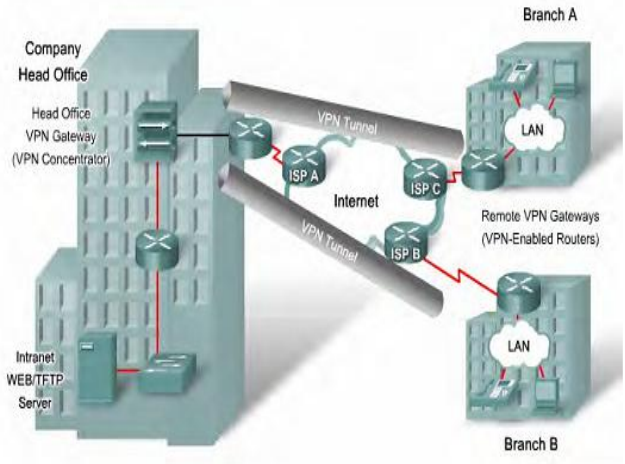
BAB II
DASAR TEORI

2.1 *VIRTUAL PRIVATE NETWORK* (VPN)

Isu yang kerap kali didengungkan terkait jaringan dengan skala besar seperti WAN adalah permasalahan perfoma dan keamanan. Sering kali ketika harus membuat jalur komunikasi antar tempat-tempat yang terpisah cukup jauh maka harus menggunakan fasilitas jaringan publik untuk menekan biaya. Jelas penggunaan jaringan publik akan jauh lebih murah ketimbang membangun jaringan sendiri dalam skala geografi yang cukup luas, namun cara ini justru menciptakan kerentanan keamanan dalam komunikasi jaringan. *Virtual private network* (VPN) muncul sebagai salah satu solusi untuk menciptakan jaringan komunikasi yang aman antara dua titik yang terhubung melalui jaringan public [1].

Ide dasar dari VPN adalah *Tunneling*, sebuah teknologi yang memungkinkan terciptanya saluran privat virtual didalam jaringan publik. *Tunnel* di dalam dunia jaringan diartikan sebagai suatu cara untuk meng-enkapsulasi atau membungkus paket IP didalam paket IP yang lain. Paket yang dikirim didalam *tunnel* ini dienkripsi dengan suatu format tertentu oleh protokol VPN lalu

dikirim dari *client* ke *server* pada VPN *tunnel*. Ketika paket sampai di node ujung *tunnel*, kemudian paket ini akan di dekripsi terlebih dahulu. Proses enkripsi-dekripsi pada VPN yang membutuhkan waktu akan menambah *delay* pada jaringan, namun bagaimanapun VPN memberi keamanan dalam komunikasi didalam jaringan [1]. Gambar 2.1. merupakan gambar dari proses *tunneling* VPN pada WAN.



Gambar 2.1. VPN *Tunnel* pada WAN [1]

VPN merupakan sebuah teknologi komunikasi yang memungkinkan seorang pegawai yang berada di dalam kantor terkoneksi ke jaringan publik dan menggunakannya untuk bergabung ke jaringan lokal. Dengan menggunakan jaringan publik ini, seorang pegawai dapat tergabung ke dalam jaringan lokal, mendapatkan hak dan pengaturan

yang sama seperti ketika pegawai tersebut berada di kantor [2].

VPN dapat terjadi antara dua *end-system* atau dua komputer atau bisa juga antara dua atau lebih jaringan yang berbeda. Data yang dikirim dienkapsulasi dengan *header* untuk mendapatkan koneksi *point-to-point* sehingga data dapat melewati jaringan publik dan dapat mencapai akhir tujuan. Sedangkan untuk mendapatkan koneksi bersifat *private*, data yang dikirimkan dienkripsi terlebih dahulu untuk menjaga kerahasiaannya sehingga paket yang tertangkap ketika melewati jaringan publik tidak terbaca karena harus melewati proses dekripsi [2].

2.1.1. Enkripsi dan Dekripsi

a. Enkripsi

Enkripsi merupakan teknik untuk mengamankan data yang dikirimkan dengan mengubah data tersebut ke dalam bentuk sandi-sandi yang hanya dimengerti oleh pihak pengirim dan pihak penerima data. Enkripsi yang banyak digunakan saat ini adalah enkripsi kunci simetris dan enkripsi kunci publik [2].

1) Kunci Simetris

Pada enkripsi jenis ini, setiap komputer memiliki kunci rahasia atau kode yang dapat

digunakan untuk mengenkripsi informasi sebelum informasi tersebut dikirim ke komputer lain melalui jaringan. Kunci yang digunakan untuk mengenkripsi data sama dengan yang digunakan untk mengenkripsi data. Oleh karena itu, kunci tersebut harus dimiliki kedua komputer [2].

2) Kunci publik

Enkripsi ini menggunakan kombinasi kunci privat dan kunci publik. Kunci privat hanya diketahui oleh pihak pengirim informasi. Sedangkan kunci publik dikirim ke pihak penerima. Untuk mendekripsi informasi, pihak penerima harus menggunakan kunci publik dan kunci privat. Kunci privat penerima berbeda dengan kunci privat pengirim, dan hanya penerima saja yang mengetahui [2].

b. Dekripsi

Dekripsi adalah kebalikan dari enkripsi yaitu teknik untuk mengubah data yang tersamar kembali menjadi data yang bisa dibaca atau dimengerti oleh pihak penerima [2].

2.1.2. Fungsi Utama VPN

1. *Confidentially* (Kerahasiaan)

   Teknologi VPN memiliki sistem kerja mengenkripsi semua data yang lewat melaluinya. Dengan adanya teknologi enkripsi ini, maka kerahasaian data menjadi lebih terjaga. Biarpun ada pihak yang dapat menyadap data, namun belum tentu pihak tersebut dapat membacanya dengan mudah. Dengan menerapkan sistem enkripsi ini, tidak ada satupun pihak lain yang dapat mengakses dan membaca isi jaringan data dengan mudah [2].

