BAB II
TINJAUAN PUSTAKA

2.1 Server

Server adalah sistem komputer yang menyediakan jenis layanan tertentu dalam sebuah jaringan komputer. Sebuah server didukung dengan prosesor yang bersifat scalable dan RAM yang cukup besar, juga dilengkapi dengan sistem operasi khusus. Server juga bertugas untuk menjalankan software administrative yakni, software yang mengontrol akses terhadap jaringan dan sumber daya yang terdapat di dalamnya. Di dalam server umumnya terdapat berbagai macam servis yang menggunakan arsitektur Client-Server. Service yang di berikan antara lain Mail Server, DHCP Server, HTTP Server, DNS Server, FTP server dan lain-lain.

2.1.1 Web Server

Web server adalah sebuah software yang memberikan layanan berbasis data dan berfungsi menerima permintaan dari HTTP atau HTTPS pada klien yang dikenal dengan nama web browser. Dalam hal ini, web browser mengirimkan kembali hasilnya dalam betuk dokumen HTML. Web browser akan melakukan transfer berkas komunikasi yang telah ditentukan sedemikian rupa. Kita akan mengetikkan URL tersebut di peramban atau browser kemudian menekan tombol enter, tanpa kita ketahui proses yang terjadi di belakang layar atau di dalam browser itu sendiri, maka akan munculah halaman website di layar monitor komputerkita. Proses yang akan terjadi pada browser adalah browser akan membentuk koneksi dengan web server, meminta halaman website dan menerimanya. Web server kemudian mengecek permintaan tersebut apakah tersedia atau tidak.

Halaman yang diminta berupa teks, video, gambar, dan file. Pemanfaatan web browser berfungsi untuk mentransfer seluruh aspek pemberkasaan dalam sebuah halaman web termasuk yang di dalam berupa teks, gambar, video, dan file. Apabila tersedia, maka web server akan mengirimkan data kepada browser. Apabila permintaan tidak ditemukan atau terjadi error maka web server akan mengirimkan pesan error kepada browser. Pembentukan koneksi, permintaan data, penerimaan data dari browser ke web server diatur dalam sebuah kode RFC2616. RFC2616 mencantumkan status web server dalam bentuk kombinasi tiga angka yang

memiliki arti berbeda-beda. Status ini muncul di peramban saat kita mengakses web server tertentu.

2.1.2 Media Server

Media server menangani pengolahan aset digital yang diolah sedemikian rupa yang kemudian di distribusi kepada clien. Media server bisa diakses oleh semua perangkat yang berada pada jaringan yang terhubung dengan media server tersebut. Media server bertugas sebagai media yang mengolah aset digital (DAM) yang menggunakan NAS sebagai media penyimpanan dan web server sebagai interface yang digunakan untuk bertinteraksi dengan user. Sebuah media server bisa menunjuk pada alat komputer khusus atau perangkat lunak aplikasi khusus, mulai dari sebuah komputer kecil pribadi atau NAS (Network Attached Storage) untuk rumah, khususnya untuk menyimpan berbagai mediadigital (seperti video digital/film, audio/musik, dan file gambar).

Dalam masalah ini media server berisi file berupa video. Video adalah teknologi untuk menangkap, merekam, memproses, mentransmisikan dan menata ulang gambar bergerak. Biasanya menggunakan film seluloid, sinyal elektronik, atau media digital. File video memiliki format yang berbeda-beda, bergantung pada aplikasi yang digunakan untuk menjalankannya (Player). Beberapa contoh format file video yang dapat dijalankan melalui komputer maupun notebook, yaitu:

1. ASF (Advanced Streaming Format / Advanced System Format)
2. AVI (Audio Video Interleaved)
3. MPEG
4. WMV (Windows Media Video)
5. 3GP (3GPP format file)
6. Flash Video
7. MP4

Satu-satunya yang diperlukan untuk server media adalah metode penyimpanan media dan koneksi jaringan dengan bandwidth yang cukup untuk memungkinkan akses ke media. Tergantung pada penggunaan dan aplikasi yang dijalankan, media server mungkin memerlukan sejumlah besar RAM, atau multicore CPU yang kuat.

2.2 Video Wall

Video wall umumnya di tampilkan dalam satu dinding besar, merupakan gabungan dari beberapa projector/ led monitor, dapat berupa gabungan dari 3/6/9/ lebih projector/led monitor menampilkan gambar dari berbagai sumber input signal seperti signal Composite, RGB, component, HDMI. Ditampilkan di video wall dalam berbagai bentuk dan ukuran. Jadi dengan 1 video wall bisa menampilkan 1 gambar penuh salah satu sumber signal input atau 1 layar besar/led besar dengan berbagai ukuran tampilan signal input.

