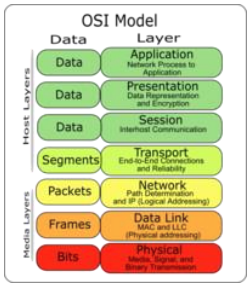
BAB II
TEORI PENUNJANG

2.1 OSI Layer (Open System Interconnection)

OSI (*Open System Interconnection*) adalah standar komunikasi yang diterapkan di dalam jaringan komputer. Standar itulah yang menyebabkan seluruh alat komunikasi dapat saling berkomunikasi melalui jaringan. Model referensi OSI menggambarkan bagaimana informasi dari suatu software aplikasi di sebuah komputer berpindah melewati sebuah media jaringan ke suatu software aplikasi di komputer lain. Model referensi OSI secara konseptual terbagi ke dalam 7 lapisan dimana masing-masing lapisan memiliki fungsi jaringan yang spesifik.

Model Open Systems Interconnection diciptakan oleh International Organization for Standardization, yang menyediakan kerangka logika terstruktur bagaimana proses komunikasi data berinteraksi melalui jaringan. Standard ini dikembangkan untuk industri komputer agar komputer dapat berkomunikasi pada jaringan yang berbeda secara efisien.

7 lapisan layer pada model OSI, Setiap layer bertanggungjawab secara khusus pada proses komunikasi data. Misalnya, satu layer bertanggungjawab untuk membentuk koneksi antar perangkat, dan layer lainnya bertanggungjawab untuk mengoreksi terjadinya “error” selama proses transfer data berlangsung.



Gambar II.I Tujuh Layer Model OSI

2.1.1 Physical layer

Lapisan ke-1 ini berfungsi untuk mendefinisikan media transmisi jaringan, metode pensinyalan, sinkronisasi bit, arsitektur jaringan (seperti halnya *Ethernet* atau *Token Ring*), topologi jaringan dan pengabelan. Selain itu, level ini juga mendefinisikan bagaimana Network Interface Card (NIC) dapat berinteraksi dengan media kabel atau radio. Pada lapisan ini tidak mempunyai protokol yang spesifik, yang bertanggung jawab atas proses data menjadi bit dan mentransfernya melalui media, seperti kabel, dan menjaga koneksi fisik antar sistem, pada layer ini hanya mengirimkan bit bit data.

2.1.2 Data-link layer

Lapisan ke-2 ini berfungsi untuk menentukan bagaimana bit-bit data dikelompokkan menjadi format yang disebut sebagai frame. Selain itu, pada level ini terjadi koreksi kesalahan, flow control, pengalamatan perangkat keras, dan menetukan bagaimana perangkat-perangkat jaringan seperti hub, bridge, repeater, dan switch layer 2 beroperasi. Spesifikasi IEEE 802, membagi level ini menjadi dua level anak, yaitu lapisan Logical Link Control (LLC) dan lapisan Media Access Control (MAC).

Protokol yang berada dalam lapisan ini :

1. PPP (*Point to Point Protocol*) protokol yang digunakan untuk point to point pada suatu jaringan.
2. SLIP (*Serial Line Internet Protocol*) protokol yang digunakan untuk menyambung serial.

2.1.3 Network layer

Lapisan ke-3 ini berfungsi untuk mendefinisikan alamat-alamat IP, membuat header untuk paket-paket, dan kemudian melakukan routing melalui internetworking dengan menggunakan router dan switch layer-3.

Protokol yang berada dalam lapisan ini :

1. IP (*Internetworking Protocol*) mekanisme transmisi yang digunakan untuk menstransportasikan data dalam-dalam paket yang disebut datagram.
2. ARP (*Address Resulotion Protocol*) protokol yang digunakan untuk mengetahui alamat IP berdasarkan alamat fisik dari sebuah komputer.
3. RARP (*Reverse Address Resulotion Protocol*) protokol yang digunakan untuk mengetahui alamat fisik melalui IP komputer.
4. ICMP (*Internet Control Message Protocol*) mekanisme yang digunakan oleh sejumlah host untuk mengirim notifikasi datagram yang mengalami masalah pada hostnya.
5. IGMP (*Internet Group Message Protocol*) protokol yang digunakan untuk memberi fasilitas message yang simultan kepada group penerima.

2.1.4 Transport layer

Lapisan ke-4 ini berfungsi untuk memecah data ke dalam paket-paket data serta memberikan nomor urut ke paket-paket tersebut sehingga dapat disusun kembali pada sisi tujuan setelah diterima. Selain itu, pada level ini juga membuat sebuah tanda bahwa paket diterima dengan sukses (*acknowledgement*), dan mentransmisikan ulang terhadp paket-paket yang hilang di tengah jalan.

