BAB II

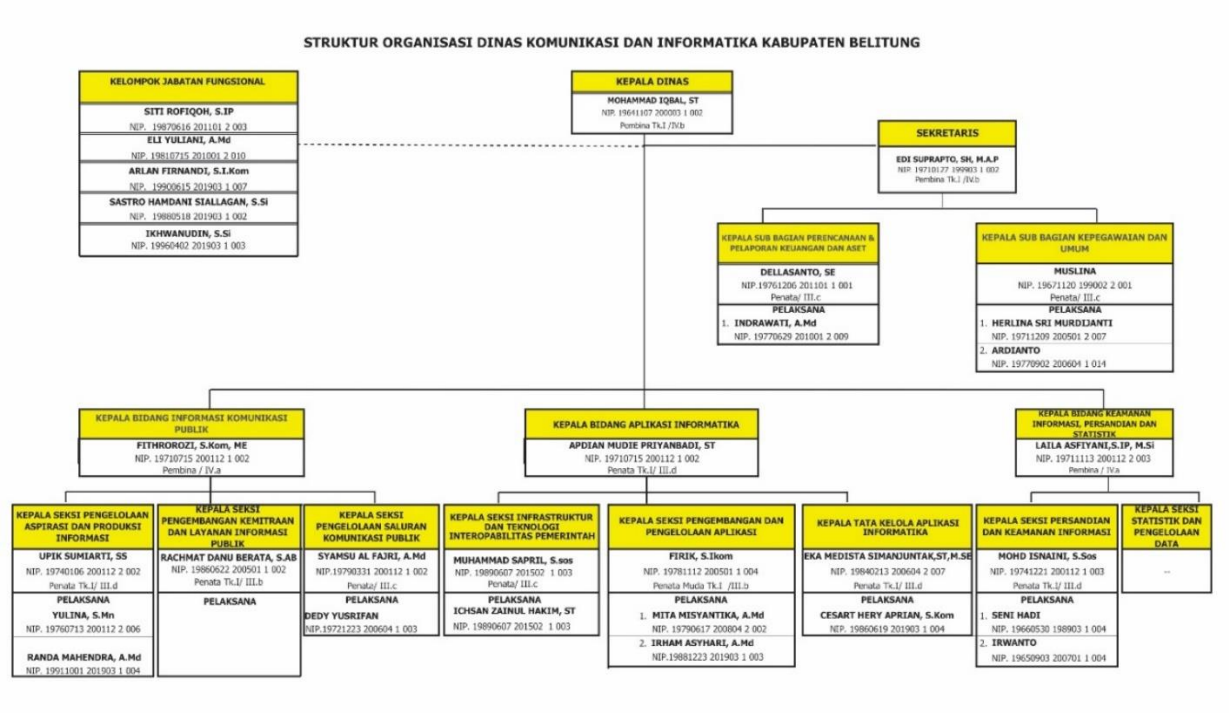
LANDASAN TEORI

2.1 Profil Tempat Penelitian

Dinas Komunikasi dan Informatika (DISKOMINFO) adalah bagian pelaksana urusan pemerintahan dalam bidang komunikasi dan informatika, urusan pemerintahan bidang persandian, dan urusan pemerintahan bidang statistic yang dipimpin oleh Kepala Dinas yang berkedudukan di bawah dan bertanggung jawab kepada Bupati melalui Sekretaris Daerah. Tugas pokok dari Dinas Komunikasi dan Informatika ini yaitu mengkaji dan merumuskan data dan informasi lingkup perencanaan, evaluasi dan pengembangan sumber daya teknologi informasi dan komunikasi. Dan yang kedua menyusun rencana dan program kerja lingkup perencanaan, evaluasi dan pengembangan sumber daya teknologi informasi dan komunikasi. Lokasi penelitian yang penulis jadikan sebagai tempat studi kasus adalah Dinas Komunikasi Dan Informatika (DISKOMINFO) Kabupaten Belitung. Yang ber alamat di Jl. Anwar Dalam Komp.Marakas, Lesung Batang, Tanjungpandan, Belitung Regency, Bangka Belitung Islands 33412. Berikut adalah logo DISKOMINFO Belitung yang dapat dilihat pada Gambar 2.1

Gambar 1.1 Logo DISKOMINFO BELITUNG

2.1.1 Struktur Organisasi DISKOMINFO Belitung



Gambar 2.2 Struktur Organisasi Diskominfo Belitung

2.2 Optimalisasi

Optimasi berasal dari kata optimal yang berarti “terbaik” atau “tertinggi”. Mengoptimalkan berarti menjadikan yang terbaik atau yang tertinggi [8]. Oleh karena itu, tujuan optimalisasi ini adalah upaya optimal untuk mencapai hasil terbaik dalam penyelenggaraan pengelolaan lembaga dan sarana prasarana pendidikan sesuai harapan dan tujuan yang direncanakan. Optimal dengan demikian erat kaitannya dengan kriteria hasil yang dicapai. Suatu perusahaan dapat dikatakan optimal jika mencapai keuntungan maksimum dengan kerugian minimum [9].

2.3 Bandwidth

Bandwidth adalah perhitungan penggunaan data yang tersedia dan dihitung dalam bit per detik. Bandwidth dapat direpresentasikan serta kepadatan jalan raya yang dikelola, arus lalu lintas dan seberapa sering serta seberapa banyak data dapat ditransmisikan dalam suatu koneksi jaringan [10]. Bandwidth (juga dikenal sebagai transmisi data atau lalu lintas data) adalah kapasitas atau kemampuan kabel Ethernet untuk membawa sejumlah lalu lintas paket data tertentu. Data yang masuk dan keluar (upload) disebut juga dengan bandwidth [11].

Dalam sistem jaringan komputer dan berbagai sistem digital lainnya, bandwidth

sering kali didefinisikan dalam bit per detik, seperti jaringan. Bandwidth dapat digunakan untuk mengukur aliran data analog dan data digital. Bandwidth merupakan salah satu konsep pengukuran terpenting dalam jaringan, namun konsep ini memiliki kelemahan atau keterbatasan terlepas dari bagaimana pengguna mengirimkan data atau media apa yang digunakan untuk mengirimkan data tersebut. Hal ini karena alasan fisik dan teknis sehingga menimbulkan keterbatasan dalam hal panjang media yang digunakan, kecepatan maksimum yang digunakan dan penanganan khusus terhadap media yang digunakan [12].

Bandwidth Komputer Dalam jaringan komputer, bandwidth sering disamakan dengan kecepatan transfer data, yaitu jumlah data yang dapat ditransfer dari satu titik ke titik lain dalam jangka waktu tertentu (biasanya detik). Bandwidth jenis ini biasanya diukur dalam satuan bps (bit per second). Terkadang juga dinyatakan dalam bps (byte per second). Modem 57.600 bps memiliki bandwidth dua kali lipat dari modem 28.800 bps. Secara umum, koneksi bandwidth yang besar/tinggi memungkinkan transfer data dalam jumlah besar, seperti transmisi gambar dalam presentasi video. Dihitung dalam satuan bit per detik (bit per second)[13]. Perhatikan bahwa bandwidth yang tercantum untuk komunikasi nirkabel, modem data, komunikasi digital, elektronik, dll. adalah bandwidth yang terkait dengan sinyal analog, diukur dalam Hertz (arti asli istilah tersebut), yang lebih akurat dikenal sebagai bit rate daripada sekarang. ditulis sedikit dalam sedetik. Perhitungan ini juga sangat penting dalam hal kinerja dan biaya jaringan, serta menjadi acuan untuk kebutuhan pengembangan di masa depan. Packet loss (hilangnya paket data dalam proses transmisi) dan desequencing merupakan masalah yang berkaitan dengan kebutuhan bandwidth, namun lebih dipengaruhi oleh stabilitas jaringan, metode antrian yang efisien, router, dan penggunaan kemacetan. Kontrol (memuat informasi) secara online. Packet loss terjadi ketika data terakumulasi pada jalur yang akan dikirim dan menyebabkan buffer overflow pada router [14].

Bandwidth mengacu pada kecepatan transfer data yang didukung oleh koneksi jaringan yang terhubung ke jaringan. Biasanya dinyatakan dalam bit per detik (bps) atau terkadang dalam byte per detik (bps). Bandwidth jaringan mewakili kapasitas koneksi jaringan. Namun, penting untuk memahami perbedaan antara kinerja teoretis dan hasil aktual. Misalnya, jaringan Gigabit Ethernet 1000BASE-T (menggunakan UTP - kabel twisted pair tanpa pelindung) secara teoritis mendukung 1000 megabit per detik (Mbps), namun tingkat ini tidak pernah dapat dicapai dalam praktiknya karena perangkat keras dan perangkat lunak sistem menjadi rusak. Hal ini menghadirkan tantangan ketika menghitung bandwidth [15].

Adapun parameter dalam menentukan Estimasi penggunaan Bandwidt adalah:

1. Jumlah PC Client pada masing-masing distrik
2. Batas bandwidth yang digunakan
3. Aplikasi apa saja yang dijalankan, dan bagaimana performa service-level agreement (SLA) untuk aplikasi - aplikasi tersebut.

Cara untuk memperkirakan seberapa besar kebutuhan bandwidth adalah dengan: Bandwidth yang dibutuhkan = jumlah PC (User) x batas bandwidth Ada dua langkah dasar dalam menghitung bandwidth:

1. Menentukan Jumlah bandwidth jaringan yang sudah ada.
2. Menentukan penggunaan rata-rata aplikasi tertentu.

Kedua langkah ini harus dinyatakan dalam Bps. Jika jaringan Anda dalah GbE (Gigabyte Ethernet), berarti tersedia 125,000,000 Bps. Ini dihitung dengan mengambil 1000 Mbps (untuk jaringan Gigabit); yang setara dengan 1 milyar (1,000,000,000) bps dan membaginya dengan 8 untuk mendapatkan byte. (1,000,000,000 bps / 8 = 125,000,000 Bps) Setelah memastikan besar bandwidth jaringan, Anda perlu menentukan berapa banyak bandwidth yang digunakan aplikasi. Gunakan network analyzer untuk mendeteksi angka Bps dari aplikasi yang dikirim melintasi jaringan[8].