2. *Data Integrity* (Keutuhan Data)

   Ketika melewati jaringan internet, data sebenarnya sudah berjalan sangat jauh melintasi berbagai negara. Di tengah perjalan, apapun bisa terjadi terdapat isi data, baik itu hilang, rusak, bahkan dimanipulasi oleh pihak lain. VPN memiliki teknologi yang dapat menjaga keutuhan data yang dikirim agar sampai ke tujuannya tanpa cacat, hilang, rusak, atau dimanipulasi oleh orang lain [2].

3. *Origin Authentication* (Autentikasi Sumber)

   Teknologi VPN memiliki kemampuan untuk melakuka autentikasi terhadap sumber-sumber pengirim data yang akan diterima. VPN akan

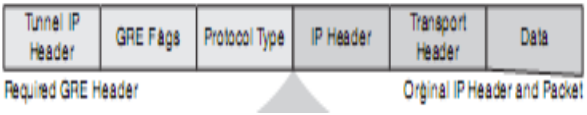
melakukan pemeriksaan terhadap semua data yang masuk dan mengambil informasi *source* datanya. Kemudian alamat *source* data ini akan disetujui jika proses autentikasinya berhasil. Dengan demikian, VPN menjamin semua data yang dikirim dan diterima berasal dari sumber yang semestinya. Tidak akan ada data yang dipalsukan atau dikirimkan oleh pihak-pihak lain [2].

2.1.3. GRE (*Generic Routing Encapsulation*)

VPN dibangun untuk membuat *tunnel* privat melewati sistem jaringan publik untuk meneruskan data ke *site* yang di-*remote*. Salah satu jenis *tunnel* yang dapat digunakan pada VPN adalah GRE (*Generic Routing Encapsulation*). GRE adalah cara yang paling sederahana untuk menghasilkan sebuah jalan untuk melakukan encapsulasi berbagai protokol *layer* jaringan melalui berbagai protokol *layer* jaringan lainnya. GRE mengijinkan *router* untuk bertindak seakan *router* memiliki sebuah koneksi *point-to-point* virtual ke *router* lain. *Tunnel* GRE mengijinkan *routing* protokol (seperti RIP dan OSPF) untuk dilanjutkan ke *router* lain melewati internet [3].

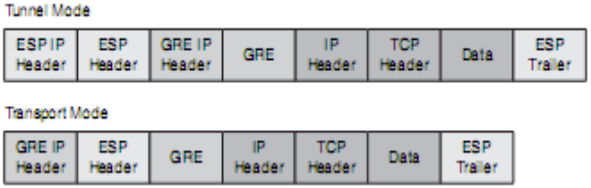
Tunnel GRE dibangun dengan membuat titik awal *tunnel* dan titik akhir *tunnel*. Sebagai contoh,

tunnel GRE dapat mengkoneksikan *router* A ke *router* B dan menyediakan jalur data diantara keduanya. Jalur data yang dihasilkan tidak terjamin keamanannya. Oleh karena itu IPsec harus digunakan di dalam *tunnel* GRE untuk menciptakan keamanan data. Data di-*routing* kan oleh sistem ke titik akhir *tunnel* GRE dengan jalur yang telah dibangun di dalam *routing* tabel. Ketika sebuah data diterima oleh titik awal GRE, data akan di enkapsulasi di dalam sebuah GRE *header* dan dilanjutkan menuju ke titik akhir *tunnel* yang telah dikonfigurasi [3].



Gambar 2.2. GRE *Header* [4]

Tunnel GRE menawarkan keamanan yang lemah. Meskipun di dalam GRE itu sendiri terdapat mekanisme dasar enkripsi, akan tetapi kunci dari enkripsi tersebut dibawa bersamaan dengan paket di mana hal ini dapat menghancurkan tujuan dari enkripsi itu sendiri. Oleh karena itu ditambahkan protokol IPsec di dalam GRE *tunnel*. [4]



Gambar 2.3. Format *Header* GRE-IPsec [4]

IPsec adalah standart keamanan untuk pengguna komunikasi berbasis internet protokol (IP) dengan cara enkripsi atau authentikasi semua paket IP yang lewat. IPsec menyediakan keamanan pada level *layer network*. IPsec diimplementasikan ke dalam *layer network*, yaitu *layer* ketiga pada *layer* OSI yang mengerjakan layanan *routing* jaringan, *flow control*, *segmentation*, dan *error control functions* [2].

Berdasarkan fungsinya, di dalam IPsec terdapat dua protokol yang berjalan di belakang IPsec, yaitu [2]:

1. *Aunthetication Header*

   Protokol ini menyediakan layanan *aunthetication*, *integrity*, *replay protection* pada *header* IP namun tidak menyediakan layanan *confidentiality*.

2. *Encapsulating Security Payload*

   Menyediakan layanan *Authentication*, *integrity*, *replays protection*, dan *confidentiality* terhadap data (ESP melakukan pengamanan

data terhadap segala sesuatu dalam paket data setelah *header*).

2.1.4. Keuntungan dan Kerugian VPN

Ada beberapa keuntungan yang dapat diperileh dengan menggunakan VPN, antara lain [2]:

1. Jangkauan jaringan lokal yang dimiliki suatu perusahaan akan menjadi luas, sehingga perusahaan dapat mengembangkan bisnisnya di daerah lain. Waktu yang dibutuhkan untuk menghubungkan jaringan lokal ke tempat lain juga semakin cepat, karena proses instalasi infrastruktur jaringan dilakukan dari perusahaan atau kantor cabang yang baru.
2. VPN dapat mengurangi biaya pembuatan jaringan karena tidak membutuhkan kabel (*leased line*) yang panjang. VPN menggunakan internet sebagai media komunikasinya. Media internet telah tersebar ke seluruh dunia karena internet digunakan sebagai media komunikasi publik yang bersifat terbuka.
3. Biaya operasional perusahaan juga akan berkurang bila menggunakan VPN. Hal ini disebabkan karena pelayanan akses *dial-up*

dilakukan oleh ISP (*Internet Service Provider*), bukan oleh perusahaan yang bersangkutan.