Protokol yang berada dalam lapisan ini :

1. TCP (*Trasmission Control Protocol*) protokol yang menyediakan layanan penuh lapisan transport untuk aplikasi.
2. UDP (*User Datagram Protocol*) protokol connectionless dan proses-to-procces yang hanya menambahkan alamat port, cheksum error control dan panjang informasi data pada layer di atasnya.

2.1.5 Session layer

Lapisan ke-5 ini berfungsi untuk mendefinisikan bagaimana koneksi dapat dibuat, dipelihara, atau dihancurkan. Selain itu, di level ini juga dilakukan resolusi nama.

Protokol yang berada dalam lapisan ini :

1. NETBIOS, berfungsi sebagai penyiaran pesan maksud nyamemungkinkan user mengirim pesan tunggal secara serempak ke komputer lain yang terkoneksi.
2. NETBEUI (*NETBIOS Extended User Interface*) berfungsi sama dengat NETBIOS hanya sedikit di kembangkan lagi dengan menambahkan fungsi yang memungkinkan bekerja dengan beragam perangkat keras dan perangkat lunak.
3. ADSP (*AppleTalk Data Stream Protocol*) berfungsi protokol ini memantau aliran datadiantara dua komputer dan untuk memeriksa aliran data tersebut tidak terputus.
4. PAP (*Printer Access Protocol*) berfungsi printer Postscript untuk akses pada jaringan AppleTalk dan untuk mengendalikan bagaimana pola komunikasi antar node.
5. SPDU (*Session Protokol Data unit*) berfungsi mendukung hubungan antara dua session service user.

6. RCP

2.1.6 Presentation Layer

Lapisan ke-6 ini berfungsi untuk mentranslasikan data yang hendak ditransmisikan oleh aplikasi ke dalam format yang dapat ditransmisikan melalui jaringan.

Protokol yang berada dalam level ini :

1. TELNET protokol yang digunakan untuk akses remote masuk ke suatu host, data berjalan secara lain teks.
2. SMTP (*Simple Mail Transfer Protocol*) salah satu protokol yang biasa digunakan dalam pengiriman e-mail di internet atau untuk mengirimkan data dari komputer pengirim e-mail ke server e-mail penerima.

3. SNMP (*Simple Network Management Protocol*) protokol yang digunakan dalam suatu manajemen jaringan.

2.1.7 Application Layer

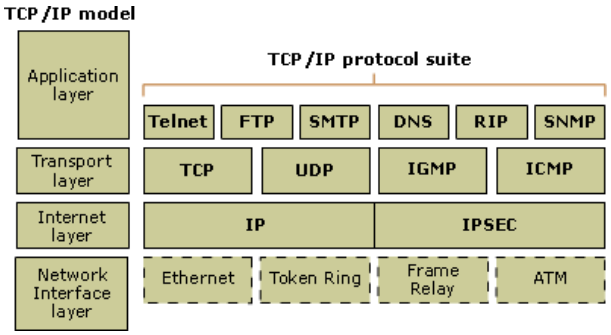
Lapisan ke-7 ini menjelaskan spesifikasi untuk lingkup dimana aplikasi jaringan berkomunikasi dengan layanan jaringan. Menyediakan jasa untuk aplikasi pengguna. Layer ini bertanggungjawab atas pertukaran informasi antara program komputer, seperti program e-mail, dan service lain yang jalan di jaringan, seperti server printer atau aplikasi komputer lainnya. Berfungsi sebagai antarmuka dengan aplikasi dengan fungsionalitas jaringan, mengatur bagaimana aplikasi dapat mengakses jaringan, dan kemudian membuat pesan-pesan kesalahan.

Protokol yang berada dalam lapisan ini :

1. Tidak mempunyai protokol yan spesifik di layer ini, bertanggung jawab atas proses data menjadi bit dan mentransfernya melalui media, seperti kabel, dan menjaga koneksi fisik antar sistem, pada layer ini hanya mengirimkan bit bit data.

2.2 Layer TCP/IP

Arsitektur TCP/IP tidaklah berbasis model referensi tujuh lapis OSI, tetapi menggunakan model referensi DARPA. Seperti diperlihatkan dalam diagram di bawah , TCP/IP mengimplementasikan arsitektur berlapis yang terdiri atas empat lapis. Empat lapis ini, dapat dipetakan (meski tidak secara langsung) terhadap model referensi OSI. Empat lapis ini, kadang-kadang disebut sebagai DARPA Model, Internet Model, atau DoD Model, mengingat TCP/IP merupakan protokol yang awalnya dikembangkan dari proyek ARPANET yang dimulai oleh Departemen Pertahanan Amerika Serikat.



