

BAB II

LANDASAN TEORI

A. JARINGAN KOMPUTER

Jaringan Komputer adalah sekelompok komputer otonom yang saling berhubungan satu sama lainnya menggunakan protokol komunikasi melalui media komunikasi sehingga dapat saling berbagi informasi, aplikasi, dan perangkat keras secara bersama-sama[5]. Perangkat jaringan menggunakan berbagai protokol dan algoritma untuk menentukan dengan tepat bagaimana endpoint harus mengirim dan menerima data. Tujuan jaringan komputer adalah agar dapat mencapai tujuannya, setiap bagian dari jaringan komputer dapat meminta dan memberikan layanan (service). Pihak yang meminta/menerima layanan disebut klien (client) dan yang memberikan/mengirim layanan disebut peladen (server). Desain ini disebut dengan sistem client-server, dan digunakan pada hampir seluruh aplikasi jaringan komputer.

B. *INTERNET PROTOCOL (IP)*

IP (internet protocol) merupakan protokol yang paling penting yang harus berada pada layer Internet *TCP/IP*. Semua protokol *TCP/IP* yang berasal dari layer mengirimkan data melalui protokol IP ini. Seluruh data dilewatkan, dioalah oleh protokol IP dan dikirimkan sebagai datagram IP untuk sampai ke sisi penerima. Dalam melakukan pengiriman data, protokol IP ini bersifat *unreliable connectionless*, dan *datagram delivery service*[6].

IP Address (internet protocol address) merupakan deretan angka biner antara 32 bit sampai dengan 128 bit yang digunakan sebagai alamat identifikasi untuk tiap komputer host dalam jaringan internet. Angka 32 bit digunakan untuk alamat ip address versi IPv4 dan angka 128 bit digunakan untuk menunjukkan alamat dari komputer pada jaringan internet berbasis *TCP/IP*[7].

Ada berbagai macam jenis protokol *TCP/IP* yang sering digunakan untuk bertukar data, antara lain seperti :

BAB II

a. TCP PROTOCOL

TCP (*Transmission Control Protocol*) merupakan protokol yang berada pada layer transfer dari layer TCP/IP. TCP juga merupakan protokol yang handal, protocol ini berusaha keras secara saksama untuk mengirimkan data ketujuan, memeriksa kesalahan, mengirim data ulang bila diperlukan dan mengirim eror kelapisan atas hanya bila TCP tidak berhasil mengadakan komunikasi. TCP didesain untuk memenuhi kebutuhan (DOD) akan pengiriman data akurat pada masa dimana jaringan wide-area masih belum begitu handal, dan tetap sesuai digunakan untuk aplikasi yang membutuhkan pengiriman data yang handal.[8]

b. ICMP PROTOCOL

ICMP (*Internet Control Message Protocol*) merupakan IP yang tidak didesain sebagai protokol yang handal ICMP hanya bertugas untuk mengirimkan pesan-pesan khusus atau pesan-pesan kesalahan yang memerlukan perhatian, dan tidak memerlukan keamanan yang tinggi karena pengirimannya dalam bentuk datagram IP. Pesan ICMP ini akan dikirim jika terjadi masalah layer IP dan layer di atasnya (TCP atau UDP) Pesan ICMP tersebut ditentukan dari kombinasi tipe dan kodenya.[8][9]

c. UDP PROTOCOL

Pada section ini dijelaskan tentang protokol UDP. Memperkuat pernyataan Tenenbaum, pada bagian lain blog ini yaitu protocol TCP bahwa layer transport terdapat 2 protokol utama yaitu protokol UDP (*User Datagram Protocol*) dan protokol TCP (*Transmission Control Protokol*). Protokol ini untuk mendukung konsep jaringan berbasis IP. Telah diketahui bahwa IP (*internet protocol*) sebagai protokol jaringan internet yang mengkomunikasikan dua titik jaringan serta secara spesifik semua aplikasi dan layanan terpengaruh port tetapi kondisi konsep jaringan IP tidak memberikan jaminan. Jaminan tersebut adalah jaminan bahwa data akan tersampaikan pada destination yang benar dan data tersampaikan dengan benar.[8]

BAB II

C. ROUTING PROTOCOL

Routing adalah proses pencarian jalur pengiriman data dari client menuju server atau sebaliknya. Alat yang digunakan dinamakan dengan Router. Proses ini sangat penting mengingat pada dasarnya internet terbentuk dari banyak jaringan komputer yang saling terhubung, sehingga jalur pengiriman data dapat berubah setiap saat. Semakin pendek jalur pengiriman data nya maka semakin cepat pula proses pengiriman data dari client ke server dan sebaliknya.