Maka, cara menghitung *bandwidth* tersebut dengan dibagi menjadi 3 bagian yaitu Pengguna Berat, Pengguna Sedang, danh Pengguna Ringan dapat dilihat rumusnya adalah seperti berikut:

Bandwidth yang dibutuhkan = jumlah perangkat (user) x batas bandwidth untuk satu perangkat

Dan dapat dijabarkan juga sebagai berikut :

(jumlah pengguna(userBerat) x batas bandwidth satu perangkat(Kbps)) + (jumlah pengguna(userSedang) x batas bandwidth satu perangkat(Kbps)) + (jumlah pengguna(userRingan) x batas bandwidth satu perangkat(Kbps)) = Total Bandwidth yang dibutuhkan (Kbps/Mbps). **Dengan mungkin penggunaan rumus diatas dapat membantu dalam perhitungan dan pembagian sejumlah bandwidth yang tersedia[8].**

2.4 Load Balancing

Network Load Balancing, suatu teknik untuk memisahkan dua atau lebih koneksi jaringan. Dengan banyak tautan, optimalisasi penggunaan sumber daya, kinerja, atau

waktu respons menjadi lebih baik karena lebih banyak tautan dapat saling mendukung ketika jaringan sedang down dan cepat ketika jaringan normal ketika Anda membutuhkan keandalan yang tinggi. memerlukan ketersediaan koneksi 100 persen dan ingin mengamankan koneksi asli yang berbeda. Untuk mengimplementasikan sistem ini diperlukan perangkat tambahan baik berupa router Cisco atau menggunakan solusi router Mikrotik yang lebih murah namun efisien [16].

Faktanya, penyeimbang beban sederhana hanya dapat menyebabkan nama atau alamat IP yang mewakili mewakili beberapa alamat IP server di belakangnya, namun perangkat yang dirancang khusus untuk menangani penyeimbang beban yang kompleks hanya dapat mewakili layanan yang disediakan oleh server yang akan dibuka di belakangnya. . Dalam sistem loadbalancing, proses loadbalancing mempunyai teknik dan algoritma tersendiri [17]. Algoritme distribusi beban yang berbeda biasanya disediakan dalam perangkat distribusi beban yang kompleks. Tujuannya adalah untuk menyesuaikan distribusi beban dengan properti server di belakangnya. Solusi penyeimbangan beban jaringan digunakan untuk membagi bandwidth yang tersedia di jaringan backbone utama (primer) dengan bandwidth cadangan. Jadi di sini Anda memerlukan cadangan trunk yang berbeda dari cadangan utama dalam hal perutean, mil terakhir, dan bahkan penyedia. Proses penyeimbangan beban sebenarnya adalah proses fleksibel yang dapat dibangun dengan berbagai cara dan metode berbeda. Operasi ini tidak dapat dilakukan dengan perangkat atau perangkat lunak tertentu. Ada banyak cara dan sarana untuk melengkapi jaringan dengan sistem penyeimbangan beban. Cara kerja dan prosesnya juga berbeda. Namun metode yang paling umum dan tersebar luas adalah dengan mengandalkan konsep server virtual atau IP virtual.

Istilah "Virtual Server" atau "Virtual IP" sebenarnya merupakan istilah yang longgar karena sistem lain mungkin menggunakan konsep yang sama tetapi dengan terminologi yang berbeda. Secara umum konsep server virtual atau IP virtual adalah alamat IP, nama, atau bisa juga dikatakan sekelompok alamat IP bertindak sebagai jembatan antara periferal eksternal dan server atau perangkat jaringan di belakangnya.[19]. Tujuan dari sistem representasi ini adalah ketika mengakses nama atau alamat IP secara eksternal, yang menangani permintaan tidak terbatas pada satu perangkat server saja. Kelompok server atau perangkat jaringan yang diwakilinya dapat merespons permintaan ini. Ini mendistribusikan permintaan ini ke beberapa server, sehingga beban kerja di server tersebut tidak terlalu berat. Dengan cara ini, layanan dan layanan yang ditawarkan server kepada pengguna bekerja lebih baik dan dengan kualitas

lebih tinggi [20].

2.5 Jaringan Komputer

Jaringan dapat diartikan sebagai dua atau lebih komputer yang terhubung sedemikian rupa sehingga pada akhirnya mereka dapat berkomunikasi untuk meningkatkan kerja beberapa komputer dan berbagi sumber daya seperti CD-ROM, printer, berbagi file atau memungkinkan komunikasi elektronik di antara keduanya. Jaringan komputer dapat dihubungkan dengan gelombang radio, satelit, saluran telepon, infra merah, dan media kabel lainnya.

Jaringan komputer adalah kumpulan beberapa komputer dan perangkat lain yang terhubung melalui suatu media untuk berkomunikasi satu sama lain. Media berkabel maupun non-kabel dapat digunakan untuk menghubungkan media pada jaringan komputer. Jaringan komputer yang menggunakan media kabel sebagai konektornya biasanya menggunakan kabel twisted pair, coaxial, dan optik. Saat ini, jaringan komputer yang terhubung melalui media nirkabel menggunakan gelombang radio elektromagnetik untuk mengirim dan menerima informasi. Pihak yang meminta/menerima layanan disebut sebagai klien (client) dan pihak penyedia layanan/pengirim disebut sebagai server (server). Model ini disebut sistem client-server dan digunakan di hampir semua aplikasi jaringan komputer. Dua komputer, masing-masing dengan kartu jaringan, kemudian dihubungkan dengan kabel atau nirkabel sebagai alat komunikasi, dan perangkat lunak pengoperasian jaringan membentuk jaringan komputer sederhana. Jika ingin membuat jaringan komputer dengan dimensi yang lebih besar, diperlukan perangkat tambahan seperti perangkat penghubung, seperti hub, bridge, switch, router, gateway [22]. Sejarah jaringan komputer berawal dari munculnya konsep jaringan komputer di Amerika pada tahun 1940an. Ini tumbuh dari proyek pengembangan komputer MODEL I dari kelompok penelitian Bell Laboratory dan Universitas Harvard yang dipimpin oleh Profesor Howard Aiken. Pada awalnya proyek ini hanya ingin menggunakan satu perangkat komputasi yang harus digunakan secara bersamaan. Agar dapat mengerjakan beberapa proses tanpa membuang banyak waktu luang maka dibuatlah proses batch, sehingga satu komputer dapat menjalankan beberapa program dengan satu aturan antrian. Kemudian pada tahun 1950an, ketika jenis komputer mulai berkembang dan muncul superkomputer, komputer harus melayani beberapa lokasi (terminal) yang tersedia. Oleh karena itu, bentuk jaringan komputer pertama kali

digunakan [23].

2.6 Metode Queue Tree

Queue Tree adalah pelimitan yang sangat rumit dikarenakan pelimitan ini berdasarkan protokol, ports, IP Address. Queue Tree berfungsi untuk melimit bandwidth pada mikrotik yang mempunyai dua koneksi internet karena paket marknya lebih berfungsi dari pada di Simple Queue. Queue Tree juga digunakan untuk membatasi satu arah koneksi saja baik itu download maupun upload. Jika sebuah konfigurasi queue pada Queue Tree ditujukan untuk melakukan queue terhadap bandwidth download, maka konfigurasi tersebut tidak akan melakukan queue untuk bandwidth upload, demikian pula sebaliknya. Jika memiliki beberapa konfigurasi queue pada queue tree, maka konfigurasi queue tersebut akan dieksekusi secara bersamaan atau simultan. Ini menyebabkan urutan konfigurasi queue pada queue tree tidak berpengaruh terhadap hasil manajemen bandwidth yang diinginkan karena pada saat konfigurasi, tidak bisa memindahkan urutan dari konfigurasi queue yang ada. Dengan diprosesnya paket secara simultan, maka penggunaan queue tree jelas akan lebih mempercepat processing packet. Sehingga untuk melakukan queue terhadap traffic upload dan download dari sebuah komputer client, kita harus membuat 2 (dua) konfigurasi queue[6], [9].

Pada saat akan menerapkan queue pada jaringan, dikenal dua rate atau alokasi bandwidth yang akan didapat oleh setiap user, yaitu Committed Information Rate (CIR), merupakan alokasi bandwidth terendah yang bisa didapatkan oleh sebuah user jika traffic jaringan sangat sibuk. Seburuk apapun keadaan dari jaringan tersebut, komputer user tidak akan mendapatkan alokasi bandwidth di bawah dari CIR. Yang kedua adalah Maximum Information Rate (MIR), merupakan alokasi bandwidth maksimum yang bisa didapatkan komputer user. MIR biasanya akan didapatkan seorang user jika ada alokasi bandwidth yang tidak digunakan lagi oleh user lain[10]. Queue tree adalah konfigurasi yang bersifat one way (satu arah), yang berarti sebuah konfigurasi queue hanya akan mampu melakukan queue terhadap satu arah jenis traffic. Jika sebuah konfigurasi queue pada queue tree ditujukan untuk melakukan queueterhadap bandwidth download, maka konfigurasi tersebut tidak akan melakukan queue untuk bandwidth upload, demikian pula sebaliknya. sehingga untuk melakukan queue tree terhadap traffic upload dan download dari sebuah komputer pengguna, harus membuat 2 (dua) konfigurasi queue yaitu,

download dan upload[7].

Prinsip top to bottom dalam mengeksekusi konfigurasi queue treejuga tidak berlaku lagi di queue tree. Jika memiliki beberapa konfigurasi queue pada queue tree, maka konfigurasi queue tersebut akan dieksekusi secara simultan atau bersamaan. Dengan diprosesnya packet secara simultan, maka penggunaan queue tree jelas akan lebih mempercepat processing packet. Penandaan paket (Mark Packet) berfungsi mengidentifikasi sebuah aliran paket data dalam sebuah queue tree. Apabila saat penandaan paket pada firewall mangle tidak tepat, maka pekerjaan penandaan paket akan gagal[6], [7].

2.7 Mikrotik

Mikrotik merupakan salah satu distributor hardware dan software yang menyediakan hardware untuk router. Misalnya Routerboard dan RouterOs. Mikrotik RouterOs merupakan sistem operasi yang mengubah komputer menjadi router jaringan dengan berbagai fungsi untuk jaringan IP dan jaringan nirkabel, yang banyak digunakan oleh perusahaan dan instansi pemerintah pada umumnya. Mikrotik diproduksi oleh perusahaan MikroTikls di kota Riga, Latvia. Latvia adalah negara yang "memisahkan" dari bekas Uni Soviet, atau Rusia saat ini. Dengan merek Mikrotik, didirikan pada tahun 1995 dan awalnya ditujukan untuk Penyedia Layanan Internet (ISP) atau Internet Service Provider (ISP) yang melayani pelanggannya menggunakan teknologi nirkabel atau nirkabel [26]. Saat ini MikroTikls memberikan layanan kepada banyak penyedia layanan jaringan nirkabel di bidang layanan akses Internet di banyak negara di dunia dan juga mulai populer di Indonesia. Mikrotik pada perangkat standar berbasis komputer dikenal dengan kestabilan, pengendalian kualitas dan fleksibilitas dalam memproses berbagai jenis paket data dan proses routing atau lebih dikenal dengan istilah routing. Didesain sebagai router berbasis komputer, Mikrotik sangat berguna bagi ISP yang ingin menjalankan banyak aplikasi, dari yang paling sederhana hingga yang paling canggih. Contoh aplikasi yang dapat diimplementasikan Mikrotik selain routing adalah aplikasi manajemen kapasitas akses (bandwidth), firewall, wireless access point (WiFi), link backhaul, sistem hotspot, server virtual private network (VPN) dan masih banyak lagi yang lainnya [9].