Gambar II.II Layer TCP/IP

Berikut adalah macam-macam Layer TCP/IP , yaitu :

2.2.1 Application

Berfungsi menyediakan servis-servis terhadap software-software yang berjalan pada komputer. Protokol-protokol yang beroperasi pada Application Layer: HTTP, FTP, POP3, SMTP, dll.

2.2.2 Transport

Transport Layer berfungsi menyediakan servis yang akan digunakan oleh Application Layer. Mempunyai 2 protokol utama yaitu TCP dan UDP.

2.2.3 Internet

Internet Layer memiliki fungsi sebagai penyedia fungsi IP Addressing, routing, dan menentukan path terbaik. Internet Layer memiliki 1 protokol yaitu TCP/IP.

2.2.4 Network Access

Berfungsi mendefinisikan protokol-protokol dan hardware-hardware yang digunakan dalam pengiriman data. Pada layer ini terdapat protokol-protokol seperti ethernet pada LAN, PPP pada WAN, dan juga Frame Relay.

2.3 IP (*Internet Protocol*)

IP (*Internet Protocol*) adalah protokol lapisan jaringan (*network layer dalam OSI Reference Model*) atau protokol lapisan *internetwork* (*internetwork layer* dalam DARPA *reference model*) yang digunakan oleh protokol TCP/IP

untuk melakukan pengalamatan dan routing paket data antar host-host di jaringan komputer berbasis TCP/IP. Versi IP yang banyak digunakan adalah IP versi 4 (IPv4) yang didefinisikan pada RFC 791 dan dipublikasikan pada tahun 1981, tetapi akan digantikan oleh IP versi 6 pada beberapa waktu yang akan datang.

Protokol IP merupakan salah satu protokol kunci di dalam kumpulan protokol TCP/IP. Sebuah paket IP akan membawa data aktual yang dikirimkan melalui jaringan dari satu titik ke titik lainnya. Metode yang digunakannya adalah *connectionless* yang berarti tidak perlu membuat dan memelihara sebuah sesi koneksi. Selain itu, protokol ini juga tidak menjamin penyampaian data, tapi hal ini diserahkan kepada protokol pada lapisan yang lebih tinggi (lapisan transport dalam OSI Reference Model atau lapisan antar host dalam DARPA Reference Model), yakni protokol *Transmission Control Protocol* (TCP).

2.3.1 Kelas-kelas IP Address

IP address dibagi menjadi lima kelas, A sampai E. IP address yang dipakai secara umum dibagi dalam 3 kelas, sementara 2 kelas lainnya dipakai untuk kepentingan khusus. Ini untuk memudahkan pendistribusian IP address ke seluruh dunia.

1. **IP Kelas A**

   Karakteristik :

   a. Format : 0nnnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh

   b. Bit pertama : 0

   c. Panjang Network ID : 8 bit

   d. Panjang Host ID : 24 bit

   e. Byte pertama : 0 – 127

   f. Jumlah : 126 kelas A (0 dan 127 dicadangkan)

   g. Range IP : 1.xxx.xxx.xxx sampai 126.xxx.xxx.xxx

   h. Jumlah IP : 16.777.214 IP address pada tiap kelas A

IP address kelas ini diberikan kepada suatu jaringan yang berukuran sangat besar, yang pada tiap jaringannya terdapat sekitar 16 juta host.

2. IP Kelas B

Karakteristik :

a. Format : 10nnnnnn.nnnnnnnn.hhhhhhhh.hhhhhhhh
b. 2 bit pertama : 10
c. Panjang Network ID : 16 bit
d. Panjang Host ID : 16 bit
e. Byte pertama : 128 – 191
f. Jumlah : 16.384 kelas B
g. Range IP : 128.0.xxx.xxx sampai 191.155.xxx.xxx
h. Jumlah IP : 65.535 IP address pada tiap kelas B

IP address kelas ini diberikan kepada jaringan dengan ukuran sedang-besar.

3. IP Kelas C

Karakteristik :

a. Format : 110nnnnn.nnnnnnnn.nnnnnnnn.hhhhhhhh
b. Bit pertama : 110
c. Panjang Network ID : 24 bit
d. Panjang Host ID : 8 bit
e. Byte pertama : 192 – 223
f. Jumlah : 2.097.152 kelas C
g. Range IP : 192.0.0.xxx sampai 223.255.255.xxx
h. Jumlah IP : 254 IP address pada tiap kelas C

IP kelas ini dialokasikan untuk jaringan berukuran kecil.