4. VPN memberi kemudahan untuk diakses dari mana saja, karena VPN terhubung ke internet. Sehingga pegawai *mobile* dapat mengakses jaringan khusus perusahaan di manapun dia berada. Selama *user* bisa mendapatkan akses internet ke ISP terdekat, maka *user* tersebut tetap dapat melakukan koneksi dengan jaringan khusus perusahaan.

VPN juga memiliki kelemahan, yaitu [2]:

1. VPN membutuhkan perhatian yang serius pada keamanan jaringan publik (internet). Oleh karena itu diperlukan tindakan yang tepat unruk mencegah terjadinya hal-hal yang tidak diinginkan seperti penyadapan, *hacking*, dan tindakan *cyber crime* pada jaringan VPN.
2. Dengan adanya proses keamanan pada VPN, maka *delay* jaringan yang dihasilkan akan meningkat karena adanya waktu untuk melakukan proses keamanan tersebut.
3. Kecepatan dan keandalan transmisi data melalui internet yang digunakan sebagai media komunikasi jaringan VPN tidak dapat diatur

oleh pihak pengguna jaringan VPN, karena trafik yang terjadi di internet melibatkan semua pihak pengguna internet di seluruh dunia.

2.2 LAYANAN

2.2.1. FTP

File transfer protocol (FTP) adalah suatu protokol yang berfungsi untuk tukar-menukar *file* dalam suatu *network*. Dua hal yang penting dalam FTP adalah FTP *Server* dan FTP *Client* [5].

FTP *server* adalah suatu *server* yang menjalankan *software* yang berfungsi untuk memberikan layanan tukar menukar *file* dimana *server* tersebut selalu siap memberikan layanan FTP apabila mendapat permintaan dari FTP *client* [5].

FTP *client* adalah komputer yang me-*request* koneksi ke FTP *server* untuk tujuan tukar menukar *file*. Setelah terhubung dengan FTP *server*, maka *client* dapat men-*download*, meng-*upload*, me-*rename*, men-*delete*, dan lain sebagainya sesuai dengan *permission* yang diberikan oleh FTP *server* [5].

Tujuan dari FTP *server* adalah sebagai berikut [5]:

a. Untuk tujuan *sharing* data

b. Untuk menyediakan *indirect* atau *implicit remote computer*
c. Untuk menyediakan tempat penyimpanan bagi *user*
d. Untuk menyediakan transfer data yang efisien

Mode text yang dipakai untuk transfer data adalah format ASCII atau format *binary*. Secara *default*, FTP menggunakan mode ASCII dalam transfer data. Karena pengirimannya tanpa enkripsi, *username*, *password*, data yang ditransfer, maupun perintah yang dikirim dapat di-*sniffing* oleh orang dengan menggunakan *protocol analyzer* (*sniffer*) [5].

2.2.2. VoIP

VoIP (*Voice Over Internet Protocol*) adalah teknologi yang mampu melewatkan "panggilan suara", video, dan data melalui jaringan IP. Bentuk panggilan analog dikonversikan menjadi bentuk digital dan dijalankan sebagai data oleh internet protokol. Jaringan IP sendiri merupakan jaringan komunikasi data berbasis *packet switch*, sehingga bisa melakukan panggilan menggunakan jaringan IP atau Internet [6].

Perkembangan teknologi khususnya teknologi informasi membawa perubahan yang sangat mendasar bagi dunia telekomunikasi. Dalam beberapa tahun

terakhir telah banyak dilakukan penelitian untuk mengembangkan evolusi teknologi paketisasi untuk transmisi trafik suara melalui jaringan data. Sebagai hasilnya adalah suatu teknologi baru yang disebut teknologi VoIP [6].

Untuk dapat melaksanakan tugasnya menyalurkan sinyal suara, VoIP harus didukung oleh beberapa komponen, di antaranya adalah sebagai berikut:

a. Terminal

Terminal adalah peralatan yang berhubungan langsung dengan pemakai aplikasi. Peralatan terminal yang dapat digunakan untuk melakukan hubungan VoIP bermacam-macam, diantaranya yaitu *headphone*, pesawat telepon digital, pesawat telepon analog, dan komputer [6].

b. *Gateway* VoIP

Gateway VoIP adalah *interface* antara telepon tradisional dengan *network* IP, memungkinkan interoperabilitas teknologi antara jaringan yang berbeda untuk dapat saling bekomunikasi. *Gateway* ini berupa komputer atau *router* yang berfungsi untuk menghubungkan panggilan telepon ke jaringan IP [6].

c. *Network* IP

Network IP adalah jaringan yang digunakan untuk mentransimisikan trafik suara, dapat berupa Internet, Intranet, atau VPN. Jaringan IP sebenarnya adalah gabungan *router-router* yang saling berkomunikasi dengan bahasa yang sama yaitu TCP/IP. Komponen jaringan IP ini adalah *router* dan media transmisi [6].

Router mempunyai kemampuan untuk memilihkan jalur terpendek dan terbaik bagi semua paket menuju *gateway* tujuan. Paket yang sampai ke *router* diantrikan dalam *buffer* tunggu, diproses dan disalurkan ke *buffer* keluaran terlebih dahulu [6].