Video wall/wall display biasanya difungsikan sebagai digital signage ukuran besar, menampilkan Company Profile, produk, iklan, dapat juga berupa gambar cctv camera, data keuangan, data lain, gambar yang dipakai di ruang control. Video wall ditempatkan di lobby perusahaan, stasiun kereta, airport, shopping mall, atau lokasi umum misalnya untuk iklan/informasi. Dengan semangkin berkembangnya teknologi elektronika dan led monitor membuat Video wall sering dipakai dengan ukuran yang lebih besar lagi dan variasi tampilan yang lebih menarik lagi.

2.3 Real Time Protokol (RTP)

Real Time Protokol (RTP) umumnya digunakan dalam jaringan IP. RTP dirancang untuk menyediakan fungsi transport jaringan dari ujung ke ujung untuk mengirimkan data secara *real-time*. Misalnya audio dan video, melalui layanan *multicast* atau *unicast.* Frame RTP berisi informasi-informasi untuk mengidentifikasi dan mengatur tiap individu dari endponit ke enpoint. Informasi ini adalah *timestamps, sequence number,* dan *conversation synchronization. Timestamps* yang digunakan untuk pengaturan waktu suara percakapan agar terdengar seperti bagaimana yang diucapkan, dan *sequence number* digunakan

untuk pengiriman paket data dan mendeteksi adanya paket data yang hilang. *Packet Header* dari RTP dapat dilihat pada gambar berikut ini.

V	P	X	CC	M	PT	Sequance Number	Timestamps	SSRC

Gambar 0.1 Packet Header RTP

Penjelasan :

- *Version*(V), merupakan versi dari RTP
- *Padding* (P), pada umumnya digunakan jika media *stream* dienkripsi
- *Extension* (X), merupakan ekstensi tambahan yang mengikuti *header* yang dibuat oleh tipe *payload* tertentu
- *CSCR Count* (CC)
- *Marker* (M), berfungsi menandai awal dari frame baru pada video
- *Payload Type* (PT), merupakan 7-bit *field* yang menandai *codec* yang digunakan
- *Sequence Number* berfungsi untuk mendeteksi hilangnya *packet* dimana jumlah *sequence number* akan bertambah untuk setiap paket RTP yang dikirim
- *Timestamps* mengindikasi waktu relatif ketika *payload* di-*sample*
- *Synchronization Source Identifer* (SSCI), berfungsi mengidentifikasi pengirim dari RTP

RTP didesain untuk digunakan pada transport layer, namun demikian RTP digunakan diatas UDP, bukan pada TCP karena TCP tidak dapat beradaptasi pada pengiriman data yang *real-time,* dengan keterlambatan yang relatif kecil seperti pada pengiriman data komunikasi suara. Dengan menggunakan UDP yang dapat mengirimkan paket IP secara *multicast,* RTP stream yang dibentuk oleh satu terminal dapat dikirimkan kebebrapa terminal tujuan. Oleh karena itu, informasi RTP dienkapsulasi dalam paket UDP. Jika paket RTP hilang (*lost)* atau di drop di jaringan, maka RTP tidak akan melakukan *retransmission.* Hal ini dilakaukan agar *user* tidak terlalu lama menunggu atau delay. Oleh karena itu, jaringan harus didesain sebaik mungkin agar *lost packet* tidak terjadi.

2.4 Quality of Service (QoS)

Quality of Service (QoS) adalah kemampuan suatu jaringan untuk menyediakan layanan yang baik dengan menyediakan *bandwith,* mengatasi *jitter* dan *Delay*. Parameter QoS adalah *latency, jitter, packet loss, throughput, echo cancellation* dan PDD. QoS sangat ditentukan oleh kualitas jaringan yang digunakan.Terdapat beberapa factor yang dapat menurunkan nilai QoS, seperti : *Distorsi*, dan *Noise*. Performa jaringan komputer dapat bervariasi akibat dari beberapa masalah, seperti halnya masalah *bandwidth*, *latency* dan *Jitter*, yang dapat membuat efek yang cukup besar bagi banyak aplikasi.

Sebagai contoh, *video streaming* dapat membuat pengguna kesal ketika paket data aplikasi tersebut berjalan dengan *bandwidth* yang tidak cukup, dengan *latency* yang tidak dapat diprediksi, atau *Jitter* yang berlebih. Beberapa fitur *Quality of Service* (QoS) dapat menangani masalah diatas, dapat menurunkan *latency* dengan mengendalikan pengiriman paket data dan membatasi paket data tertentu dan *Jitter* dapat diprediksi dan dicocokkan dengan kebutuhan aplikasi yang digunakan di dalam jaringan tersebut.