4. IP Kelas D

Karakteristik :

a. Format : 1110mmmm.mmmmmmmm.mmmmmmmm.mmmmmmmm

b. 4 bit pertama : 1110

c. Bit Multicast : 28 bit

d. Byte Inisial : 8 bit

e. Byte pertama : 224-247

f. Deskripsi : Kelas D adalah ruang alamat Multicast (RFC 1112)

IP kelas D digunakan sebagai alamat multicast yaitu sejumlah komputer memakai bersama suatu aplikasi. 4 bit pertama IP address kelas D di set 1110. Dalam multicasting tidak dikenal network bit dan host bit.

5. IP Kelas E

Karakteristik :

a. Format : 1111rrrr.rrrrrrrr.rrrrrrrr.rrrrrrrr

b. 4 bit pertama : 1111

c. Bit Multicast : 28 bit

d. Byte Inisial : 248-255

e. Deskripsi : Kelas E adalah ruang alamat untuk keperluan eksperimental.

IP address kelas E tidak digunakan untuk umum. 4 bit pertama IP address ini di set 1111.

2.4 Subnetting

Konsep subnetting dari IP address merupakan teknik yang umum digunakan di internet untuk mengefisiensikan alokasi IP address dalam sebuah jaringan supaya bisa memaksimalkan penggunaan IP address.

Untuk beberapa alasan yang menyangkut efisiensi IP address, mengatasi masalah topologi network dan organisasi, network administrator biasanya melakukan subnetting. Esensi dari subnetting adalah "memindahkan" garis pemisah antara bagian network dan bagian host dari suatu IP address. Beberapa bit dari bagian host dialokasikan menjadi bit tambahan pada bagian network. Address suatu network menurut struktur baku dipecah menjadi beberapa sub-network. Cara ini menciptakan sejumlah network tambahan dengan mengurangi jumlah maksimum host yang ada dalam tiap network tersebut.

Jadi intinya, Subnetting adalah metode untuk membagi suatu network yang besar menjadi sub network-sub network yang lebih kecil, dengan cara mengorbankan sebagian host ID atau dengan cara meminjam bagian dari IP Address yang merupakan bagian host menjadi bagian network, agar bisa digunakan untuk membuat network ID tambahan.

Tujuan lain yang tidak kalah pentinganya dari subnetting adalah untuk mengurangi tingkat kongesti dalam suatu network. Untuk menghindari terjadinya kongesti akibat terlalu banyak host dalam suatu physical network, dilakukan segmentasi jaringan.

2.5 FTP (*File Transfer Protokol*)

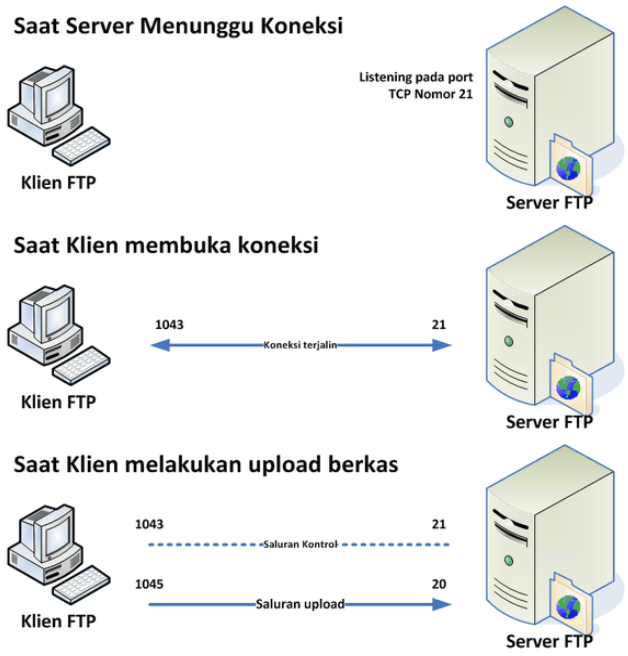
FTP (*File Transfer Protocol*) adalah suatu protokol yang berfungsi untuk pertukaran file dalam suatu jaringan komputer yang mendukung protokol TCP/IP. Dua hal pokok pada FTP yaitu FTP Server dan FTP Client. FTP juga bisa dikatakan sebuah protokol Internet yang berjalan di dalam lapisan aplikasi yang merupakan standar untuk pentransferan berkas (*file*) komputer antar mesin-mesin dalam sebuah framework.