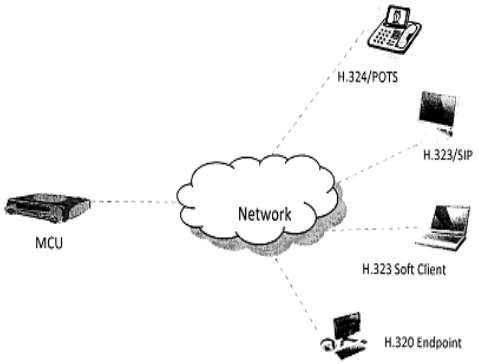
2.2.3. *Video Conferencing*

Dalam perkembangan teknologi komunikasi, dimana tuntutan kebutuhan pelayanan bagi pengguna jasa komunikasi makin tinggi, dalam penyampaian ide dan pendapat tidak hanya audio saja akan tetapi diperlukan juga visualnya, oleh karena itu dibutuhkan komunikasi yang dapat mengirimkan audio visualnya [7].

Video conference memakai telekomunikasi audio dan video untuk membawa orang ke tempat berbeda dalam waktu yang bersamaan untuk pertemuan. Ini bisa

sama sederhananya dengan percakapan di antara dua orang di jabatan pribadi (titik-ke-titik) atau melibatkan beberapa tempat (multi-titik) dengan lebih dari satu orang di kamar besar di tempat berbeda. Selain audio dan pengiriman visual, *video conferencing* bisa digunakan untuk berbagi dokumen, informasi yang diperlihatkan dengan komputer dan *whiteboards* [7].

Saat ini *video conference* sudah banyak di gunakan dalam berbagai bidang kehidupan. Misalnya, untuk bisnis, pendidikan, militer dan lain sebagainya. Didalam pendidikan *video conference* ini digunakan untuk keperluan pendidikan jarak jauh, yang dapat dimanfaatkan untuk memberikan materi pelajaran dari Guru atau Dosen kepada siswa (anak didik) yang tidak terbatas oleh tempat dan jarak [7].



Gambar 2.4. Konfigurasi *Video Conference* [7]

Gambar 2.4. merupakan konfigurasi dari *Video Conference* beserta beberapa perangkat yang digunakan. Perangkat *Video Conference* adalah perangkat teknologi telekomunikasi interaktif yang memungkinkan dua pihak atau lebih di lokasi berbeda dapat berinteraksi melalui pengiriman dua arah audio dan video secara bersamaan, serta salah satu pihak dapat melakukan presentasi dan dapat dilihat oleh masing-masing pihak, begitupun sebaliknya [8].

MCU (*Multipoint Control Unit*) ini di gunakan ketika akan melakukan *video conference* dengan lebih dari 2 peserta yang mana membutuhkan komunikasi multi*point*. MCU ini dapat memudahkan *admin* dalam mengatur komunikasi yang melibatkan banyak *user*. Sedangkan untuk *user* yang ingin melihat konferensi dapat juga mengaksesnya ke dalam MCU dan tampilannya berbentuk *streaming* [7].

Perangkat keras *endpoint* adalah perangkat yang digunakan untuk melakukan *video conference*. Dalam setiap *video conference* dibutuhkan perangkat keras end*point* agar dapat melakukan komunikasi visual baik itu *point* to *point* maupun multi*point* [7].

2.2.4. HTTP

Hypertext Transfer Protocol (HTTP) adalah sebuah protokol jaringan lapisan aplikasi yang digunakan untuk sistem informasi terdistribusi, kolaboratif, dan menggunakan *hipermedia*. Penggunaannya banyak pada pengambilan sumber daya yang saling terhubung dengan tautan, yang disebut dengan dokumen hiperteks, yang kemudian membentuk *World Wide Web* [9].

2.3 *QUALITY OF SERVICES*

Quality of Service (QoS) merupakan kemampuan jaringan untuk menyediakan *service* yang lebih baik pada suatu trafik tertentu mulai berbagai macam teknologi meliputi jaringan IP, *frame relay*, dan lain sebagainya. Elemen QoS tergantung dari informasi yang ditransmisikan (*voice*, data atau video) [1].

Dalam skripsi ini akan dilihat juga pengaruh teori antrian terhadap beberapa parameter QoS seperti *Delay*, *Delay Variation*, *Traffic Dropped*, dan *Throughput*.

1. *Delay*

   Delay adalah waktu tunda saat paket yang diakibatkan oleh proses transmisi dari satu titik lain yang menjadi tujuannya. *Packet delay* dapat

menyebabkan kualitas suara menjadi turun. Jika *delay* tidak diminimalkan maka sinyal suara yang diterima akan menyebabkan kualitas yang buruk akibat dari akumulasi seluruh *delay* yang terjadi di dalam jaringan [1].

2. *Delay Variation*

   Delay variation atau yang sering disebut dengan *jitter* merupakan masalah khas dari *packet switched network. Jitter* didefinisikan sebagai variasi *delay* yang diakibatkan oleh panjang *queue* dalam suatu pengolahan data dan *reassemble* paket-paket data di akhir pengiriman akibat kegagalan sebelumnya [1].

3. *Traffic Dropped*

   Traffic dropped merupakan besarnya trafik yang di-*drop* di dalam keseluruhan jaringan pada semua *node*. Semakin besar nilai *traffic dropped* dalam suatu jaringan, maka semakin jelek kualitas jaringan tersebut. Nilai *traffic dropped* pada dasarnya adalah sama dengan nilai *packet loss*. Yang membedakan kedua nilai tersebut adalah pada *packet loss ratio*, nilainya berbentuk presentase berapa nilai paket yang di-*dropped* di dalam jaringan dibandingkan dengan trafik yang dikirim. Pada *traffic dropped*, nilainya berbentuk

jumlah nilai trafik yang di-*dropped* di dalam jaringan sehingga dapat mempermudah dalam proses analisa.

