

## **BAB II**

### **TINJAUAN PUSTAKA**

#### **2.1. Profil Tempat Penelitian**

SMK Negeri 8 Bandung merupakan sekolah menengah kejuruan negeri yang berada di Kota Bandung, Jawa Barat, Indonesia. Berlokasi di Jalan Kliningan No. 31 RT 03 RW 06, Kelurahan Turangga, Kecamatan Lengkong, Kota Bandung. Masa pendidikan di SMK Negeri 8 Bandung ditempuh dalam waktu tiga tahun pelajaran, mulai dari kelas X hingga kelas XII, seperti pada umumnya masa pendidikan sekolah menengah kejuruan di Indonesia. Sejak berdirinya 1976 Hingga sekarang SMK Negeri 8 Bandung telah dipimpin oleh 14 orang kepala sekolah. Dapat dilihat Logo SMK Negeri 8 Bandung pada gambar 2.1 sebagai berikut.



*Gambar 2. 1. Logo SMKN 8 Bandung*

Gambar 2.1 merupakan Logo SMKN 8 Bandung dimana logo tersebut memiliki lambang setiap Jurusan yang dimiliki.

#### **2.1.1. Visi dan Misi**

Visi dan misi dari SMK Negeri 8 Bandung adalah sebagai berikut:

##### **A. Visi**

Menjadi sekolah berwawasan lingkungan yang unggul untuk menghasilkan lulusan yang berakhlak mulia dan profesional.