FTP merupakan salah satu protokol Internet yang paling awal dikembangkan, dan masih digunakan hingga saat ini untuk melakukan pengunduhan (*download*) dan pengngunggahan (*upload*) berkas-berkas komputer antara FTP Client dan FTP Server. Sebuah Client FTP merupakan aplikasi yang dapat mengeluarkan perintah-perintah FTP ke sebuah Server FTP, sementara

Server FTP adalah sebuah Windows Service atau daemon yang berjalan di atas sebuah komputer yang merespons perintah-perintah dari sebuah Client FTP.

Fungsi FTP adalah Melakukan transfer file antara komputer yang terhubung melalui jaringan, termasuk internet. Dalam bahasa teknis, FTP dikenal sebagai protokol jaringan yang memungkinkan transfer file antara komputer yang tersambung pada TCP/IP yang berbasis jaringan. Hal ini mencangkup serangkaian peraturan dan prosedur untuk transfer data digital yang aman. FTP juga berfungsi untuk mempermudah dalam pembagian file-file., mempercepat secara tidak langsung atau implicyt menggunakan komputer remote, melindungi user dari berbagai file storage system antar host.

Fungsi FTP Server adalah menjalankan perangkat lunak yang digunakan untuk pertukaran file (*File Exchange*), yang selalu siap memberikan layanan FTP apabila mendapatkan request atau permintaan dari FTP Client. FTP Client adalah komputer yang meminta koneksi ke FTP Server untuk tujuan tukar menukar file (*Upload dan Download File*).



Gambar II.III Cara Kerja FTP Server Dengan Klien

2.6 Virtual Private Network (VPN)

Virtual Private Network (VPN) adalah sebuah teknologi komunikasi yang memungkinkan pengguna untuk dapat terkoneksi ke jaringan publik dan menggunakannya untuk dapat bergabung dengan jaringan lokal. Dengan cara tersebut maka akan didapatkan hak dan pengaturan yang sama seperti halnya berada didalam LAN itu sendiri, walaupaun sebenarnya menggunakan jaringan milik publik.

VPN dapat dibentuk dengan menggunakan teknologi tunneling dan enkripsi. Konkesi VPN juga dapat terjadi pada semual layer pada protocol OSI, sehingga komunikasi menggunakan VPN dapat digunakan untuk berbagai keperluan.

2.6.1 Fungsi Teknologi VPN

Teknologi VPN menyediakan tiga fungsi utama untuk penggunanya. Ketiga fungsi utama tersebut antaralain sebagai berikut.

1. ***Confidentially*** **(Kerahasiaan)**

   Dengan digunakannnya jaringan publik yang rawan pencurian data, maka teknologi VPN menggunakan sistem kerja dengan cara mengenkripsi semua data yang lewat melauinya. Dengan adanya teknologi enkripsi tersebut, maka kerahasiaan data dapat lebih terjaga. Walaupun ada pihak yang dapat menyadap data yang melewati internet bahkan jalur VPN itu sendiri, namun belum tentu dapat membaca data tersebut, karena data tersebut telah teracak.

2. ***Data Intergrity (*****Keutuhan Data*****)***

   Ketika melewati jaringan internet, sebenarnya data telah berjalan sangat jauh melintasi berbagai negara. Pada saat perjalanan tersebut, berbagai gangguan dapat terjadi terhadap isinya, baik hilang, rusak, ataupun dimanipulasi oleh orang yang tidak seharusnya. Pada VPN

terdapat teknologi yang dapat menjaga keutuhan data mulai dari data dikirim hingga data sampai di tempat tujuan.

3. *Origin Authentication* (Autentikasi Sumber)

Teknologi VPN memiliki kemampuan untuk melakukan autentikasi terhadap sumber-sumber pengirim data yang akan diterimanya. VPN akan melakukan pemeriksaan terhadap semua data yang masuk dan mengambil informasi dari sumber datanya. Kemudian, alamat sumber data tersebut akan disetujui apabila proses autentikasinya berhasil. Dengan demikian, VPN menjamin semua data yang dikirim dan diterima berasal dari sumber yang seharusnya. Tidak ada data yang dipalsukan atau dikirim oleh pihak-pihak lain.

2.6.2 Cara Kerja VPN

1. VPN mendukung banyak protokol seperti PPTP, L2TP, IPSec dan SOCK. Protokol ini membantu cara kerja VPN untuk memproses otentikasi.

2. VPN klien dapat membuat sambungan dan mengidentifikasi orang-orang yang diberi wewenangan di jaringan.

3. Jaringan VPN juga dienkripsi akan meningkatkan fitur keamanan. hal ini juga berarti bahwa VPN biasanya tidak terlihat pada jaringan yang lebih besar.