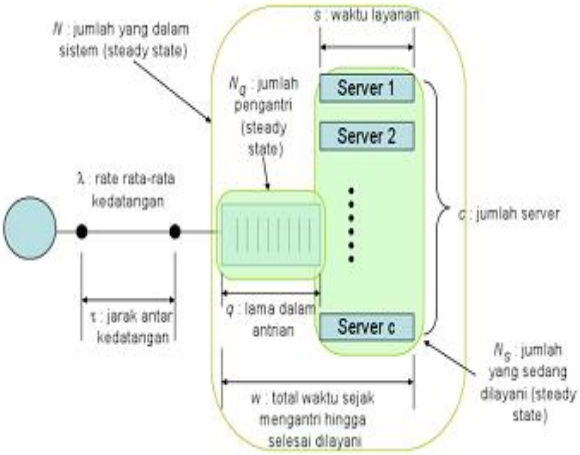
4. *Throughput*

Throughput yaitu kecepatan transfer data efektif yang dinyatakan dalam satuan bps. *Throughput* didefinisikan sebagai banyaknya bit yang sukses terkirim dari sumber sampai ke tujuan dalam selang waktu pengamatan, yang merupakan kondisi *data rate* sebenarnya dalam suatu jaringan [1].

$$\frac{jumla\ h\ paket\ \ sukses\ \ x\ waktu\ \ transmisi\ \ paket}{lama\ \ pengamatan} \quad (2.1)\ [1]$$

2.4 TEORI ANTRIAN

Kata antrian datang melalui perancis, dari bahasa *Latin cauda*, yang berarti ekor. Teori *queueing* umumnya dianggap sebagai sebuah cabang dari riset operasi karena hasilnya sering digunakan ketika membuat keputusan yang dibutuhkan untuk menyediakan layanan. Teori *queueing* langsung diterapkan pada sistem transportasi cerdas, *call center*, jaringan, telekomunikasi, *server queueing*, *mainframe* komputer *terminal queueing* telekomunikasi, sistem telekomunikasi maju, dan arus lalu lintas [11]. Gambar 2.3 menunjukkan gambaran Model Sistem Antrian secara umum.



Gambar 2.5. Model Sistem Antrian [12]

Terdapat empat karakteristik system antrian, yaitu:

1. Sumber *Input*

   Menggambarkan bentuk dan ukuran kedatangan konsumen pada fasilitas pelayanan yang kedatangannya mungkin saja tidak merata atau dapat mengikuti pola kedatangan *poisson* atau pola lain. Ukuran kedatangan konsumen yaitu jumlah total unit yang memerlukan pelayanan dari waktu ke waktu disebut juga total langganan potensial [11].

2. Antrian

   Karakteristik suatu antrian ditentukan oleh unit maksimum yang boleh ada didalam sistemnya yang terbatas maupun tidak terbatas. Struktur dasar model

antrian adalah dimulai dari sumber *input*: antrian untuk mendapatkan pelayanan: satuan hasil pelayanan yang telah dilayani [11].

3. Distribusi Pelayanan

Distribusi pelayanan berkaitan dengan cara memilih anggota antrian yang akan dilayani. Bentuk disiplin pelayanannya dapat berupa [11]:

a. *First Come First Serve* (FCFS) atau FIFO adalah system antrian yang mendahulukan yang datang lebih awal
b. *Last Come First Served* (LCFS), adalah yang datang terakhir akan lebih dahulu dilayani atau lebih dahulu keluar.
c. *Service In Random Order* (SIRO) adalah pemanggilan didasarkan pada peluang secara acak, tidak jadi persoalan siapa yang lebih dahulu datang.
d. *Priority Service* (PS), melayani lebih dahulu orang yang mempunyai prioritas lebih tinggi ketimbang orang yang mempunyai prioritas lebih rendah.

Teknik antrian yang beragam dapat digunakan untuk mengontrol paket mana yang akan ditransmisikan dan paket

mana yang akan mengantri. Beberapa teknik antrian yang biasa digunakan antara lain [13]:

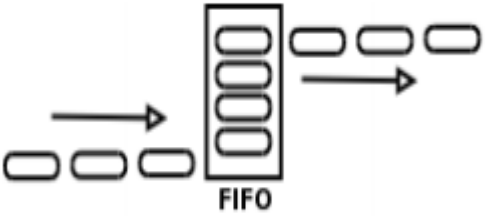
1. *First-in-first-out* (FIFO)

   FIFO merupakan singkatan dari *First in first out*. Teknik ini memiliki prinsip antrian "pertama datang pertama dilayani". Maksudnya adalah paket yang datang terlebih dahulu akan di layani dan ditransmisikan terlebih dahulu, sedangkan paket yang datang kemudian akan ditransmisikan setelah paket sebelumnya selesai dilayani atau ditransmisikan. Apabila dianalogikan seperti sekumpulan orang yang berbaris untuk mengantri, orang-orang akan masuk sesuai dengan urutan keberangkatan [13].

   FIFO merupakan teknik antrian yang paling dasar. Di dalam FIFO, semua paket diperlakukan sama dengan menempatkan paket-paket tersebut ke dalam satu garis antrian kemudian melayani sesuai dengan urutan pada antrian. FIFO juga seringa disebut dengan teknik *First Come First Serve* (FCFS) [13].

   Teknik antrian FIFO mengacu pada FCFS (*First Come First Server*), paket data yang pertama datang diproses terlebih dahulu. Paket data yang keluar terlebih dahulu di masukan ke dalam antrian FIFO, kemudian dikeluarkan sesuai dengan urutan

kedatangan. Teknik antrian FIFO sangat cocok untuk jaringan dengan *bandwidth* menengah 64 kbps tetapi cukup menghabiskan sumber daya prosessor dan memori [11].