1. STATIC ROUTING

Routing statik IP adalah suatu proses penentuan jalur untuk melewati datagram IP dari alamat pengirim ke alamat tujuan. Proses routing statik dilakukan manual dengan memasukan setiap hop. Hop adalah perjalanan paket data dari suatu router atau host ke router atau host lainnya.

2. DYNAMIC ROUTING

Dynamic Routing Protocol atau routing dinamis adalah mekanisme interkoneksi lintas jaringan dengan menggunakan Router dalam proses penerusan data (data forwarding) dari satu Router ke Router lainnya dalam jsuatu jaringan. Informasi routing dipelajari oleh Router dari Router yang lain atau Router “tetangganya”[10]

Ada berbagai jenis protocol routing dinamis yang bisa digunakan diantaranya yang populer dan banyak digunakan pada skema jaringan skala besar adalah Routing Information Protocol (RIP), Open Shortest Path First (OSPF) dan Enhanced Interior Gateway Routing Protocol (EIGRP). Ketiga protocol routing tersebut dapat digunakan untuk menghubungkan setiap jaringan – jaringan dari wilayah yang luas dan berjauhan.

Setiap Protocol Routing memiliki kelebihan dan keunggulan masing-masing, mengingat algoritma yang dipakai pada setiap protocol memiliki perbedaan. Seperti misalnya dalam penentuan

BAB II

jalur terbaik (best path) untuk menuju ke suatu jaringan, RIP menggunakan hop counts, Interior Gateway Routing Protocol (IGRP) dan EIGRP menggunakan sebuah composite metric dari Bandwidth, Reliability, Load, Delay dan ukuran MTU, sedangkan OSPF menggunakan cost metric [10].

D. VIRTUAL PRIVATE NETWORK

Virtual Private Network (VPN) adalah jaringan yang menggunakan rata-rata masyarakat transmisi (internet) sebagai link wan nya. Sebuah VPN adalah jenis jaringan pribadi yang menggunakan telekomunikasi publik. Yang menyediakan akses remote ke jaringan organisasi melalui internet daripada menggunakan jalur untuk berkomunikasi. Sebuah VPN biasa digunakan untuk menghubungkan kantor pusat dengan kantor-kantor cabangnya, VPN juga memungkinkan pengguna ponsel maupun laptop dapat terhubung ke jaringan VPN dengan mengaksesnya melalui internet. Dengan memasukan jenis VPN pada device yang digunakan serta memasukan autentikasi yang diperlukan.

1. LAYER 2 TRANSFER PROTOCOL (L2TP)

Layer 2 Transfer Protocol (L2TP) adalah pengembangan dari PPTP plus L2F. Protokol Tunneling Layer 2 (L2TP) juga sering disebut sebagai protokol dial-up virtual, karena L2TP memperluas sesi dial-up Point to Point Protocol (PPP) melalui jaringan internet public dan memiliki tingkat keamanan yang lebih tinggi dibandingkan PPTP yang hanya menggunakan MPPE.[11]

2. IPSECURITY (IPSEC)

IPSec merupakan protokol yang digunakan untuk mengamankan transmisi datagram pada jaringan berbasis TCP/IP. IPSec menawarkan 3 layanan utama, yaitu otentikasi dan integritas data, kerahasiaan, dan manajemen kunci. Untuk dapat memenuhi kebutuhan keamanan L2TP perlu dicoba implementasi keamanan dengan menggunakan protokol tipe transport IPSec atau lebih dikenal dengan protokol L2TP over IP Security (IPSec), sehingga

BAB II

paket informasi yang dikirim oleh protokol L2TP akan terenkapsulasi oleh protokol IPSec[11]

E. GNS3 SIMULATOR

GNS3 adalah sebuah program graphical network simulator yang dapat mensimulasikan topologi jaringan yang lebih kompleks dibandingkan dengan simulator lainnya. Program ini dapat dijalankan pada operating-systems, seperti Windows XP professional atau Linux Ubuntu[12]. GNS3 berfungsi, mensimulasikan topologi jaringan yang lebih kompleks, jika dibandingkan dengan jenis simulator lainnya. Hal ini dikarenakan software GNS3 menggunakan operating system asli yang berasal dari perangkat jaringan seperti cisco, juniper, mikrotik dan lainnya. Sehingga, pengguna yang memakainya akan merasa di dunia yang nyata dalam hal mengkonfigurasi router maupun simulasi jaringan lainnya.

Berikut beberapa fitur utama yang tersedia pada software GNS3 :

1. Desain kualitas tinggi dan topologi jaringan yang kompleks.
2. Mendukung banyak platform Cisco IOS router, IPS, PIX dan ASA firewall, JUNOS.
3. Simulasi Ethernet sederhana, ATM dan Frame Relay switch.
4. Koneksi jaringan simulasi ke dunia nyata
5. Packet capture menggunakan Wireshark.