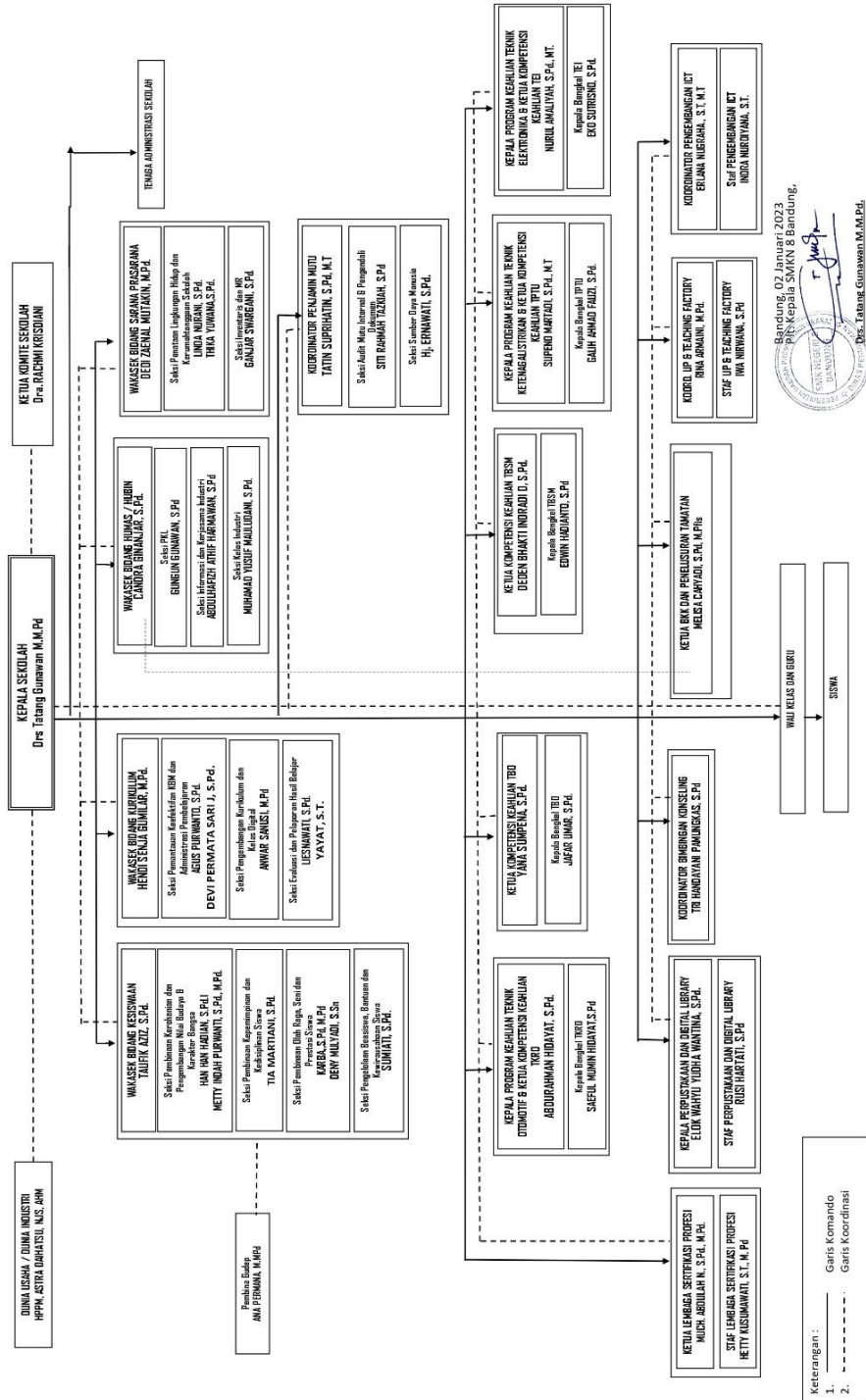
## B. Misi

1. Memberikan layanan prima melalui penerapan SMM ISO 9001:2015 kepada siswa, guru, pegawai, masyarakat dan sekolah aliansi.
2. Membentuk karakter siswa yang jujur, disiplin dan bertanggung jawab.
3. Menghasilkan tamatan yang profesional sebagai mekanik / tenaga kerja yang kompeten, wirausahawan yang sukses dan dapat melanjutkan ke perguruan tinggi.
4. Meningkatkan profesionalisme tenaga pendidik dan tenaga kependidikan.
5. Meningkatkan hubungan kemitraan dengan Stakeholder dalam rangka peningkatan mutu lulusan.
6. Meningkatkan sarana prasarana yang berwawasan lingkungan dengan mengacu kepada standar pelayanan prima.
7. Menciptakan lingkungan kerja yang kondusif dan harmonis.

### **2.1.2. Struktur Organisasi**

Struktur organisasi adalah suatu diagram yang menggambarkan rantai perintah, hubungan pekerjaan, tanggung jawab, rentang kendali dan pimpinan organisasi berfungsi sebagai kerangka kerja dan tugas pekerjaan yang dibagi, dikelompokkan dan dikoordinasi secara formal. Struktur organisasi menunjukkan alur perintah yang mengindikasikan jabatan pekerjaan yang harus dipertanggung jawabkan oleh masing-masing tipe karyawan[28], Gambar 2.2 merupakan Struktur Organisasi yang ada pada SMKN 8 Bandung ditunjukkan sebagai berikut.

**STRUKTUR ORGANISASI SMK NEGERI 8 BANDUNG**  
SEMESTER GENAP TAHUN PELAJARAN 2022/2023



Gambar 2. 2. Struktur Organisasi SMKN 8 Bandung

### **2.1.2. Deskripsi Kerja SMKN 8 Bandung**

Saat ini SMK Negeri 8 Bandung memiliki bidang kerja dan pegawai. Adapun pegawai mulai dari level Dunia Industri sampai ke siswa. Dan Berikut ini penjelasan mengenai fungsi pokok dari masing-masing bidang yang dideskripsikan sebagai berikut:

1. Dunia Industri

Dunia industri adalah mengacu pada hubungan dan kolaborasi antara sekolah dan dunia industri atau sektor bisnis. melibatkan kerja sama antara lembaga pendidikan dan perusahaan untuk meningkatkan pendidikan dan persiapan karir para siswa.

2. Kepala Sekolah

Kepala sekolah adalah individu yang bertanggung jawab atas pengelolaan dan pengawasan keseluruhan sekolah.