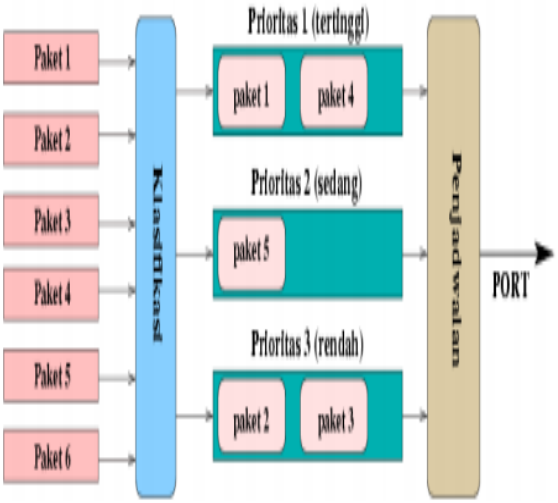


Gambar 2.6. Model FIFO [11]

Gambar di 2.6. menunjukkan kedatangan beberapa paket data yang berbeda waktu, paket pertama dari *flow* yang tiba lebih awal dikeluarkan ke *port* terlebih dahulu oleh antrian FIFO [11].

2. *Priority Queuing* (PQ)

PQ menjadi dasar dari skema penjadwalan yang berdasarkan kelas antrian. Mekanisme skema ini adalah setiap paket ditandai dengan suatu prioritas kemudian paket diklasifikasikan oleh sistem, dan dimasukkan pada kelas-kelas prioritas yang berbeda-beda. Dalam masing-masing kelas prioritas tersebut paket-paket kemudian dijadwalkan berdasarkan prioritas [10].



Gambar 2.7. Prioritas Antrian [11]

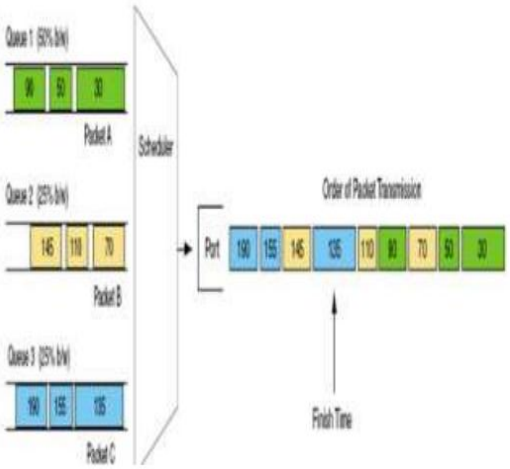
Priority Queuing membuat beberapa antrian pada sebuah interface jaringan di mana masing-masing antrian diberikan level prioritas. Sebuah paket antrian yang memiliki prioritas lebih tinggi akan diproses terlebih dahulu daripada paket yang memiliki prioritas lebih rendah. Secara *default*, masing-masing antrian memiliki kapasitas paket 20, 40, 60, dan 80 [13].

Gambar 2.7 menunjukkan deskripsi dari teori antrian PQ. Ketika sebuah paket dikirimkan melalui sebuah *interface*, prioritas antrian dari paket tesebut akan di-*scan* terlebih dahulu untuk diurutkan

berdasarkan level prioritasnya. Antrian dengan prioritas tinggi akan di-*scan* terlebih dahulu, kemudian antrian dengan prioritas medium, begitu seterusnya sampai antrian dengan prioritas terendah. Proses ini terjadi berkali-kali sepanjang waktu ketika sebuah paket dikirimkan [13].

3. *Weighted-fair Queuing* (WFQ)

Tujuan utama di balik metode WFQ adalah untuk menjamin *fairness* di antara semua jenis trafik. Mirip dengan PQ, paket tiba pertama-tama diklasifikasikan dan ditetapkan ke dalam salah satu kelas antrian berdasarkan informasi yang diambil dari *header* paket. Masing-masing antrian diberikan bobot berdasarkan pada kebutuhan *bandwidth* masing-masing trafik. Dimana bobot dari tiap-tiap antrian berbeda berdasarkan level prioritasnya. Sehingga dalam metode *scheduling* ini, trafik dengan level prioritas rendah pun akan terlayani dan mendapat jaminan *resources* atau *bandwidth* dari jaringan, sehingga akan meminimalkan *packet dropped* [14]. Kelebihan dari WFQ ini adalah WFQ menjamin kemanan ke setiap kelas layanan [15].



Gambar 2.8. Teori Antrian WFQ [16]

2.5 *DIFFERENTIATED SERVICE CODE POINT* (DSCP)

DSCP merupakan pengembangan dari *Field Type of Service* (ToS). Pada mulanya *field* ToS banyak digunakan untuk menyediakan QoS pada jaringan IP. QoS yang dimaksud adalah dengan membagi-bagi prioritas masing-masing layanan. *Field* ToS menggunakan 3 bit untuk membagi layanan yang disebut dengan nilai IP *Precedence*. Pada *field* ToS, nilai IP *Precedence* inilah yang menentukan prioritas suatu layanan [14].

Tabel 2.1. NILAI-NILAI IP *PRECEDENCE* [14]

IP *Precedence*	***Binary***	***Priority***
0	000	*Routine*
1	001	*Priority*
2	010	*Immediate*
3	011	*Flash*
4	100	*Flash Override*
5	101	*Critical*
6	110	*Internetwork Control*
7	111	*Network Control*

Nilai IP *Precedence* yang paling penting adalah *Critical, Flash override*, dan *Flash*. Pada umumnya *Critical* (5) digunakan untuk trafik VoIP atau trafik *realtime (time sensitive), Flash override* (4) untuk trafik video, dan *Flash* (3) untuk *multimedia streaming*. Pada umumnya, trafik lainnya dipetakan ke trafik *best effort* atau *Routine* (0) [14].