F. QUALITY OF SERVICE

Quality of service (Qos) adalah sebuah tata cara atau protocol untuk memberikan kemampuan kepada seorang admin jaringan komputer pada sebuah jaringan komputer yang telah dibuat untuk melakukan kegiatan pengelolaan bandwidth, loss, jitter dan congestion dari throughput dalam sebuah jaringan.[4] QoS biasanya digunakan untuk mengukur sekumpulan atribut performansi yang telah dispesifikasikan. Pada jaringan berbasis IP, IP QoS mengacu pada performansi dari paket-paket IP yang lewat melalui satu atau lebih jaringan. Pada implementasinya QoS memiliki beberapa

BAB II

parameter yang cukup penting bagi kualitas layanan yang diterima pelanggan[13]. Berikut beberapa parameter dari TIPHON :

1. Delay (Latency)

Delay merupakan waktu yang dibutuhkan data untuk menempuh jarak dari asal ke tujuan.

$$\text{Rata-rata delay} = \frac{\text{Jumlah Delay Jumlah}}{\text{Paket yang diterima}}$$

Kategory Latency	Besar Delay (ms)	Indeks
Sangat Bagus	< 150	4
Bagus	150 ms s/d 300 ms	3
Sedang	300 ms s/d 450 ms	2
Jelek	> 450 ms	1

Tabel 1 Kategori Delay (Sumber : TIPHON)

2. Jitter

Jitter terjadi karena variasi-variasi dalam panjang antrian, waktu pengolahan data, dan juga waktu penghimpunan ulang paket-paket diakhir perjalanan.

$$\text{Jitter} = \frac{\Sigma \text{Variasi Delay}}{\Sigma \text{Paket yang diterima} - 1}$$

Untuk mencari nilai Variasi Delay menggunakan rumus :

$$\text{Variasi Delay} = \text{delay (n)} - \text{delay (n-1)}$$

Kategory Jitter	Jitter (ms)	Indeks
Sangat Bagus	0 ms	4
Bagus	0 ms s/d 75 ms	3
Sedang	75 ms s/d 125 ms	2
Jelek	125 ms s/d 225 ms	1

Tabel 2. Kategori Delay (Sumber : TIPHON)

BAB II

3. Packetloss

Packet Loss merupakan suatu parameter yang menggambarkan suatu kondisi yang dapat menunjukkan paket yang hilang karena collision dan congestion pada jaringan.

$$Packetloss = \frac{\text{Jumlah paket yang gagal}}{\text{Jumlah paket yang dikirim}}$$

Kategory Packet Loss	Throughput (bps)	Indeks
Sangat Bagus	0	4
Bagus	3	3
Sedang	15	2
Jelek	25	1

Tabel 3. Kategori Delay (Sumber : TIPHON)

G. MIKROTIK CHR

Mikrotik Cloud Hoster Router adalah sebuah produk dari mikrotik yang dapat digunakan router mikrotik dengan teknologi virtualisasi. CHR dapat digunakan pada virtualisasi seperti VirtualBox, VM Ware, GNS3 dan lainnya. CHR memiliki RouterOS lengkap yang diaktifkan secara default tetapi memiliki model lisensi yang berbeda dari versi RouterOS lainnya. Perbedaan yang paling mendasar antara routerOS biasa dengan CHR yaitu terletak pada sistem lisensi. Dimana CHR hanya ada 4 lisensi dan pembatasan hanya di si speed maksimal setiap interfacenya. Saat pertamakali CHR diinstall, maka akan mendapatkan lisensi free dengan batasan kecepatan interfasi maksimal 1 mbit.

H. WIRESHARK

Wireshark merupakan software yang dapat menganalisa aktivitas jaringan komputer sehingga dapat membantu mendeteksi serangan yang akan terjadi sehingga pengguna tidak perlu khawatir dengan serangan tersebut. Wireshark dalam memonitor suatu jaringan komputer dapat membantu memudahkan seorang administrator jaringan untuk melakukan pengawasan terhadap suatu jaringan komputer.[14] Dengan aplikasi wireshark ini dapat melakukan monitoring, meninjau serta melakukan

BAB II

penyimpanan informasi sebuah paket baik paket yang keluar maupun paket yang masuk didalam suatu jaringan secara detail. Selain itu tampilan grafis (GUI) pad wireshark cukup baik sehingga lebih memudahkan dalam memonitoring semua aktifitas serta kegiatan yang dilakukan pada suatu jaringan atau pada jaringan yang dimiliki.