Teknologi QOS ini adalah teknologi yang memungkinkan administrator jaringan untuk dapat menangani berbagai efek akibat terjadinya kemacetan pada lalu lintas aliran paket dari berbagai layanan yaitu dengan mengatur dan memberikan prioritas pada jaringan tersebut, ini akan mengoptimalkan aplikasi yang kritis atau yang memiliki *delay* sensitif untuk dapat berjalan sebagaimana mestinya. Dengan implementai QOS, *network administrator* akan memiliki fleksibilitas yang tinggi untuk ,mengontrol aliran dan kejadian-kejadian yang ada di aliran paket pada jaringan.

2.4.1 Parameter QOS

Performansi mengacu ke tingkat kecepatan dan keandalan penyampaian berbagai jenis beban data di dalam suatu komunikasi. Performansi merupakan kumpulan dari beberapa parameter teknis yaitu :

1. Delay

   Delay adalah waktu yang di butuhkan untuk menempuh jarak dari asal ke tujuan. *Delay* dapat dipengaruhi oleh jarak, media fisik atau juga waktu proses yang lama. *Delay* versi *Telecommunications and Internet Protocol Harmonization Over Networks* (TIPHON) dikelompokkan menjadi empat kategori seperti terlihat pada Tabel 2.4.1

$$\text{Delay} = \frac{total\ delay}{total\ paket\ yang\ di\ terima}$$

Tabel 2.1 Delay

Kategori Degradasi	**Delay**
Sangat Bagus	<150ms
Bagus	150 ms s/d 300 ms
Sedang	300 ms s/d 450 ms
Buruk	>450 ms

2. Jitter

   Hal ini Jitter diakibatkan oleh variasi-variasi dalam panjang antrian, dalam waktu pengolahan data, dan juga dalam waktu penghimpunan ulang paket-paket di akhir perjalanan jitter. Jitter lazimnya disebut variasi Delay ,berhubungan erat dengan latency, yang menunjukkan banyaknya variasi Delay pada taransmisi data di jaringan.

$$\text{Jitter} = \frac{total\ variasi\ delay}{total\ paket\ yang\ di\ terima - 1}$$

Kategori Degradasi	**Jitter**
Sangat Bagus	0 ms
Bagus	0 ms s/d 75 ms
Sedang	75 ms s/d 125 ms
Buruk	125 ms s/d 225 ms

Tabel 0.2Jitter

3. Packet loss

   Merupakan suatu parameter yang menggambarkan suatu kondisi yang menunjukkan jumlah total paket yang hilang, dapat terjadi karena *collision* dan *congestion* pada jaringan dan hal ini berpengaruh pada semua aplikasi karena *retransmisi* akan mengurangi efisiensi jaringan secara keseluruhan meskipun jumlah *bandwidth* cukup tersedia untuk aplikasi-aplikasi tersebut. Umumnya perangkat jaringan memiliki *buffer* untuk menampung data yang diterima. Jika terjadi kongesti yang cukup lama, *buffer* akan penuh, dan data baru tidak akan diterima.

$$\text{Packet Loss } = \frac{\text{paket dikirim } - \text{ paket diterima}}{\text{paket di kirim}} \times 100\%$$

Tabel 0.3 Packet Loss

Kategori Degradasi	**Packet Loss**
Sangat Bagus	0 %
Bagus	3%
Sedang	15%
Buruk	25%

4. Throughtput

   Throughput adalah kecepatan (*rate*) transfer data efektif, yang diukur dalam bps. *Troughput* merupakan jumlah total kedatangan paket yang sukses yang di amati pada *destination* selama *interval* waktu tertentu dibagi oleh durasi *interval* waktu tersebut.

$$\text{Throughput} = \frac{\text{jumlah data yang di terima}}{\text{waktu pengiriman data}}$$

2.5 Wireshark

Wiresrak adalah sebuah *Network Protocol Analyzier* untuk berbagai kebutuhan analisis kerja jaringan. Wireshark difungsikan untuk menangkap setiap data yang lewat melalui salah satu *network interface*dari komputer dimana aplikasi tersebut terpasang. Dengan kata lain wireshark digunakan untuk mengetahui kejadian yang terjadi pada saat kita melakukan interaksi dengan internet. Dengan wireshark dapat dilihat proses-proses berbagai format protokol pun akan mudah ditangkap dan dianalisa.

Wireshark merupakan suatu software yang mengerti struktur dari banyak protokol yang berbeda. Karena wireshark merupakan pcap untuk menangkap paket data, wireshark hanya dapat menangkap paket data dari network yang didukung pcap. Umumnya, wireshark digunakan ileh administrator jaringan komputer untuk memecahkan masalah jaringan, memeriksa masalah keamanan jaringan, dan sebagian pengembang untuk *debug* implementasi protokol jaringan dan belajar internal protokol jaringan. Hal ini lebih mudah dilakukan dan di implementasikan pada jaringan lokal. Hasil yang ditangkap oleh wireshark dapat digunakan sebagai perbandingan antar jaringan.