Gambar 2.9. Kelas-Kelas DSCP [14]

Gambar 2.9. merupakan pembagian kelas-kelas dalam DSCP. DSCP merupakan perluasan dari IP *Precedence* dan masih bisa dikodekan sebagai nilai ToS. Nilai DSCP adalah IP *Precedence* ditambah dengan variable *delay*, *throughput*, dan *reliable*. Pada implementasi DSCP, variabel *delay* dan *throughput* disebut *drop probability*. Nilai-nilai DSCP yang sering digunakan adalah kelas-kelas *expedited forwarding* (EF) dan *assured forwarding* (AF) [14].

Tabel 2.2. NILAI DSCP DAN KELAS LAYANAN [14]

Nama	**Biner**	**IP *Prec***	***Drop Pecedence***	**Layanan**
CS0	000 000	0		Standar (DNS, DHCP)
CS1	001 000	1		*Low Priority Data* (Semua trafik yang tidak mendapat jaminan *bandwidth*
AF11	001 010	1	*Low*	*High-Throughput Data (Transfer File, Store and forward application)*
AF12	001 100	1	*Medium*	
AF13	001 110	1	*High*	
CS2	010 000	2		OAM (OAM&O)

Nama	**Biner**	**IP *Prec***	***Drop Pecedence***	**Layanan**
AF21	010 010	2	*Low*	Data *latency* rendah (Transaksi web, transfer keuangan)
AF22	010 100	2	*Medium*	
AF23	010 110	2	*High*	
CS3	011 000	3		*Broadcast Video (broadcast TV & live events, video surveillance, video on demand)*
AF31	011 010	3	*Low*	*Multimedia Streaming (Buffered Streaming Audio, Webcast)*
AF32	011 100	3	*Medium*	
AF33	011 110	3	*High*	
CS4	100 000	4		*Real-time interactive (video conference,)*
AF41	100 010	4	*Low*	*Multimedia Conferencing (H323/v2 video conferencing)*
AF42	100 100	4	*Medium*	
AF43	100 110	4	*High*	
CS5	101 000	5		*Signaling (Perr-to-peer IP, IP telephony)*

Nama	**Biner**	**IP *Prec***	***Drop Pecedence***	**Layanan**
EF	101 110	5		*Telephony (VoIP, Voice)*
CS6	110 000	6	*Routing*	*Network Control (Network Routing)*
CS7	111 000	7	*Network*	

2.6 STANDARISASI ITU-T G.1010

Berikut merupakan standarisasi ITU-T G.1010 yang dijadikan rujukan dalam penelitian ini:

Tabel 2.3. Standarisasi ITU-T G.1010 [17]

Layanan	**Aplikasi**	***Key Performance Parameters and target value***		
		End-to-end delay	***Delay Variation***	***Packet Loss Ratio***
Audio	*Conversational Video*	<150 ms *preferred* <400 ms *limit*	<1 ms	<3% *Packet loss ratio*
Audio	*Video Messaging*	<1 s for *playback* <2s for *record*	<1 ms	<3% *Packet loss ratio*
Audio	*High quality streaming audio*	<10 s	<<1 ms	<1% *Packet loss ratio*

Layanan	**Aplikasi**	***Key Performance Parameters and target value***		
		End-to-end delay	***Delay Variation***	***Packet Loss Ratio***
Video	*One way*	<10 s		<1% *Packet loss ratio*
Data	*Web browsing HTML*	*Preferred* <2s /*page* *Acceptable* <4s / page	N.A.	*Zero*
Data	*Bulk data transfer/ retrieval*	*Preferred* <15s *Acceptable* <60 s	N.A.	*Zero*
Data	*Transaction Services-high priority*	*Preferred* <2s *Acceptable* <4s	N.A.	*Zero*
Data	*Command/ control*	<250 ms	N.A.	*Zero*
Data	*Still Image*	*Preferred* <15s *Acceptable* <60 s	N.A.	*Zero*
Data	*Interactive Game*	<200 ms	N.A.	*Zero*
Data	*Telnet*	<200 ms	N.A.	*Zero*

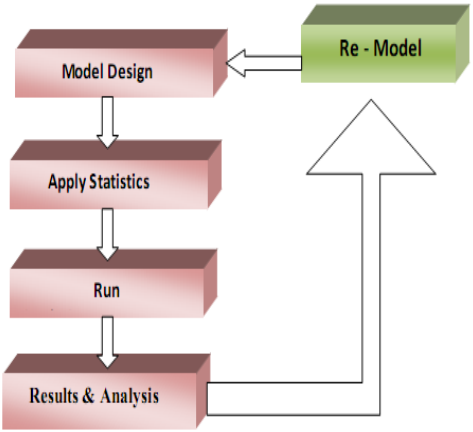
Layanan	**Aplikasi**	***Key Performance Parameters and target value***		
		End-to-end delay	***Delay Variation***	***Packet Loss Ratio***
Data	*E-mail (Server Access)*	*Preferred* <2s *Acceptable* <4s	N.A.	*Zero*
Data	*E-mail (Server to server transfer)*	*Can be several minutes*	N.A.	*Zero*
Data	*Fax ("real-time")*	<30 s/page	N.A.	$< 10^{-6}$ BER
Data	*Fax (Store & Forward)*	*Can be several minutes*	N.A.	$< 10^{-6}$ BER
Data	*Low priority transactions*	<30 2	N.A.	*Zero*
Data	*Usenet*	*Can be several minutes*	N.A.	*Zero*

2.7 OPNET MODELER 14.5

Opnet Modeler merupakan salah satu aplikasi simulator jaringan yang menyediakan perangkat komunikasi jaringan secara virtual. Opnet Modeler terkenal digunakan untuk studi penelitian, pemodelan dan *engineering* jaringan, serta analisa operasi dan performa R & D. Opnet Modeler

memegang peranan penting dalam dunia teknik saat ini khususnya dalam pembuatan dan pengembangan protokol teknologi *wireless* seperti WIMAX, WiFi, UMTS, dan lain sebagainya [18].