4. Teknologi saat ini semakn banyak mendasarkan perkembangan VPN karena mobilitas yang disediakan dan saat ini Virtual Private Network juga membuka jalan untuk koneksi WiFI dan jaringan nirkabel pribadi.

2.6.3 Kelebihan Jaringan VPN

1. Sebagai solusi biaya efektif untuk organisasi bisnis besar dengan fasilitas jaringan khusus.

2. Meningkatkan mobilitas organisasi dengan langsung menghubungkan jaringan rumah atau para pekerja yang mobile di organisasi.

3. Fitur keamanan dapat disesuaikan.

2.6.4 Kekurangan Jaringan VPN

Dengan penyediaan akses ke mahasiswa secara global, faktor keamanan adalah resiko tersendiri. Hal ini juga menempatkan informasi sensitif jurusan yang dapat diakses secara global. VPN membutuhkan perhatian ekstra untuk penetapan sistem keamanan yang jelas.

2.7 SSH (*Secure Shell*)

Secure Shell (SSH) adalah sebuah protokol jaringan kriptografi untuk komunikasi data yang aman, login antarmuka baris perintah, perintah eksekusi jarak jauh, dan layanan jaringan lainnya antara dua jaringan komputer. Ini terkoneksi, melalui saluran aman atau melalui jaringan tidak aman, server dan klien menjalankan server SSH dan SSH program klien secara masing-masing. Protokol spesifikasi membedakan antara dua versi utama yang disebut sebagai SSH-1 dan SSH-2.

SSH menggunakan kriptografi kunci publik untuk mengotentikasi komputer remote dan biarkan komputer remote untuk mengotentikasi pengguna, jika perlu. Ada beberapa cara untuk menggunakan SSH, salah satunya adalah dengan menggunakan secara otomatis public-privat key pasangan untuk dengan sederhana mengenkripsi koneksi jaringan, dan kemudian menggunakan otentikasi password untuk login.

Penggunaan yang lain dengan menghasilkan secara manual pasangan public-privat key untuk melakukan otentikasi, yang memungkinkan pengguna atau program untuk login tanpa harus menentukan password. Dalam skenario ini, siapa pun dapat menghasilkan pasangan yang cocok dari kunci yang berbeda (*publik* dan *privat*). Kunci publik ditempatkan pada semua komputer yang harus memungkinkan akses ke pemilik private key yang cocok (pemilik menjaga rahasia kunci privat). Sementara otentikasi didasarkan pada kunci privat, kunci itu sendiri

tidak pernah ditransfer melalui jaringan selama otentikasi. SSH hanya memverifikasi apakah orang yang sama yang menawarkan kunci publik juga memiliki kunci pribadi yang cocok. Dalam semua versi SSH adalah penting untuk memverifikasi kunci publik yang tidak diketahui, yaitu mengaitkan kunci publik dengan identitas, sebelum menerima mereka dengan valid. Menerima serangan kunci publik tanpa validasi akan mengotorisasi penyerang yang tidak sah sebagai pengguna yang valid.

2.7.1 Penggunaan SSH

SSH adalah sebuah protokol yang dapat digunakan untuk berbagai aplikasi. Beberapa aplikasi di bawah ini mungkin membutuhkan fitur-fitur yang hanya tersedia atau yang kompatibel dengan klien atau server SSH yang spesifik. Sebagai contoh, menggunakan protokol SSH untuk mengimplementasikan VPN adalah dimungkinkan, tapi sekarang hanya dapat dengan implementasi server dan klien OpenSSH.

1. Dalam kombinasi dengan SFTP, sebagai alternatif yang aman untuk FTP transfer file.
2. Dalam kombinasi dengan rsync untuk mem-backup, menyalin dan me-mirror file secara efisien dan aman.
3. Untuk port forwarding atau tunneling port (jangan dikelirukan dengan VPN yang rute paket antara jaringan yang berbeda atau menyambung dua wilayah broadcast menjadi satu).
4. Untuk digunakan sebagai VPN yang terenkripsi penuh, klien yang mendukung fitur ini.
5. Untuk meneruskan X11 melalui beberapa host.
6. Untuk browsing web melalui koneksi proxy yang dienkripsi dengan klien SSH yang mendukung protokol SOCKS.

7. Untuk mengamankan mounting direktori di server remote sebagai sebuah sistem file di komputer lokal dengan menggunakan SSHFS.
8. Untuk mengotomasi remote monitoring dan pengelolaan server melalui satu atau lebih dari mekanisme seperti yang dibahas di atas.
9. Untuk internet unlimited gratis tanpa kuota yang telah di tetapkan oleh operator.