2.8 OpenWRT

OpenWrt adalah Sebuah sistem operasi Linux dan OpenSource yang dirancang khusus untuk router dan perangkat jaringan lainnya. OpenWrt dibuat untuk menjadi sistem operasi dengan fitur lengkap dan mudah dimodifikasi untuk perangkat tertanam atau *embedded*. Dalam artian user dapat memiliki semua fitur openwrt yang dibutuhkan tanpa *bloatware*. Openwrt juga menyediakan *filesystem* yang dapat ditulis dengan sesuka hati, yang dimana pengguna dibebaskan dari batasan pemilihan fitur dan konfigurasi yang disediakan vendor atau memungkinankan pengguna menyesuaikan fitur yang digunakan agar sesuai dengan aplikasi yang digunakan[11].

Dan Openwrt juga didukung oleh kernel Linux yang lebih baru dibandingkan kebanyakan distro lainnya, Openwrt juga bebas dari General Public License (GPL) dimana banyak kontributor relawan yang membantu dalam pengembangan Openwrt, dan openwrt juga bebas biaya berlangganan atau lisensi (openwrt dokumen). , 2023). Setiap perangkat jaringan tetap dan nirkabel yang dijual di pasaran harus memiliki sertifikat nirkabel. Masing-masing perangkat tersebut memiliki standar yang berbeda-beda tergantung kemampuannya, namun kini sebagian besar terutama router sudah mengadopsi standar 802.11n. Masing-masing router tersebut mempunyai fitur-fitur yang digunakan untuk mendukung jaringan nirkabel seperti: sistem keamanan jaringan dan kemampuan komunikasi jaringan nirkabel dengan perangkat lain. Namun, router yang ada di pasaran belum bisa dikatakan optimal [27].

Karena kesatuan ruangan yang berbeda. Oleh karena itu, perlu adanya perubahan firmware dari yang asli ke firmware OpenWRT yang mendukungnya untuk memaksimalkan kemampuan perangkat router. Selain itu, tujuan penggunaan fitur ini biasanya untuk memigrasikan firmware asli ke firmware sumber terbuka. Namun penggunaan fitur ini disertai dengan penggunaan modul tambahan untuk membangun sistem hotspot portabel yang dapat dengan mudah diimplementasikan dengan perangkat lain. Kelemahan OpenWRT adalah ia menimbulkan konsumsi daya tambahan, yang sebenarnya terbatas pada router. Namun, Anda masih dapat menemukan solusi menggunakan hub USB dengan DC/adaptor. Sehingga konsumsi dayanya tidak membebani kinerja router. Selain itu, terdapat kelemahan lain pada arsitektur router, yaitu dapat ditransfer ke perangkat lain [27].

Hal inilah yang dianalisa dalam penelitian ini untuk mengetahui sejauh mana sistem hotspot portable berjalan dengan baik dan memberikan fasilitas penyimpanan lokal, audio player, video player dan chatting. Dalam melakukan analisa ini digunakan bantuan

modul-modul perangkat lunak dan modul-modul perangkat keras. Hasil analisa ini diharapkan sistem hotspot portable dapat di terapkan pada perangkat lain.

2.9 Router

Router adalah perangkat jaringan komputer yang dapat mengirim data dari satu jaringan ke jaringan lain dengan menemukan jalur terbaik untuk mengirim data tersebut. Kegunaan alat ini adalah untuk mentransfer paket IP dari satu host ke host lainnya. Lebih tepatnya, alat untuk menyelaraskan jaringan IP yang berbeda sehingga dapat berkomunikasi satu sama lain. Di warnet, router bertindak sebagai pintu gerbang antara LAN warnet dan jaringan lainnya. Router bertindak sebagai jembatan jaringan; H. dapat meneruskan paket data jaringan dan juga membagi jaringan menjadi beberapa segmen atau menghubungkan segmen jaringan. Router dapat dibagi sebagai berikut.

Router Aplikasi Router jenis ini adalah aplikasi yang dapat Anda instal pada sistem operasi komputer Anda, sehingga sistem operasi komputer Anda dapat bertindak sebagai router, misalnya. B. Aplikasi WinGate, WinProxy Winroute, SpyGate dll. Tipe lainnya adalah perangkat keras router. Perangkat keras router adalah perangkat keras yang memiliki fitur seperti router, memungkinkan Anda berbagi alamat IP dengan perangkat keras tersebut. Perangkat keras router dapat digunakan untuk berbagi jaringan internet di suatu area[12]. Misalnya router ini adalah base station, area yang menerima alamat IP dan koneksi Internet disebut hot spot. Yang ketiga adalah router komputer. Router komputer adalah komputer yang telah dimodifikasi untuk digunakan sebagai router. Anda tidak harus menggunakan komputer dengan spesifikasi tinggi untuk membuat router komputer. Komputer dengan prosesor Pentium Dua, hard disk 10 GB dan memori RAM 64 serta kartu LAN sudah dapat digunakan sebagai router komputer. Sistem operasi router khusus harus diinstal pada komputer yang digunakan sebagai router. Sistem operasi yang populer saat ini untuk router PC adalah Mikrotik[28].

Cara Kerja Router Tugas utama router adalah meneruskan paket (informasi). Sebuah router mempunyai kemampuan routing, artinya router dapat dengan cerdas mendeteksi ke mana suatu rute data (paket) harus pergi, apakah ditujukan ke host lain di jaringan yang sama atau di jaringan berbeda. Jika paket ditujukan ke host di jaringan lain, router meneruskannya ke jaringan tersebut. Di sisi lain, jika paket ditujukan ke host di jaringan yang sama, router akan memblokir paket keluar.

Dan router juga mempunyai fungsi yaitu fungsi utama router adalah menghubungkan beberapa jaringan untuk mentransfer data dari satu jaringan ke jaringan lainnya. Namun, router berbeda dengan switch karena switch hanya menghubungkan beberapa komputer dan membentuk LAN (Local Area Network). Ketika router digunakan untuk menghubungkan satu LAN ke LAN lainnya. Kedua, router juga digunakan untuk mentransfer data dari satu jaringan ke jaringan lain, yang sistemnya bertindak sebagai jembatan. Ketiga, router juga menghubungkan jaringan lokal ke koneksi DSL, yang juga dikenal sebagai router DSL. Router-router ini biasanya memiliki firewall yang memfilter paket berdasarkan alamat sumber dan tujuan paket, namun tidak semua router memiliki fitur yang sama. Router dengan fitur pemfilteran paket juga dapat disebut sebagai filter paket. Fungsi umum dari router ini adalah untuk memblokir lalu lintas yang dikirim untuk mencegah badai siaran, yang dapat memperlambat kinerja jaringan [29].

2.10 IP Address

IP Address adalah singkatan dari Internet Protocol Address. IP address digunakan sebagai alat identifikasi untuk tiap komputer dalam jaringan Internet berbasis TCP/IP. *Transmission Contro Protocol/Internet Protocol* (TCP/IP) adalah alamat host dalam jaringan yang dibuat oleh *Departement of Defence* (DoD) supaya komunikasi berjalan lancar. TCP/IP pada model DoD tidak seperti model OSI, hanya terdiri dari empat layer yaitu layer process/application, layer *Host-to-Host, layer internet, layer network access*. IP address memiliki dua fungsi. Selain sebagai alat identifikasi host atau antarmuka jaringan, juga sebagai alamat lokasi jaringan[13].

Fungsi IP address sebagai alamat lokasi jaringan dapat diilustrasikan sebagai sebuah nama untuk mempermudah mengingat kata daripada mengingat deretan angka yang menunjuk pada suatu website, sebuah alamat untuk mengetahui di mana website tersebut, dan juga sebuah rute agar dapat mencapai alamat tersebut. Pada awalnya para pembuat sistem IP address menggunakan bilangan sepanjang 32-bit. Alamat IP merupakan pasangan dari identitas jaringan (network id) dan identitas komputer atau perangkat lain (host id) yang terhubung dalam suatu jaringan komputer[14]. Alamat IP ini digunakan untuk mengirim dan menerima paket data dari dan ke perangkat yang terhubung dalam suatu jaringan komputer. Tetapi karena semakin tinggi tingkat pertumbuhan jumlah dan kapasitas Internet, maka menyebabkan dibutuhkan sistem pengalamat yang lebih besar. Sistem pengalamatan tersebut dikenal sebagai IPv6 dan

diperkenalkan sejak tahun 1995[15].

2.11 Internet Service Povider (ISP)

ISP adalah produsen atau lembaga yang memberikan pelayanan kepada konsumen supaya bisa mengakses internet dan berbagai lokasi. Tentu saja Anda tidak bisa mendapatkannya secara gratis, karena ini adalah layanan berbayar. Internet Service Provider lebih familiar dengan sebutan provider internet atau penyedia internet. Jaringan yang ditawarkan oleh ISP luas, bisa untuk penggunaan lokal maupun internasional sehingga bisa saling terhubung secara global. Data bisa mengalir melalui jaringan transmisi data dari satu tempat ke tempat yang lain dengan hitungan detik. Ada banyak jalur transmisinya, bisa melalui sinyal radio, modem, kabel, dan jalur lainnya[16].

Tentu saja ada biaya bulanan untuk layanan berbayar ISP yang terbagi dalam dua kategori, layanan modem dan broadband. Pada kategori sambungan jaringan telepon atau sambungan modem, harganya relatif lebih murah. Kabel telepon yang tersedia secara komersial, yang dapat dipasang di kantor atau di rumah, berfungsi sebagai media transmisi Internet broadband, asalkan dapat diakses. Kategori kedua adalah broadband, atau broadband, yang biasanya ditransmisikan melalui internet nirkabel, modem, satelit, dan lain-lain.

Koneksi broadband lebih cepat, namun harganya lebih tinggi. Internet Broadband dapat menjadi solusi bagi wilayah yang belum terjangkau oleh infrastruktur jaringan kabel. ISP bertindak sebagai jembatan antara komputer pengguna, perangkat, dll. ke Internet melalui modem router. Fungsi ISP memeriksa alamat IP pengguna, bila perlu modem terhubung ke Internet [33].

