dan kesehatan

   Konferensi *video* adalah teknologi yang sangat berguna untuk *telemedicine* dan aplikasi telenursing, seperti diagnosis, konsultasi, pengiriman gambar medis, dan lain-lain. Dengan menggunakan konferensi *video* , pasien dapat menghubungi perawat dan dokter dalam keadaan darurat atau situasi rutin, dokter dan paramedis profesional dapat mendiskusikan kasus di jarak yang jauh. Daerah pedesaan dapat menggunakan teknologi konferensi *video* untuk tujuan diagnostik sehingga menyelamatkan nyawa dan membuat penggunaan uang perawatan kesehatan menjadi lebih efisien. Perangkat khusus seperti mikroskop dilengkapi dengan kamera digital, *video* endoscopes perangkat USG, otoscopes, dan lain-lain dapat digunakan bersama-sama dengan peralatan konferensi *video* untuk mengirimkan data tentang pasien.

4. Hubungan media

   Konsep press *vide conference* dikembangkan pada Oktober 2007 oleh African Press Organization atau APO untuk mengizinkan wartawan Afrika internasional untuk berpartisipasi dalam konferensi pers tentang masalah pembangunan dan pemerintahan yang baik. Press *video* conference memungkinkan untuk mengatur sebuah konferensi pers internasional menggunakan konferensi *video* melalui Internet. Wartawan dapat berpartisipasi untuk sebuah konferensi pers internasional dari mana saja tanpa meninggalkan kantor. Wartawan hanya perlu duduk di depan komputer yang terhubung ke internet dan mengajukan pertanyaan-pertanyaan kepada pembicara.

2.10.2 Aplikasi *Video* Conference

Terdapat banyak aplikasi *video conference yang* tersedia, ada yang gratis dan ada juga yang berbayar. jenis-jenis aplikasi *video conference* diantaranya adalah :

1. *Google Plus Hangout*

   Dengan dukungan lebih dari 10 koneksi yang bisa berjalan bersamaan, software gratis ini mampu menghubungkan Anda dengan kawan-kawan Anda d jejaring sosial Google. Layanan ini juga terintegrasi dengan Google Drive yang memungkinkan Anda mengubah dokumen secara langsung. Terlebih lagi Anda dapat menyimpan Hangout Anda dan menyiarkannya agar dapat dilihat orang-orang nantinya. Selain dalam bentuk aplikasi web, *software* ini juga hadir untuk sistem operasi Android dan iOS.

2. *Skype*

   Skype adalah aplikasi *video* chat paling terkenal, tidak hanya hadir dengan fitur berkirim pesan instan tapi Skype juga menyuguhkan platform yang sudah solid, layanan telepon gratis, dan *video call*. *Skype* yang pada tahun 2011 diakuisisi oleh Microsoft, kini juga mendukung beberapa sistem operasi

komputer seperti Windows, Mac, dan Linux, seperti halnya sistem operasi mobile Android, iOS, dan Windows Phone.

3. *FaceTime Software Apple*

   Ini memungkinkan Anda melakukan *video chat* lintas gadget Apple. Dari iPhone ke MacBook, dari MackBook ke iPod, dari iPod ke iPad, dan seterusnya. Aplikasi ini menggunakan layanan data seluler atau Wi-Fi dan mendukung *video* chat resolusi tinggi. Aplikasi ini gratis dan hanya dapat digunakan pada produk-produk Apple saja.

4. ooVoo

   Dengan antarmuka berbasis browser dan aplikasi yang berdiri sendiri, ooVoo dapat mendukung 12 pengguna secara langsung dalam *video* group chat. Software ini mendukung sistem operasi komputer seperti Windows, Mac, dan juga sistem operasi mobile seperti iOS dan Android. Layanan ini juga mendukung perekaman *video chat* sehingga kita dapat menyebarkannya ke YouTube. Aplikasi ini hadir dalam dua versi yakni gratis dan berbayar.