2.7.2 Kelemahan SSH

Sejak SSH memiliki kelemahan desain yang melekat dan membuatnya rentan (misalnya, terhadap serangan man-in-the-middle), Dalam semua versi SSH, penting untuk memverifikasi kunci publik sebelum menerimanya secara valid. Menerima seorang kunci publik atttacker sebagai kunci publik yang valid memiliki efek membuka password yang ditransmisikan dan memungkinkan serangan man in-the-middle.

2.8 FTP Server

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 (*request*) dari FTP client.

Layanan FTP bisa diatur menjadi FTP publik, dimana semua orang bisa mengakses data-data yang ada di server FTP dengan mudah. Selain dapat diatur menjadi FTP public, layanan FTP ini juga bisa diatur agar tidak semua orang dapat mengakses data-data yang ada di server, jadi hanya pengguna terdaftar saja yang memiliki izin untuk mengakses data-data tersebut. FTP berkerja menggunakan salah satu protokol yang dapat diandalkan untuk urusan komunikasi data antara client dan server, yaitu protokol TCP (lebih tepatnya menggunakan port nomor 21).

2.8.1 Cara kerja FTP Server

Sebuah Klien FTP merupakan aplikasi yang dapat mengeluarkan perintah-perintah FTP ke sebuah server FTP. Sementara server FTP adalah sebuah

Windows Service atau daemon yang berjalan di atas sebuah komputer yang merespons perintah-perintah dari sebuah klien FTP. Perintah-perintah FTP dapat digunakan untuk mengubah direktori, mengubah modus pengiriman antara biner dan ASCII, menggugah berkas komputer ke server FTP, serta mengunduh berkas dari server FTP.

2.9 Mikrotik

Mikrotik adalah sebuah perusahaan yang bergerak di bidang produksi perangkat keras (*hardware*) dan perangkat lunak (*Software*) yang berhubungan dengan sistem jaringan komputer yang berkantor pusat di Latvia, bersebelahan dengan Rusia. Mikrotik didirikan pada tahun 1995 untuk mengembangkan router dan sistem ISP (*Internet Service Provider*) nirkabel.

2.9.1 Jenis-jenis Mikrotik

Mikrotik di bagi kedalam 2 jenis yaitu yang petama adalah (*software*) Mikrotik RouterOS, dan yang kedua adalah (*hardware*) Mikrotik RouterBoard.

2.9.2 Mikrotik RouterOS

MikroTik RouterOS™ adalah sistem operasi dan perangkat lunak yang dapat digunakan untuk menjadikan komputer manjadi router network yang handal, mencakup berbagai fitur yang dibuat untuk ip network dan jaringan wireless, cocok digunakan oleh ISP dan provider hotspot. Untuk instalasi Mikrotik tidak dibutuhkan piranti lunak tambahan atau komponen tambahan lain. Mikrotik didesain untuk mudah digunakan dan sangat baik digunakan untuk keperluan administrasi jaringan komputer seperti merancang dan membangun sebuah sistem jaringan komputer skala kecil hingga yang kompleks sekalipun.

2.9.3 Mikrotik Routerboard

RouterBoard adalah router embedded produk dari mikrotik. Routerboard seperti sebuah pc mini yang terintegrasi karena dalam satu board tertanam prosesor, ram, rom, dan memori flash. Routerboard menggunakan os RouterOS yang berfungsi sebagai router jaringan, bandwidth management, proxy server, dhcp, dns server dan bisa juga berfungsi sebagai hotspot server.

Ada beberapa seri routerboard yang juga bisa berfungsi sebagai wifi. sebagai wifi access 3point, bridge, wds ataupun sebagai wifi client. seperti seri RB411, RB433, RB600. dan sebagian besar ISP wireless menggunakan routerboard untuk menjalankan fungsi wirelessnya baik sebagai ap ataupun client. Dengan routerboard Anda bisa menjalankan fungsi sebuah router tanpa tergantung pada PC lagi. karena semua fungsi pada router sudah ada dalam routerboard. Jika dibandingkan dengan pc yang diinstal routerOS, routerboard ukurannya lebih kecil, lebih kompak dan hemat listrik karena hanya menggunakan adaptor. untuk digunakan di jaringan wifi bisa dipasang diatas tower dan menggunakan PoE sebagai sumber arusnya.

2.10 Operating Sistem Windows

Windows merupakan sistem operasi yang dirilis oleh Microsoft Windows yang mana tidak seperti pendahulunya yang banyak sekali memperkenalkan banyak fitur-fitur baru, tetapi Windows lebih fokus kepada pengembangan dasar Windows itu sendiri. Dengan tujuan agar bisa lebih kompatibel terhadap aplikasi-aplikasi dan juga perangkat keras pada komputer yang kompatibel dengan Windows Vista.