2.12 Paket Loss

Paket Loss didefinisikan selaku hilangnya beberapa paket data pada jaringan komputer sepanjang proses transmisi paket data menggapai tujuannya. Aspek pemicu Paket Loss bisa terjalin sebab collision serta congestion antara data pada jaringan serta perihal ini mempengaruhi pada seluruh aplikasi yang terdapat di jaringan LAN, sebab retransmisi hendak mengurangi efisiensi jaringan secara totalitas walaupun jumlah bandwidth lumayan ada buat aplikasi-aplikasi tersebut. Packet Loss, adalah persentase paket yang hilang selama mentransmisikan data. Hal ini disebabkan oleh banyak faktor seperti penurunan sinyal dalam media jaringan, kesalahan

perangkat keras jaringan, atau juga radiasi dari lingkungan sekitar[17].

Pada beberapa network transfer protocol seperti TCP yang bersifat connection oriented, menyediakan pengiriman kembali (restransmission) atau pengiriman secara otomatis (resends) paket yang hilang selama proses transmisi walau segmen telah tidak diakui. Walaupun TCP memiliki kelebihan tersebut, jika TCP melakukan retransmitting atau resends, throughput jaringan semakin menurun. Berbeda halnya dengan protokol UDP yang bersifat connectionless, tidak menyediakan retransmission maupun Resends jika terjadi kehilangan paket. Misalkan pl adalah packet lost, pt adalah paket yang dikirim, dan pr adalah paket yang diterima, nilai standar nya dapat dilihat pada tabel 2.1 berikut.

Table 2.1. Standar Packet Loss

Kategori Degrasi	Packet Loss
Sangat Bagus	0%
Bagus	3%
Sedang	15%
Tidak bagus	25%

Untuk mengukur nilai packet loss dapat menggunakan rumus persamaan pada Gambar 2.4 berikut.

$$Packet\ Loss = \frac{\text{Paket Data Dikirim} - \text{Paket Data Diterima}}{\text{Paket Data Dikirim}} \times 100$$

Gambar 2.4 Rumus mengukur nilai Packet Loss

2.13 Throughput

Throughput merupakan keahlian sesungguhnya sesuatu jaringan dalam melaksanakan pengiriman data. Umumnya throughput senantiasa berhubungan dengan bandwidth yang sesungguhnya pada waktu tertentu serta pada keadaan jaringan internet tertentu. Dalam throughput ialah jumlah total kehadiran paket yang sukses yang diamati pada tujuan sepanjang interval waktu tertentu dipecah oleh durasi interval waktu tersebut. Throughput diukur dalam satuan bit per-second serta rumus yang digunakan buat mencari throughput. Dapat dilihat pada tabel 2.2 dibawah adalah standar nilai throughput[17].

Table 2.2. Standar Throughput

Kategori Throughput	Throughput %	Indeks
Sangat Bagus	100%	4

Bagus	75%	3
Sedang	50%	2
Tidak bagus	25%	1

Untuk mengukur nilai throughput dapat menggunakan rumus persamaan dapat dilihat pada Gambar 2.6 berikut.

$$Throughput = \frac{\text{Jumlah Data Diterima}}{\text{Lama Pengamatan}}$$

$$\%\ Throughput = \frac{Throughput}{Alokasi\ Bandwidth\ User} \times 100\ \%$$

Gambar 2.6 Rumus mengukur nilai Throughput

2.14 Delay

Delay merupakan waktu yang diperlukan oleh satu paket dari asal ke sumber tujuan. Di tegaskan kembali oleh yang berkata kalau delay merupakan waktu tunda sesuatu paket yang disebabkan oleh proses transmisi dari satu titik ke titik lain yang jadi tujuannya. Delay atau latency atau round trip time delay, adalah waktu yang dibutuhkan untuk sebuah paket yang dikirimkan dari suatu komputer ke komputer yang dituju. Delay dalam sebuah proses transmisi paket dalam sebuah jaringan komputer disebabkan karena adanya antrian yang panjang, atau mengambil rute lain untuk menghindari kemacetan pada routing. Untuk mencari delay pada paket yang ditransmisikan dengan membagi antara panjang paket (satuannya bit) dibagi dengan link bandwidth (satuannya bit/s). Untuk mengukur delay pada suatu jaringan komputer menggunakan perintah ping yang merupakan salah satu perintah yang dimiliki oleh command prompt sistem operasi Windows, dimana time pada hasil perintah ping menunjukkan delay pada paket yang dikirimkan Menurut versi TIPHON, besarnya delay bisa dihitung dengan persamaan seperti pada tabel 2.3 berikut[17].

Table 2.3. Standar Delay

Kategori Delay	Besar Delay (ms)	Indeks
Sangat Bagus	< 150 ms	4
Bagus	150 ms – 300 ms	3
Sedang	300 ms – 450 ms	2
Tidak bagus	>450 ms	1

Untuk mengukur nilai delay dapat menggunakan rumus persamaan dapat dilhat pada

Gambar 2.8 berikut.

$$\text{Rata} - \text{Rata } Delay = \frac{\text{Total } Delay}{\text{Total Paket Diterima}}$$

Gambar 2.8 Rumus mengukur nilai Delay

2.15 Jitter

Secara universal jitter ialah perbandingan waktu kehadiran dari sesuatu paket ke penerima dengan waktu yang diharapkan. Jitter diakibatkan sebab variasi-variasi dalam panjang antrian, dalam waktu pengelolaan data, serta pula dalam waktu penghimpunan ulang paket-paket diakhiri ekspedisi jitter. Jitter atau variasi delay , adalah variasi dari delay atau selisih antara Delay pertama dengan delay selanjutnya. Jika variasi delay dalam transmisi terlalu lebar, maka akan mempengaruhi kualitas data yang ditransmisikan. Jumlah toleransi jitter dalam jaringan dipengaruhi oleh kedalaman dari buffer jitter dalam peralatan jaringan. Jika buffer jitter tersedia lebih banyak, maka jaringan dapat mereduksi efek dari jitter. Contoh dari jitter, misalnya hasil ping menunjukkan delay dengan rentang 2ms, 4ms, 7ms. Maka jitter dapat dihitung dengan mengurangi delay akhir dengan delay sebelumnya, seperti contoh tersebut maka jitternya adalah 7ms-4ms=3ms. Untuk mengukur jitter dapat kita gunakan fasilitas UDP test pada perangkat lunak iperf Jitter bisa dihitung dengan persamaan seperti pada tabel 2.4 berikut[17].

Table 2.4. Standar Jitter

Kategori Jitter	Jitter (ms)	Indeks
Sangat Bagus	0 ms	4
Bagus	0 ms – 75 ms	3
Sedang	75 ms – 125 ms	2
Tidak bagus	125 ms – 225 ms	1

Untuk mengukur nilai jitter dapat menggunakan rumus persamaan dapat dilhat pada Gambar 2.10 berikut.

$$Jitter = \frac{\text{Total Variasi } Delay}{\text{Total Paket Diterima}}$$

$$= \frac{Delay - (\text{Rata} - \text{Rata } Delay)}{\text{Total Paket Diterima}}$$

Gambar 2.10 Rumus mengukur nilai Jitter

2.16 LAN

LAN seringkali menggunakan teknologi transmisi kabel tunggal. LAN tradisional beroperasi pada kecepatan mulai 10 sampai 100 Mbps (Mega Bits per detik) dengan delay rendah (puluhan micro second) dan mempunyai faktor kesalahan yang kecil, LAN-LAN modem dapat beroperasi pada kecepatan yang lebih tinggi, sampai ratusan megabit per detik. Sistem LAN yang sering digunakan adalah system Ethernet yang dikembangkan oleh perusahaan Xerox. Penggunaan titik koneksi Intermediate (seperti Repeater, Bridge, dan Switch) memungkinkan LAN terkoneksi membentuk jaringan yang lebih luas. LAN juga dapat terkoneksi ke WAN (Wide Area Network), atau MAN (Metropolitan Area Network) lain dengan menggunakan Router[18].

2.17 WAN

Jaringan area luas (bahasa Inggris: Wide Area Network; WAN) merupakan jaringan komputer yang mencakup area yang besar sebagai contoh yaitu jaringan komputer antar wilayah, kota atau bahkan negara, atau dapat didefinisikan juga sebagai jaringan komputer yang membutuhkan router dan saluran komunikasi publik. WAN digunakan untuk menghubungkan jaringan area lokal yang satu dengan jaringan lokal yang lain, sehingga pengguna atau komputer di lokasi yang satu dapat berkomunikasi dengan pengguna dan komputer di lokasi yang lain[19].

Jaringan area metropolitan, atau biasa disebut Metropolitas Area Network disingkat MAN, adalah jaringan komputer yang mencakup wilayah kampus, kantor, administratif, atau metropolitan, biasanya menghubungkan jaringan area lokal melalui jaringan tulang punggung berkecepatan tinggi. Jaringan MAN merupakan perpaduan beberapa jaringan lokal. Jangkauannya 10-50 km. MAN adalah jaringan yang menghubungkan pengguna ke sumber daya komputasi di wilayah geografis atau wilayah yang lebih besar dari yang dicakup oleh LAN tetapi lebih kecil dari yang dicakup oleh WAN. Istilah ini digunakan untuk menghubungkan jaringan metropolitan menjadi jaringan yang lebih besar (yang pada gilirannya juga memungkinkan koneksi yang efisien ke jaringan WAN). Istilah ini juga mengacu pada interkoneksi beberapa jaringan lokal dengan menjembataninya dengan jalur utama. Beberapa universitas besar juga menggunakan istilah MAN untuk menggambarkan jaringannya[36].

MAN merupakan pilihan yang tepat untuk membangun jaringan antar lokasi

dalam kota antara pabrik/kantor dan kantor pusat dalam jarak yang mudah dijangkau. Untuk membangun jaringan MAN, operator telekomunikasi biasanya perlu menghubungkan jaringan komputer. MAN mendukung data teks dan audio bahkan dapat dihubungkan ke jaringan TV kabel atau gelombang radio. MAN (seperti WAN) biasanya tidak dimiliki oleh satu organisasi. MAN, tautan dan perangkat telekomunikasinya biasanya dimiliki oleh komunitas pengguna atau oleh penyedia layanan jaringan yang menjual layanan kepada pengguna. Di kota-kota di seluruh dunia, contoh jaringan metropolitan dengan berbagai ukuran meliputi wilayah metropolitan London, Inggris; Lodz, Polandia. Misalnya, kota Cambridge dan Massachusetts telah mengembangkan perangkat MAN yang menghubungkan puluhan LAN di kampus dan fasilitas medis [37].