Cara kerja penggunaan Opnet Modeler secara umum dibagi kedalam empat tahapan, yaitu desain model, memilih statistik, menjalankan simulasi, dan melihat hasil serta menganalisa hasil simulasi. Jika hasilnya tidak benar atau terjadi kesalahan, maka model harus di desain ulang dan memilih statistik yang baru. Alur kerja penggunaan Opnet Modeler dapat dilihat pada gambar 2.10 [18].

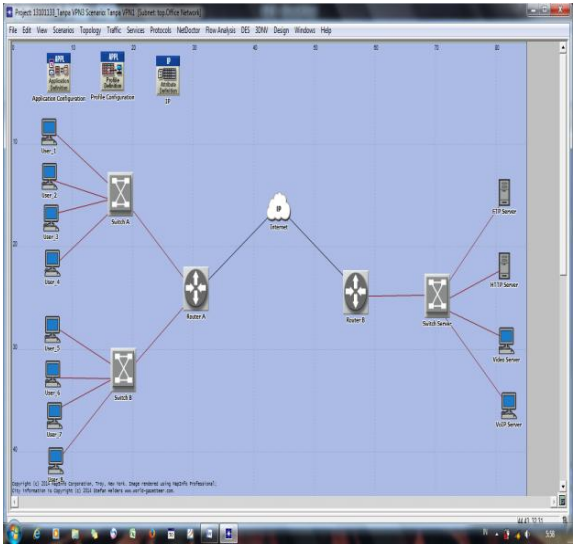


Gambar 2.10. Alur Kerja Penggunaan Opnet Modeler[18]

1. Desain Model

   Dalam membuat desain model langkah pertama yang dilakukan adalah menjalankan Opnet

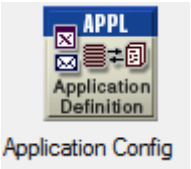
Modeler, kemudian membuat skenario baru sehingga muncul lembar kerja yang baru. Pada lembar kerja tersebutlah didesain jaringan yang akan dibuat dengan menggunakan komponen jaringan yang diperlukan [18]. Komponen-komponen tersebut antara lain *Application Configuration*, *Profile Configuration*, VPN *Configuration*, *Server*, *Nodes*, dan lain sebagainya. Komponen-komponen tersebut dapat ditemukan pada *tools "Object palette"* dari Opnet Modeler. Gambar 2.11. merupakan desain skenario yang digunakan pada penelitian.



Gambar 2.11. Desain Skenario yang Digunakan

2. *Application Configuration*

Application Configuration digunakan untuk memilih aplikasi yang diperlukan dari beberapa aplikasi yang tersedia pada Opnet Modeler seperti FTP, HTTP, *Email, Database, Print*, dan lain sebagainya. Selain dapat memilih aplikasi juga dapat membuat nama aplikasi yang dipilih sesuai dan memberikan gambaran yang relevan tentang aplikasi yang didefinisikan. Pada penelitian ini menggunakan 4 buah aplikasi atau layanan, yaitu: FTP, HTTP, Video, dan VoIP. Gambar 2.12. merupakan gambar dari komponen *Application Configuration.*



Gambar 2.12. *Application Configuration*

3. *Profile Configuration*

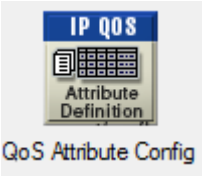
Profile Configuration digunakan untuk membuat *profiles user* yang mana *profile* tersebut dapat dispesifikasikan pada node yang berbeda pada desain jaringan untuk membangkitkan traffik layanan. Pada penelitian ini *profile* yang dibuat sesuai dengan aplikasi yang didefinisikan pada

Application Configuration sehingga terdapat 4 buah *profile* dengan nama yang sesuai. Gambar 2.13. merupakan gambar komponen dari *Profile Configuration*.

Gambar 2.13. *Profile Configuration*

4. IP QoS *Configuration*

Komponen ini digunakan untuk melakukan pengaturan terhadap parameter-parameter pada setiap teori antrian. Pada penelitian ini, teori antrian yang digunakan menggunakan parameter default sehingga pada komponen ini tidak dilakukan pengaturan. Komponen IP QoS *Configuration* pada Opnet Modeler dapat dilihat pada gambar 2.14.



Gambar 2.14. QoS *Configuration*

5. Komponen Jaringan VPN

Komponen-komponen jaringan VPN yang terdapat dalam Opnet Modeler yaitu:

a. *Workstation*, merupakan komputer PC yang digunakan sebagai *client*, yang menjalankan fungsi PC biasa pada infrastruktur jaringan. *Workstation* ini akan mengakses aplikasi-aplikasi yang terdapat pada *server* [1].

Gambar 2.15. *Workstation*

b. *Router*, perangkat ini berfungsi sebagai penghubung antar jaringan-jaringan yang berbeda. *Router* bertugas untuk menyampaikan paket dari sumber ke tujuan yang terpisah pada jaringan yang berbeda, proses penyampaian paket ini disebut *routing* [1].

Gambar 2.16. *Router*

c. Internet, merupakan jaringan komputer publik yang merepresentasikan jaringan WAN yang lebih besar [1].

Gambar 2.17. Internet

d. *Switch*, merupakan penghubung beberapa perangkat untuk membentuk jaringan kecil atau *Local Area Network* (LAN) [1].

Gambar 2.18. *Switch*

e. *Server*, berfungsi sebagai perangkat penyedia layanan dalam jaringan komputer [1].

Gambar 2.19. *Server*