2.10.3 Openmmeetings

apache Openmeetings adalah sebuah software open source yang dibuat untuk keperluan web conference.Web conference sendiri adalah sebuah wadah rapat / conference / konferensi yang dilakukan secara online.Implementasi dari web conference seperti rapat yang dilaksanakan oleh suatu perusahaan besar yang mempunyai banyak cabang dimana cabang-cabang tersebut tersebar di berbagai daerah yang berjauhan jaraknya.Jika perusahaan mengumpulkan perwakilan cabang dalam satu tempat dan satu waktu tertentu maka akan memakan banyak waktu,biaya dan tenaga , sehingga rapat tidak intensif.Dengan adanya web conference , perusahaan dapat mengajak semua cabang untuk melakukan rapat besar-besaran melalui web secara online yang dipasang di server perusahaan yang memungkin kesemuanya dapat membicarakan hal-hal penting dalam rapat.

2.11 Sistem Operasi IPCop

IPCop Router Appliance adalah suatu distribusi Linux yang menyediakan fitur simple-to-manage firewall appliance berbasis perangkat keras computer [6]. IPCop juga merupakan suatu stateful firewall dibuat berdasarkan pada Linux netfilter framework. Distro ini awalnya dikembangkan oleh tim yang mengembangkan Smoothwall Linux firewall, perkembangan selanjutnya, proyek IPCop dikembangkan dengan bebas, dan saat ini sudah terpisah sepenuhnya. IPCop sangat simple, dan memiliki fitur user-managed untuk mekanisme update security-nya. Bahkan cenderung mudah dipahami untuk yang para pemula, dan handal untuk yang sudah berpengalaman.Sebelum memulai instalasi IPCop perlu diperhatikan bahwa installer akan menggunakan seluruh kapasitas harddisk. Jadi pastikan tidak ada penting di dalam PC yang akan digunakan untuk instalasi. Spesifikasi hardware PC yang digunakan juga tidak perlu terlalu bagus.

IPCop masih akan berjalan lancar di atas PC dengan spesifikasi menengah ke bawah. Installer IPCop dapat diunduh dari situs resminya PCop menyediakan fasilitas yang lengkap untuk memanage jaringan lokal , seperti kemampuan memberian IP secara otomatis ke seluruh komputer di jaringan lokal (komputer client) kemampuan ini disebut dengan DHCP *server*, kemudian kemampuan sebagai proxy yang dapat menyimpan *file-file* dari website yang pernah diakses oleh client sehingga bila client mengakses website yang sama client tidak perlu mengambil (*download*) langsung dari situs tersebut di internet (*cache*). Hal ini akan membantu kecepatan akses dan menghemat bandwidth. IPCop juga memiliki kemampuan sebagai URL Filtering yaitu kemampuan untuk mem-blok akses ke situs-situs tertentu dengan berbagai kategori seperti situs porno, judi online, situs-situs yang mengandung konten berbahaya seperti virus, serta situs-situs lain yang ingin diblok. IPCop juga bisa membatasi waktu akses internet di perusahaan atau sekolah, misalnya ingin mengaktifkan internet untuk client pada jam 12.00 - 13.00 (Jam istirahat) kita bisa melakukannya dengan perangkat tambahan yg dimiliki IPCop (*Addons*) yaitu CoFilter.

2.12 Wireshark

Alat ukur yang digunakan dalam laporan ini ialah *network protocol analyzer* Wireshark. *Network protocol analyzer* adalah perangkat yang digunakan untuk mengetahui kondisi trafik yang ditransmisikan pada jaringan [7]. Data paket trafik yang diperoleh dapat digunakan untuk menganalisis performa paket dan jaringan. Program yang digunakan adalah Wireshark. Wireshark merupakan perangkat lunak yang bersifat *open source* dapat di-*download* langsung dari internet.

Sebagai salah satu *network protocol analyzer*, tentu saja Wireshark memiliki beberapa fitur. Berikut merupakan fitur utama Wireshark :

1. Multi *platform* bisa digunakan pada Unix dan Windows.
2. *Open source* dan gratis .
3. Dapat menampilkan dan menyimpan paket yang di-*capture*.
4. Mendukung beberapa macam protokol jaringan. Protokol – protokol tersebut antara lain TCP, IP, RTP, UDP, RTCP, RTSP, dan lain lain.