2.18 SSH

Pada awalnya SSH dikembangkan oleh Tatu Yl nen di Helsinki University of Technology. SSH memberikan alternatif yang secure terhadap remote session tradisional dan file transfer protocol seperti telnet dan relogin.Protokol SSH mendukung otentikasi terhadap remote host, yang dengan demikian meminimalkan ancaman pemalsuan identitas client lewat IP address spoofing maupun manipulasi DNS. Selain itu SSH mendukung beberapa protocol enkripsi secret key (DES,TripleDES,IDEA, dan Blowfish) untuk membantu memastikan privacy dari keseluruhan komunikasi, yang dimulai dengan username/password awal.SSH menyediakan suatu virtual private connection pada application layer, mencakup interactive logon protocol (ssh dan sshd) serta fasilitas untuk secure transfer file (scd)[20]. Setelah meng-instal SSH, sangat dianjurkan untuk mendisable telnet dan rlogin. Implementasi SSH pada linux diantaranya adalah OpenSSH[21]. SSH merupakan paket program yang digunakan sebagai pengganti yang aman untuk rlogin, rsh dan rcp. Ia menggunakan public-key cryptography untuk mengenkripsi komunikasi antara dua host, demikian pula untuk autentikasi pemakai. Ia dapat digunakan untuk login secara aman ke remote host atau menyalin data antar host, sementara mencegah man-in-themiddle attacks (pembajakan sesi) dan DNS spoofing atau dapat dikatakan Secure Shell adalah program yang melakukan loging terhadap komputer lain dalam jaringan, mengeksekusi perintah lewat mesin secara remote, dan memindahkan file dari satu mesin ke mesin lainnya.

SSH tidak dirancang untuk dimasukkan ke gateway jaringan seperti router atau firewall sebagai solusi lengkap VPN. Hal ini dimungkinkan untuk membuat VPN dengan

tunneling PPP melalui SSH, tetapi membutuhkan banyak overhead dan tidak dimaksudkan untuk menangani koneksi dengan banyak kebutuhan bandwidth seperti IPsec. TLS / SSL dan IPsec hampir benar-benar transparan untuk digunakan, tetapi SSH tidak, untuk menggunakan SSH Anda harus login ke account pengguna untuk memanfaatkan keamanan lapisan transport. SSH digunakan untuk aplikasi scripting, sedangkan TLS / SSL dan IPSec adalah dimasukkan ke dalam aplikasi dan TCP / IP stack. UDP dan ICMP juga masalah dengan SSH. Tidaklah mungkin untuk terowongan lalu lintas UDP atau ICMP. Protokol-protokol ini memang dapat berguna dalam beberapa VPN, misalnya mengamankan audio streaming melalui VPN. Masalah lain dengan SSH adalah bahwa ada begitu banyak implementasi berbeda dari protokol bahwa masalah interoperabilitas adalah mulai muncul, misalnya implementasi yang berbeda dari server mungkin tabrakan dengan klien dan wakil sebaliknya. Hal ini terjadi meskipun yang SSH menjadi standar oleh IETF[21].

SSH adalah program yang memungkinkan anda untuk login ke sistem remote dan memiliki koneksi yang terenkripsi. SSH merupakan paket program yang digunakan sebagai pengganti yang aman untuk rlogin, rsh dan rcp. Ia menggunakan public-key cryptography untuk mengenkripsi komunikasi antara dua host, demikian pula untuk autentikasi pemakai. SSH sangat murah, bahkan gratis untuk penggunaan non-komersial dan biaya sedikit untuk penggunaan komersial. SSH tersedia dua versi SSH-1 dan SSH-2. SSH-2 adalah versi terbaru dan paling aman dan SSH-1 masih sangat popular (dapat ditemukan sebagai lisensi GPL untuk semua platform). Dan memiliki beberapa keterbatasan dalam fitur dan memiliki beberapa masalah keamanan yang berbahaya, misalnya menggunakan CRC untuk perlindungan integritas tidak aman. SSH memiliki ketersediaan tinggi dan berjalan pada hampir seluruh platform. SSH-2 guna mendukung banyak algoritma enkripsi seperti 3DES, IDEA, Blowfish, Twofish dan Cast. SSH VPN dalam bentuk yang paling sederhana menggunakan kemampuan SSH ke port layanan terowongan di Internet di dalam sebuah session SSH. Meskipun memiliki keterbatasan, mudah untuk melakukan setup, kebutuhan non-administratif akses dan bekerja dengan andal. Anda dapat pula menggunakan SSH dari stasiun kerja Windows anda ke server SSH Linux. Terdapat beberapa implementasi client Windows yang tersedia gratis dan juga implementasi komersil dari DataFellows[22].

Menurut OpenSSH page OpenSSH adalah versi FREE dan SSH sebagai tool untuk melakukan konektivitas pada jaringan. Jika anda menggunakan telnet, rlogin, dan ftp mungkin tanpa anda sadari bahwa password yang terkirim tanpa melalui enkripsi.

Sedangkan dengan menggunakan OpenSSH melakukan enkripsi kepada semua trafik (termasuk password), secara efektif untuk menghindari hal-hal yang tidak diinginkan. Secara tambahan, Open SSH memiliki tunneling yang aman dan beberapa metode autentikasi dan juga mendukung semua versi protokol SSH. Open SSH sangatlah pas untuk bisa menggantikan rlogin dan telnet dengan program SSH, rcp dengan SCP dan ftp dengan sftp. Juga termasuk sshd (paket server-side), dan juga tool lain seperti ssh-add, sshagent, ssh-keysign, sshkeyscan, ssh-keygen dan sftp-server. Suatu contoh dalam SSH Client, anda asumsikan memiliki account di server : namaserver.com (ip address) dan mesin tersebut menjalankan ssh server[23].

Account Anda pada server di refer pada username dan password Anda misal password 123. Untuk dapat masuk menggunakan ssh, anda dapat dengan melakukan perintah : ssh -l username : namaserver.com atau jika Anda belum memiliki namaserver, dengan menggunakan ip address : ssh -l username xxx.xxx.xxx.xxx (x merepresentasikan ip address) alternatif jika tidak menggunakan parameter -l : ssh username@namaserver.com atau ssh username@xxx.xxx.xxx.xxx Dengan melakukan perintah tersebut Anda lalu akan diminta memasukkan password. SCP Client Selain itu kita juga bisa melakukan copy file. Misal Anda akan melakukan transfer file yang bernama file.txt pada mesin yang berbeda : scp /home/username/file.txt username@namaserver.com:~/home/username/ Pertama kita menuliskan perintah scp, selanjutnya kita menentukan letak file yang ingin kita copy berada "/home/username/file.txt". Lalu seperti menggunakan ssh selanjutnya kita menentukan username dan namaserver, terakhir menentukan letak file yang ingin kita tuju ":~/home/username/". Jika kita ingin mengcopy isi folder dengan menambahkan parameter -r seperti ini : scp -r /home/username/direktori username@namaserver.com:~/home/username/ Jika mengubah port dari SSH, standarnya port ssh adalah 22, dengan mengubahnya, maka saat anda melakukan koneksi dari client anda harus menspesifikasikan port tersebut, misal : ssh -l username xxx.xxx.xxx.xxx 44 Pada port tersebut telah di buka. Juga buka file konfigurasi untuk opsi lebih lanjut yang dapat diubah : /etc/ssh/ssh_config (untuk client) dan atau /etc/ssh/sshd_config (untuk server). Jika merubah apapun yang ada di sshd_config, jangan lupa untuk merestart kembali ssh server tersebut[21].

Manfaat SSH diantaranya untuk terowongan berbasis TCP aplikasi melalui SSH, misalnya email protokol, tool pemrograman dan bahkan aplikasi bisnis seperti Oracle. Untuk sebagian besar pengguna SSH tampaknya terminal emulator mirip dengan Telnet.

Para pengguna tidak melihat enkripsi dan oleh karena itu keamanan transparan bagi pengguna. Untuk administrator sistem SSH adalah populer remote administrasi platform. SSH dirancang untuk menggantikan protokol telnet dan FTP yang mempunyai banyak fitur lain, tetapi tujuan utamanya memang untuk mengamankan komunikasi melalui internet. SSH merupakan produk serbaguna yang dirancang untuk melakukan banyak hal, yang kebanyakan berupa penciptaan tunnel antar host. Beberapa implementasi SSH tergantung pada SSL libraris karena SSH dan SSL menggunakan banyak menggunakan algoritma enkripsi yang sama (misalnya TripleDES (Pengembangan dari DES oleh IBM)[21].

2.19 Konfigurasi

Konfigurasi dalam bahasa inggris ‘configuration’ adalah istilah umum artinya bentuk, wujud untuk menjelaskan mengenai orang ataupun benda. Dalam ilmu geografi konfigurasi memiliki arti bentuk horizontal dan vertikal dari bumi, sedangkan pada ilmu kimia konfigurasi adalah kedudukan atom yang satu dengan atom yang lain dalam suatu molekul. Konfigurasi sistem akan digunakan untuk menentukan batasan tugas masing – masing komponen akan disimpan pada suatu lokasi didalam sistem atau sudah terdefenisi didalam sistem itu melalui komponen yang lain. Lokasi ini disebut ruang konfigurasi. Suatu sistem akan bekerja dengan apabila semua komponen sudah berkonfigurasi, adanya suatu sistem akan bekerja secara optimal apabila konfigurasi optimal pula.Suatu sistem, seperti komputer, robot, mobil, manusia, alam dan sebagainya terdiri dari kumpulan objek – objek (disebut komponen) yang saling bekerjasama satu dengan yang lain dalam suatu tatanan mengikuti aturan tertentu untuk mencapai tujuan. Oleh sebab itu dapat dikatakan bahwa suatu sistem adalah sesuatu yang terorganisasi adalah suatu sistem. Setiap komponen daripada sistem mempunyai fungsi masing – masing secara berbeda dan tujuan akan dapat dicapai apabila sistem mempunyai konfigurasi untuk mengatur hubungan dan kegunaan antara satu komponen dengan komponen lain[40][55].

Dan pada ilmu komputer konfigurasi, artinya bagian yang mencakup dari susunan piranti keras maupun piranti lunak yang digerakkan dengan sistem untuk menyelesaikan berbagai keperluan. Biasanya kita bisa saksikan, pada pertunjukan drum band atau marching band, anggotanya bergerak secara semangat dalam struktur tertentu untuk menciptakan suatu konfigurasi, seperti sebuah logo, wajah tokoh, dan lain sebagainya. Konfigurasi mempunyai makna yaitu, suatu model ataupun pola dari kultur suatu daerah

pada waktu tertentu. Model ataupun pola kultur itu, telah terbentuk menjadi ciri khas dari suatu wilayah tersebut, dan pastinya berbeda dari wilayah lainnya. Konfigurasi merupakan wujud, susunan, setting, penjelasan keadaan dari suatu sitem terkhusus untuk mengoprasikan suatu metode[25].