2.10.1 Kelebihan Opeating Sistem Windows

Berikut adalah beberapa kelebihan yang dimiliki windows diantaranya sebagai berikut:

1. Yang pertama yaitu pada proses bootingnya dan proses shut downya pada Windows lebih cepat Bootingnya delai time, dan juga waktu durasi bootingnya juga lebih cepat.

2. Yang kedua pada Windows mempunyai Device Storage tampilan yang terbaru yang mana berguna agar mempermudah kita untuk ditampilkan pada semua hal yang berhubungan kepada peripheral tertentu, seperti halnya pada tampilan konfigurasi dan dokumentasi.

3. Dapat menghemat konsumsi daya Dapat menghemat daya, oleh karena itu Windows bisa lebih stabil jika dibandingkan dengan Windows Vista.
4. Mengoptimasi dalam prefetching yang mana pada Optimasi proses load datanya untuk HD maupun SSD.
5. System pencarian datanya lebih cepat.
6. Kitapun bisa memilih jaringan Wireless dengan hanya mengkliknya pada sistem trainya.
7. Pada Windows mendukung Teknologi multi touch (layar sentuh).
8. Dan memiliki interface atau tampilan dan juga aplikasinya yang lebih menarik diantaranya :
    a. Snap yang mana aplikasi ini bisa di buka secara bersamaan dan dapat ditampilkan secara bersebelahan.
    b. Home group dimana pada proses berbagi file dan peripheralnya bisa dilakukan dengan cara menghubungkan beberapa PC dengaan System jaringan.
    c. Windows Media Center berfungsi untuk merekam siaran TV, dan dapat menonton tv online.
    d. Jump List dapat memberikan kita kemudahan terhadap user karena hanya dengan mengklik pada pin denga cepat makan bisa membuka kembali salah satu dari beberapa aplikasi yang sedang berjalan.
    e. Web Slices yaitu sebuah fitur yang tersedia yang mana berfungsi untuk memotong bagian dari sebuah situs yang kita targetkan dan kemudian ditempatkan pada toolbar Internet Explorer 8 sebagai referensi yang lebih mudah dan cepat tentunya.

f. Windows Live Essential dimana user dapat mengakses data offline dan bisa melakukan banyak hal untuk foto, video dan juga hal-hallainnya.

g. Parental Control yaitu sebuah kontrol yang berfungsi untuk membatasai hak akses kepada anak-anak contohnya : pengaturan waktu dan juga lamanya akses yang diperbolehkan kepada anak-anak.

2.10.2 Kekurangan Opeating Sistem Windows

Windows memiliki beberapa kekurangan diantaranya sebagai berikut:

1. Mempunyai beberapa program atau aplikasi yang belum bisa beroperasi pada Windows .
2. Pada WIndows di player 12 sering terjadi Bug.
3. Terdapat sebuah hardware yang mana bisa langsung dikenali pada Windows Vista, tetapi tidak bisa dikenali pada Window.
4. Software pada mulanya yang bisa dipaksa untuk di instal pada Windows Vista, tetapi tidak dapat dipaksa untuk kita instal pada Windows.

2.11 Filezilla

FileZilla atau juga dikenal dengan sebutan FileZilla Client, adalah salah satu software FTP yang bersifat free, open source dan cross-platform Fitur utama dari Filezilla adalah :

1. *Site manager* (*Manajer fitur*)

   Mengizinkan pengguna untuk membuat daftar situs FTP beserta data koneksinya, seperti nomor port yang akan difunakan, protokol yang digunakan, dan apakah akan menggunakan log anonim atau normal. Untuk log normal, nama pengguna dan kata sandinya tersebut akan disimpan. Penimpanan kata sandi adalah opsional.

2. *Massage log* (*log* pesan)

   Fitur ini menampilkan output berjenis konsol (*console-type*) yang menunjukkan perintah yang dikirim oleh FileZilla dan respons yang diterima dari server.

3. *File and folder view*

   Ditampilkan di bawah pesan log (*Message log*), menyediakan sebuah tampilan grafis antarmuka untuk FTP. Pengguna dapat menavigasi folder dan melihat dan mengubah isinya pada komputer lokal dan server dengan menggunakan tampilan antarmuka gaya Explorer. Pengguna dapat mendrag dan drop file antara komputer lokal dan server.

4. *Transfer queue (Transfer antrian)*

   Ditampilkan di sepanjang bagian bawah jendela, menunjukkan status realtime setiap antrian atau transfer file yang aktif.