2.20 Quality of Service (QoS)

Quality of Service (QoS) merupakan metode pengukuran tentang seberapa baik jaringan dan merupakan suatu usaha untuk mendefinisikan karakteristik dan sifat dari satu servis. QoS digunakan untuk mengukur sekumpulan atribut kinerja yang telah dispesifikasikan dan diasosiasikan dengan suatu servis. Analisis jaringan menggunakan QoS (Quality of Service) khususnya adalah latency dan throughput mampu memberikan analisis jaringan yang baik, dimana aspek ini yang sering digunakan didalam analisis jaringan. QoS didefinisikan sebagai sebuah mekanisme atau cara yang memungkinkan layanan dapat beroperasi sesuai dengan karakteristiknya masing-masing dalam jaringan IP (Internet Protocol). QoS mengacu pada kemampuan jaringan untuk menyediakan layanan yang lebih baik pada trafik jaringan tertentu melalui teknologi yang berbeda-beda. QoS menawarkan kemampuan untuk mendefinisikan atribut-atribut layanan jaringan yang disediakan, baik secara kualitatif maupun kuantitatif. Pada Tabel I diperlihatkan nilai presentase dari QoS. Dapat dilihat pada Gambar 2.11 dibawah[26].

Nilai	Persentase (%)	Indeks
3,8 – 4	95 – 100	Sangat Memuaskan
3 – 3,79	75 – 94,75	Memuaskan
2 – 2,99	50 – 74,75	Kurang Memuaskan
1 – 1,99	25 – 49,75	Jelek

Gambar 2.11 Persentase Dan Nilai QoS

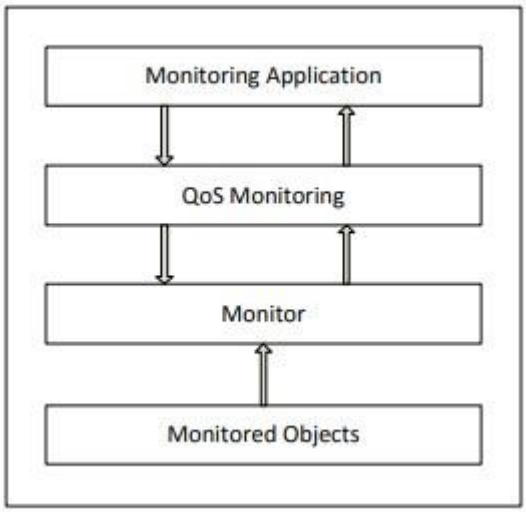
Hasil analisis QoS (Quality of Service), dapat dijadikan rekomendasi untuk implementasi fisik jaringan internet yang harapan kedepannya bisa menunjang penambahan layanan-layanan yang dapat menunjang kegiatan kantor. Pada penelitian ini mengukur layanan jaringan internet dari parameter delay/latency, jitter, packet loss dan throughput. Tujuan dari penelitian ini adalah menganalisis jaringan internet di Satuan Kerja UPT. Loka Uji Penambangan Jampang Kulon – LIPI yang telah ada dengan menggunakan parameter QoS (Quality of Service), untuk menghasilkan suatu informasi berupa, Waktu yang dibutuhkan oleh sebuah paket data terhitung dari saat pengiriman oleh transmitter sampai saat diterima oleh receiver (throughput). Perbedaan selang waktu

kedatangan antar paket di terminal tujuan (delay/latency)[27]. Banyaknya paket yang hilang selama proses transmisi ke tujuan (packet loss). Jumlah bit yang diterima dengan sukses perdetik melalui sebuah sistem atau media komunikasi (kemampuan sebenarnya suatu jaringan dalam melakukan pengiriman data) (jitter).

Model Monitoring QoS terdiri dari komponen monitoring application, QoS monitoring, monitor, dan monitored object

1. Monitoring Application Merupakan sebuah antarmuka bagi administrator jaringan. Komponen ini berfungsi mengambil informasi lalu lintas paket data dari monitor, menganalisanya dan mengirimkan hasil analisis kepada pengguna. Berdasarkan hasil analisis tersebut, seorang administrator jaringan dapat melakukan operasi-operasi yang lain.
2. QoS Monitoring Menyediakan mekanisme monitoring QoS dengan mengambil informasi nilai-nilai parameter QoS dari lalu lintas paket data.
3. Monitor Mengumpulkan dan merekam informasi lalu lintas paket data yang selanjutnya akan dikirimkan kepada monitoring application. Monitor melakukan pengukuran aliran paket data secara waktu nyata dan melaporkan hasilnya kepada monitoring application.
4. Monitored Objects Merupakan informasi seperti atribut dan aktifitas yang dimonitor di dalam jaringan. Di dalam konteks QoS monitoring, informasi-informasi tersebut merupakan aliran-aliran paket data yang dimonitor secara waktu nyata. Tipe aliran paket data tersebut dapat diketahui dari alamat sumber (source) dan tujuan (destination) di layer-layer IP, port yang dipergunakan misalnya UDP atau TCP, dan parameter di dalam paket RTP[43][55].

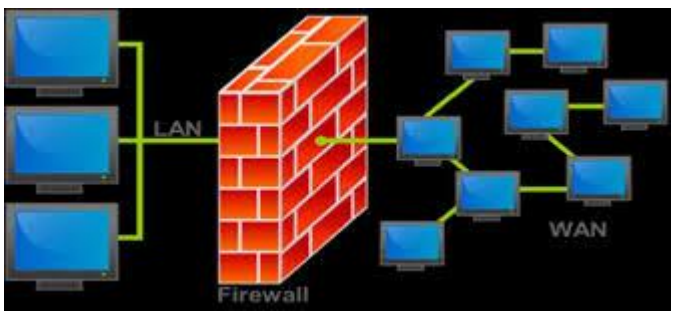
Menurut informasi QoS yang dapat diperoleh, monitoring QoS dapat diklasifikasikan ke dalam dua kategori yaitu monitoring QoS dari ujung ke ujung (end to end QoS monitoring (EtE QM)) dan monitoring distribusi QoS per Node (distribution monitoring (DM)). Di dalam EtE QM, monitoring QoS dilakukan dengan cara mengukur parameter-parameter QoS dari pengirim kepada penerima. Sedangkan di dalam DM, proses monitoring QoS dilakukan di segmen-segmen jalur pengiriman atau antara node-node tertentu yang dikehendaki di sepanjang jalur pengiriman paket data dapat dilihat pada Gambar 2.12 Model Monitoring QoS dibawah[29].



Gambar 2.12 Model Monitoring QoS

2.21 Firewall

Firewall didefinisikan sebagai sebuah komponen atau kumpulan komponen yang membatasi akses antara sebuah jaringan yang diproteksi dan internet, atau antara kumpulan-kumpulan jaringan lainnya Firewall merupakan solusi untuk mengatasi keamanan di dalam dunia internet baik itu keamanan komputer maupun keamanan jaringan yang banyak dipenuhi dengan berbagai ancaman baik dari dalam maupun dari luar. Dengan suatu konfigurasi yang tepat pada firewall maka kemungkinan untuk mengamankan suatu data atau komputer pada jaringan menjadi jauh lebih aman. Suatu konfigurasi firewall yang baik dan optimal dapat mengurangi ancamanancaman tersebut. Konfigurasi firewall terdapat 3 jenis diantaranya adalah screened host firewall system (single-homed bastion), screened host firewall system (Dual-homed bastion), dan screened subnet firewall. Dan juga mengkonfigurasikan firewall dengan membuka port-port yang tepat untuk melakukan hubungan koneksi ke internet, karena dengan mengkonfigurasi port-port tersebut suatu firewall dapat menyaring paket-paket data yang masuk yang sesuai dengan policy atau kebijakannya[30]. Berikut dapat dilihat penggambaran firewall pada Gambar 2.13.



Gambar 2.13 Penggambaran Firewall

Arsitektur firewall ini yang akan digunakan untuk mengoptimalkan suatu firewall pada jaringan Konfigrasi suatu firewall yang pertama adalah penentuan policy atau kebijakan firewall tersebut tentang apa saja yang akan dikenai kebijakan tersebut, siapa saja yang akan dikenai kebijakan tersebut dan layananlayanan yang dibutuhkan tiap individu tersebut. Kemudian menentukan port-port yang digunakan oleh berbagai protokol dan membuka port-port tersebut kedalam firewall, dan juga membuka port yang digunakan untuk file sharing dan request ping. Selanjutnya adalah menentukan suatu konfigurasi yang tepat dan sesuai dengan keadaan jaringannya. Screened subnet merupakan konfigurasi yang paling tinggi tingkat keamanannya. Dengan konfigurasi tersebut memungkinkan firewall kita dapat menigkatkan keamanan yang jauh lebih baik dari ancaman-ancaman internet. Namun tidak menutup kemungkinan bahwa jaringan kita tetap dapat diserang oleh hacker yang serangannya sangat terarah. Namun lebih baik sedikit terlindungi daripada tidak sama sekali. Firewall merupakan alat untuk mengimplementasikan kebijakan security (security policy)[45][56].

Sedangkan kebijakan security, dibuat berdasarkan perimbangan antara fasilitas yang disediakan dengan implikasi security-nya. Semakin ketat kebijakan security, semakin kompleks konfigurasi layanan informasi yang tersedia di jaringan Dalam dunia nyata, firewall adalah dinding yang bisa memisahkan ruangan, sehingga kebakaran pada suatu ruangan tidak menjalar ke ruangan lainnya. Tapi sebenarnya firewall di Internet lebih seperti pertahanan disekeliling benteng, yakni mempertahankan terhadap serangan dari luar. Diantara kegunaannya yaitu :

1. Membatasi gerak orang yang masuk ke dalam jaringan internal
2. Membatasi gerak orang yang keluar dari jaringan internal
3. Mencegah penyerang mendekati pertahanan yang berlapis

firewall tersebut (tidak melalui chocke point).

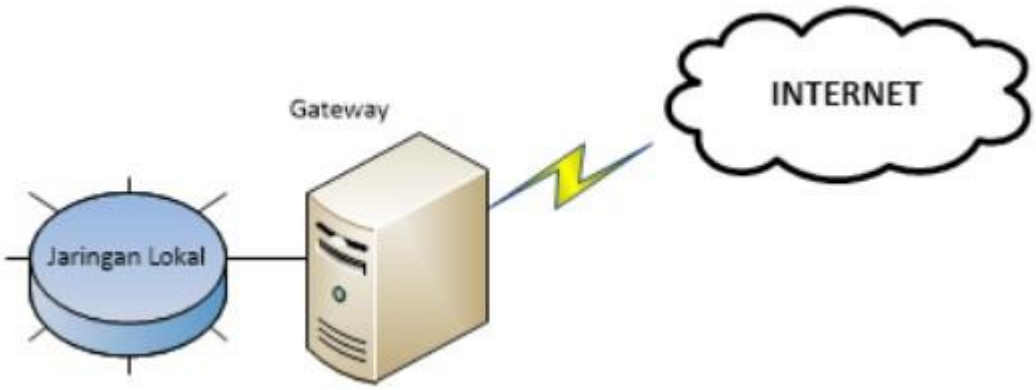
1. Firewall tidak bisa melindungi jaringan internal terhadap serangan-serangan model baru.

Tugas tugas firewall yaitu di antaranya yang pertama adalah memfilter jaringan yang tidak di inginkan dengan kebijakan sistem security di jaringan (site security policy). yang kedua, semua trafik yang ada untuk dilewatkan firewall bagi semua pemberian dan pemanfaatan layanan informasi. Firewall secara umum di peruntukkan untuk melayani, Mesin/Komputer, Jaringan Terpenting harus dapat mengimplementasikan kebijakan security di jaringan (site security policy), Melakukan filtering, Merekam atau mencatat

serta memberitahu administrator terhadap segala usaha menembus kebijakan security[30].

2.22 NAT (Network Address Translator)

Network Address Translation (NAT) adalah suatu metode untuk menghubungkan lebih dari satu komputer ke jaringan internet dengan menggunakan satu alamat IP publik (Grang and Gupta, 2013). Metode NAT banyak digunakan di seluruh dunia termasuk di Indonesia. Pada dasarnya semua jenis NAT beroperasi dengan cara client – server. Dalam hal ini, klien di zona internal yang memulai permintaan untuk memperoleh sumber daya dari server di zona internet publik (Masoud, 2013). Di sini semua klien akan mendapatkan alamat IP lokal yang diberikan oleh komputer server. Dengan mekanisme NAT terbatasnya IP publik tidak menjadi masalah. Salah satu syarat untuk menghubugkan komputer ke jaringan internet adalah dengan menggunakan IP publik. Melalui NAT memungkinkan beberapa node untuk berbagi satu atau lebih alamat IP publik. Dapat dilihat pada Gambar 2.14 dibawah bagaimana mekanisme NAT[31].



Gambar 2.14 Mekanisme NAT

Gateway NAT berada pada batas jaringan lokal dan publik dan memodifikasi alamat IP lokal dan port dari paket yang diperuntukkan untuk jaringan publik. Paket IP yang dibundel dengan IPSec, seperti AH dan ESP secara intrinsik dimaksudkan untuk melindungi integritas dari paket IP (termasuk sumber dan tujuan alamat) dari perubahan atau gangguan karena peran fundamental NAT gateway untuk memodifikasi alamat IP dalam header paket, IPSec, dan NAT memiliki ketidakcocokan intrinsik (Ahmad and Yaacob, 2012). NAT bekerja dengan mengalihkan suatu paket data dari suatu alamat IP ke alamat IP lainnya. Ketika suatu paket dialihkan, NAT akan mengingat dari mana asal paket dan kemana tujuan paket tersebut. Apabila paket kembali, NAT akan

mengirimkannya ke alamat asal atau dengan kata lain host hanya akan menerima paket yang dikirim atau yang dimintanya sehingga komunikasi dapat berjalan dengan baik. Jaringan komputer LAN yang menggunakan NAT disebut dengan NATted Network. Sebagai contoh, di MikroTik NAT digunakan untuk komunikasi internal dan komunikasi eksternal maksudnya pengalihan data dapat dilakukan untuk paket yang berasal dari jaringan NATted (internal) ke jaringan luar eksternal atau dari jaringan luar menuju jaringan NATted. Hal tersebut sering disebut dengan komunikasi dua arah dari dan ke jaringan NATted atau internal. Untuk mengetahui mekanisme bagaimana sebuah NAT bekerja. Bentuk NAT yang melupakan penerjemahan dua arah, terutama jika terdapat nomor yang sama antara alamat IP public dan local. Agar tidak terjadi konflik, maka NAT mengubah nomor IP public menjadi nomor yang tidak terdapat dalam jaringan local[18].

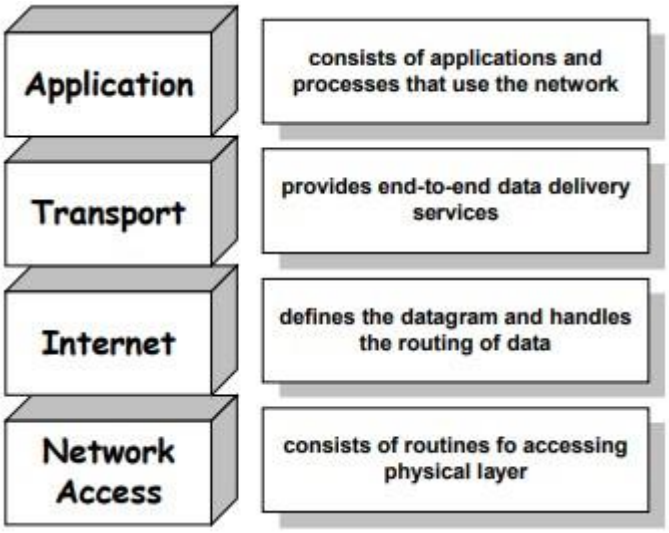
Ada beberapa fungsi NAT yaitu Melakukan penghematan terhadap IP legal yang disediakan oleh internet service provider (ISP), Meminimalisir adanya duplikasi alamat IP dalam jaringan, Ketika terjadi perubahan jaringan, menghindari proses pengalamatan Kembali, Menambah fleksibilitas untuk terhubung dengan jaringan internet, Melakukan peningkatan terhadap keamanan sebuah jaringan, Dibandingkan dengan aplikasi alternatif seperti proxy, penggunaan NAT memberikan fleksibilitas dan performa yang lebih baik. Walaupun begitu, dibalik semua fungsi dan kelebihannya, sebetulnya ada juga beberapa kekurangan yang mesti dirasakan pengguna NAT, seperti misalnya mengalami delay switching Ketika proses translasi, kehilangan kemampuan melacak IP end to end, dan juga ada beberapa aplikasi yang menolak bekerja saat menggunakan NAT[32].

2.23 Protocol TCP/IP

TCP/IP merupakan standar komunikasi data yang digunakan dalam proses tukar-menukar data dari satu komputer ke komputer lain. TCP/IP merupakan jaringan terbuka yang bersifat independen terhadap mekanisme transport pada 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 banyak 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 untuk membentuk jaringan yang heterogen.

TCP/IP (Tranmission Control Protocol/Internet Protocol) memungkinkan

hubungan virtual antar komputer, dimana dua komputer atau lebih akan dapat saling berhubungan untuk pertukaran data serta layanan aplikasi jaringan lainnya. Pada model TCP/IP terdapat empat lapisan yang memiliki fungsionalitas masing-masing, yaitu : Physical Layer, Network Access, Internet Layer, Transport Layer, Application Layer. TCP/IP lahir dari sebuah proyek yang dibiayai oleh Defense Advanced Reasearch Project Agency (DARPA) pada tahun 1969, jauh sebelum model OSI dipublikasikan. TCP/IP mulai popular pada pengembangan di Universitas Barkely Amerika Serikat dan implementasinya dalam sistem berbasis UNIX. Di lain pihak, protokol TCP/IP hanya terdiri dari 5 (lima) lapisan yaitu physical, data link, network, transport dan application. Empat lapisan pertama (paling bawah) dari TCP/IP mewakili empat lapisan terbawah dari model OSI yaitu physical, data link, network, transport. Sedangkan lapisan paling atas TCP/IP (application) mewakili tiga lapisan model OSI paling atas yaitu session, presentation dan application[33]. Dalam beberapa buku literatur, arsitektur protokol TCPI/IP beserta fungsinya dapat dilihat pada Gambar 2.15 dibawah dengan urutan sebagai berikut[34].



Gambar 2.15 Lapisan Protocol TCP/IP

Tujuan daripada desain TCP/IP adalah yang pertama, Standart protokol yang open, artinya spesifikasi dapat diperoleh dengan bebas dan dikembangkan sesuai dengan hardware yang dimiliki. Dengan demikian TCP/IP dapat diimplementasikan pada platform hardware yang beragam. Yang kedua, Tidak tergantung pada jaringan fisik hardware. TCP/IP dapat diintegrasikan pada jaringan fisik yang bermacam-macam melalui ethernet, token ring, dial up (telepon) RS232 dan media tramsmisi lainnya. Yang ketiga, Skema address yang luas. Skema adress internet memungkinkan komputer mempunyai identitas tunggal (IP-address), sehingga walaupun mempunyai jangkauan

international (wordwide), komputer manapun dapat dicapai dengan mudah karena mempunyai identitas yang jelas. Dan yang terakhir Standar aplikasi. Utilitas standar yang akan memudahkan pemakaiannya dalam melakukan file transfer, remote login dan remote execution[34].

2.24 PC Router

Router PC adalah sebuah komputer yang dimodifikasi sedemikian rupa sehingga dapat digunakan sebagai router. Untuk membuat sebuah router PC tidak harus menggunakan komputer dengan spesifikasi yang tinggi. Komputer dengan prosesor pentium dua, hard drive 10 GB dan ram 64 serta telah tersedia LAN Card sudah bisa digunakan sebagai router PC. Komputer yang dijadikan router ini harus diinstal dengan sistem operasi khusus untuk router. Sistem operasi yang populer untuk router PC saat ini adalah Mikrotik. Sistem operasi yang banyak dipakai pada PC router adalah Linux dan BSD. Ternyata Linux yang digunakan pada penelitian ini dalam keadaan instalasi default, performa transfer data yang dihasilkan belum optimal[35].

Fungsi PC router sama dengan dedicated router, namun dari sisi performa dan kinerja, tidak dapat dipungkiri dedicated router lebih unggul dalam beberapa hal. PC router dapat di-install oleh sistem operasi apa saja, asalkan sistem operasi itu mendukung untuk routing. Untuk itu penelitian ini bertujuan untuk mengoptimasi PC router agar transfer data yang dilakukan menjadi optimal dan efisien. Karena karakeristik Linux yang open source, penulis mencoba optimasi dari sisi operating sistem yang ada, yaitu pada kernel dan service. Perubahan pada nilai MTU (Maximum Transfer Unit) yang diujikan ternyata memberikan dampak yaitu penurunan throughput pada PC router[36].

2.25 Failover

Failover adalah sebuah teknik menambahkan koneksi di mikrotik, dimana jika salah satu koneksi internet mati (koneksi utama) maka koneksi yang satunya (koneksi cadangan) akan mem-backup koneksi utama. Dan pergantian koneksi dari koneksi utama ke koneksi cadangan akan berjalan secara otomatis. Menurut (Malau, 2022) Failover dapat memberi bantuan jika ada masalah pada salah satu jalur internet (ISP). Dengan cara memindahkan gateway ke jalur aktif secara otomatis. Menurut (Dani & Suryawan, 2017) failover adalah hal yang bisa dilakukan sistem jaringan untuk melakukan pindah ke sistem backup jika sistem utama mengalami kegagalan. Menurut (Wahyudi et al., 2019)

Teknik yang dapat mengalihkan jalur internet utama ke jalur internet cadangan sehingga komunikasi dapat berlanjut meskipun jalur internet utama mengalami kegagalan disebut teknik failover[37].

2.26 Multi Wan (MWAN3)

Multi Wan (MWAN3) merupakan sebuah paket yang disediakan oleh Openwrt dan dikembangkan oleh Adze dan Arfett.dan mulai diperkenalkan pada OpenWrt versi 12.09 (Attitude Adjustment" yang dirilis pada tahun 2012. Yang dimana Mwan3 sendiri memiliki script untuk melakukan Loadbalancing secara berdasarkan interface yang disetting. Mwan3 Menggunakan metode Linux Policy routing untuk menseimbangkan koneksi yang keluar dari Multi Wan tersebut, Mwan sendiri menggunakan Loadbalancing Per-IP Connection basic, yang dimana akan menandai paket yang menuju *gateway* tertentu, dan ketika paket kembali akanmelalui *gateway* yang dilewati.

Mwan3 bekerja berdasarkan "hotplug-event", ketika interface *UP* atau muncul, maka Mwan3 akan membuat kustom *Routing table* dan *iptales Rules*. Tabel tersebut akan dibuat untuk setiap interface WAN. Kemudian Script Mwan3 akan membuat aturan iptables dan menggunakan iptables MARK untuk menandai trafik tertentu. Berdasarkan aturan ini, kernel dapat menentukan tabel routing mana yang akan digunakan. Ketika sebuah interface mati, maka Mwan3 akan menghapus semua aturan dan rute ke interface yang mati tersebut[19].

2.27 Ethernet

Model Interface Ethernet ditemukan di Xerox Palo Alto Research Center (PARC) di tahun 1970-an oleh Dr. Robert M. Metcalfe. Ethernet pertama berjalan dengan kecepatan 3 Mbps dan dikenal sebagai Ethernet Eksperimental. Interface ini merupakan sebuah card yang terhubung ke card yang lain melalui ethernet hub dan kabel UTP atau hanya menggunakan sebuah kabel BNC yang diterminasi di ujungnya. Dasar pemikiran dirancangnya ethernet dapat menggunakan satu kabel untuk berkomunikasi. Karena hanya digunakan satu kabel saja, maka proses pemancaran data harus dilakukan bergantian. Mirip ketika terjadi pembicaraan di forum atau rapat[38]. Jika seseorang sedang berbicara, maka orang lain seharusnya diam dan mendengarkan. Jika pada saat bersamaan terdapat dua orang yang berbicara, pendengar akan merasa terganggu. Sebelum satu card ethernet memancarkan datanya pada kabel, dia harus mendeteksi

terlebih dahulu ada tidaknya card lain yang sedang memancar. Jika tidak ada maka dia akan memancar. Jika ada maka card ethernet akan menunggu sampai kabel dalam keadaan kosong. Jika pada saat bersamaan dua card memancarkan data maka terjadilah collison / tabrakan (hal ini dideteksi oleh card yang bersangkutan dengan memeriksa tegangan kabel, jika tegangan ini melampaui batas tertentu, maka terjadi collison). Jika collison terjadi maka masing-masing card berhenti memancar dan menunggu lagi dengan selang waktu yang acak untuk mencoba memancar kembali. Karena selang waktu pancar masing-masing card yang acak ini, maka kemungkinan collison lebih lanjut menjadi lebih kecil. Karena dalam satu kabel terdapat banyak card ethernet, maka kita harus mempunyai suatu metode untuk mengenali dan membedakan masing-masing card ethernet tersebut. Untuk itu, pada setiap card ethernet telah tertera kode khusus sepanjang 48 bit yang dikenal sebagai ethernet address[39].

2.28 Winbox

Winbox adalah sebuah software atau utility yang di gunakan untuk meremote sebuah server mikrotik ke dalam mode GUI (Graphical User Interface) melalui operating system windows. Kebanyakan teknisi banyak mengkonfigurasi mikrotik os atau mikrotik routerboard menggunakan winbox dibanding dengan yang mengkonfigurasi langsung lewat mode CLI (Command Line Interface). Menurut Divine dalam bukunya yang berjudul Network Infrastructure Administration, Winbox merupakan aplikasi bawaan dari Mikrotik untuk melakukan administrasi routerboard, semua fungsi router dapat dikelola dengan aplikasi tersebut. Dan winbox merupakan software jaringan yang berfungsi sebagai konektivitas dan konfigurasi Mikrotik dengan menggunakan MAC Address atau protocol IP.

2.29 Switch

Switch LAN adalah perangkat yang secara tipikal mempunyai beberapa port untuk menghubungkan beberapa segmen LAN lain yang berkecepatan rendah, switch pada prinsipnya sama seperti hub. Perbedaannya adalah switch dapat beroperasi dengan mode half-duplex dan mampu mengalihkan jalur dan memfilter informasi ke dan dari tujuan yang spesifik. Dengan kata lain, dapat menentukan jalur transfer data. Ada dua jenis arsitektur dasar yang digunakan pada switch, yaitu cut-through dan store-and-forward. Switch cut-through memiliki kelebihan di sisi kecepatan karena ketika sebuah paket

datang, switch hanya memperhatikan alamat tujuannya sebelum meneruskan paket ke segmen tujuan. Sedangkan pada switch store-and-forward, ketika menerima paket, isi paket akan dianalisa terlebih dahulu sebelum meneruskannya ke alamat tujuan, sehingga memungkinkan switch untuk mengetahui adanya kerusakan pada paket dan mencegahnya agar tidak mengganggu kerja jaringan[53].

Switch pada dasarnya mempunyai fungsi seperti Hub yaitu sebagai pembagi sinyal dan penguat sinyal pada jaringan komputer akan tetapi switch lebih cerdas dari pada Hub karena Switch dapat mengenali alamat data yang harus ditransmisikan dan mampu mengatur lalu lintas data dalam jaringan secara lebih baik dibandingkan dengan Hub. Switch merupakan titik percabangan dari proses transfer data sehingga jika switch mengalami masalah maka seluruh koneksi jaringan dan proses transfer data akan terganggu. Switch biasanya memiliki banyak port yang akan menghubungkan ke jaringan komputer dan port - port tersebut akan berhubungan dengan konektor RJ 45[53]. Berikut merupakan Gambar yang menunjukkan bentuk fisik dari switch, dapat dilihat pada Gambar 2.16 sebagai berikut.

Gambar 2.16 Switch

Setiap komputer yang tergabung dalam sebuah jaringan akan ditandai dengan alamat yang berbeda-beda. Kalau diibaratkan, IP address ini seperti alamat rumah pada sebuah jalan. Jaringan yang akan kita bangun diistilahkan sebagai jalanan, dan komputer-komputer yang tergabung dalam jaringan tersebut diibaratkan rumah-rumah. Jadi antara komputer memiliki IP address yang berbeda-beda antara satu dengan yang lainnya. Bayangkan apa jadinya bila dalam sebuah jalan terdapat dua rumah yang memiliki nomor alamat yang sama. Jika terdapat surat yang hendak dikirim ke nomor alamat yang sama tersebut, pastilah surat tersebut tidak akan pernah sampai pada tujuannya, karena bingung mana alamat yang benar. Begitu pula dengan penggunaan IP address pada setiap

komputer yang ada dalam jaringan. Jika terdapat alamat yang sama[53].

2.30 Access Points

Access Points (AP) merupakan perangkat wireless yang berfungsi sebagai pusat akses jaringan yang biasa dikenal juga sebagai wireless router. AP dalam menyebarkan jaringan biasa digunakan pada indoor atau outdoor. Perbedaan pada AP untuk indoor dan outdoor memiliki perbedaan yang sangat signifikan yaitu pada outdoor memiliki daya dan jangkauan radio yang lebih luas dibanding indoor. Dalam membangun sebuah Internet Service Provider (ISP) dengan menggunakan AP kita dapat menggunakannya untuk memberikan service pada client wireless. Pada dasarnya AP memiliki fungsi sebagai bridge antara jaringan wireless dan jaringan kabel LAN. AP memiliki prinsip kerja seperti switch atau hub yang digunakan untuk jaringan berbasis kabel. Dari kedua perangkat keras tersebut yang membedakan adalah dalam melakukan transmisi data switch dan hub menggunakan kabel UTP, sedangkan AP menggunakan gelombang radio pada medium udara[53][54]. Berikut merupakan Gambar yang menunjukkan bentuk fisik dari Access Points, dapat dilihat pada Gambar 2.17 berikut.

Gambar 2.17 Access Points (AP)

Access point terhubung langsung ke jaringan area lokal berkabel, biasanya Ethernet. Access point kemudian menyediakan koneksi nirkabel menggunakan teknologi LAN nirkabel, biasanya Wi-Fi, untuk perangkat lain yang menggunakan koneksi kabel itu. Access point mendukung koneksi beberapa perangkat nirkabel melalui satu koneksi kabelnya[54]. Access point bekerja saat ada perangkat yang mencoba mengakses jaringan. Biasanya pada layar smartphone akan muncul tampilan yang berisi permintaan pengisian sandi. Selanjutnya access point akan mengatur agar perangkat tersebut bisa terhubung dengan cara mencocokan apakah sandi yang dimasukan ke access point sudah benar atau belum. Apabila sandi yang dimasukan sudah tepat maka akan memberikan

alamat IP ke perangkat supaya bisa terhubung ke jaringan. Access point menyediakan koneksi antara jalur data sinyal RF (Radio Frekuensi) yang dibentuk oleh wifi dengan jalur data elektrik pada kabel ethernet[54].