3. Komite Sekolah

Komite Sekolah adalah kelompok atau badan yang dibentuk di sekolah dengan tujuan untuk membantu dalam pengambilan keputusan, pengawasan, dan perencanaan program-program sekolah.

4. Pembina Gugus Depan

Pembina Gugus Depan adalah individu yang bertanggung jawab atas pembinaan dan pengawasan kelompok gugus dalam sistem penilaian dan pengembangan guru.

5. Kesiswaan

Kesiswaan mengacu pada aspek-aspek yang terkait dengan siswa dalam lingkungan sekolah. Dimulai dari membina siswa, aktivitas Ekstrakurikuler, Bimbingan Konselin, Pengembangan karakter dan nilai, Partisipasi orang tua.

6. Kurikulum

Kurikulum adalah seperangkat rencana pembelajaran yang merinci mata pelajaran, tujuan pembelajaran, metode pengajaran, dan penilaian yang akan digunakan dalam pendidikan formal di suatu lembaga pendidikan, seperti sekolah atau perguruan tinggi.

7. **Humas / Hubin**

Humas atau "Hubungan Masyarakat" atau Hubin (Hubungan Industri) adalah divisi yang bertanggung jawab atas pengelolaan dan komunikasi antara sekolah dengan masyarakat, orang tua siswa, dan pihak-pihak eksternal lainnya.

8. **Sarana Prasarana**

Sarana prasarana adalah fasilitas fisik atau infrastruktur yang digunakan dalam pendidikan, bisnis, atau kegiatan lainnya. Dalam konteks pendidikan, sarana prasarana mencakup berbagai fasilitas dan infrastruktur di sekolah atau perguruan tinggi yang mendukung proses pembelajaran dan kegiatan siswa.

9. **Korbid**

Koordinator bidang adalah seorang yang ditunjuk untuk bertanggung jawab menjalankan bidang yang berada dalam organisasi tersebut.

10. **Kepala Program**

Kepala Program adalah individu yang bertanggung jawab atas pengelolaan dan pengawasan program akademik di suatu institusi pendidikan.

11. **ICT**

ICT (Information and Communication Technology) adalah penggunaan teknologi informasi dan komunikasi dalam proses pembelajaran dan pengelolaan administrasi sekolah.

12. **Guru**

Guru adalah seorang pengajar suatu ilmu, guru bertugas untuk mendidik, mengajar, membimbing, mengarahkan, melatih, menilai dan mengevaluasi peserta didik.

## **2.2. Landasan Teori**

Berikut ini adalah beberapa landasan teori yang digunakan oleh peneliti sebagai pendukung teori dasar dari "Optimalisasi Load Balancing untuk Manajemen Bandwidth Openwrt Multi ISP dengan Sistem Konfigurasi di SMKN 8 Bandung".

### 2.2.1. *Optimalisasi*

Menurut Kamus Besar Bahasa Indonesia, optimalisasi berasal dari kata "optimal," yang merujuk pada yang terbaik, tertinggi, atau paling menguntungkan. Optimalisasi merujuk pada proses, tindakan, atau metodologi untuk meningkatkan sesuatu agar mencapai tingkat kesempurnaan, kinerja yang lebih baik, atau efektivitas yang lebih tinggi. Dengan kata lain, itu adalah upaya untuk meningkatkan performa dan efisiensi sistem atau proses yang telah dilakukan, sehingga mencapai potensi maksimal.

Optimalisasi dapat digunakan untuk mencapai hasil yang maksimal dengan biaya yang minimal. Dalam bidang Jaringan, Optimalisasi dapat digunakan untuk meningkatkan performa jaringan maupun efisiensi penggunaan jaringan.

### 2.2.2. *Load Balancing*

*Load Balancing* Adalah teknik untuk mendistribusikan beban trafik pada dua atau lebih jalur koneksi secara seimbang, agar trafik *bandwidth* dapat berjalan optimal, memaksimalkan *throughput*, Memperkecil waktu tanggap dan dapat menghindari *Overload* pada salah satu jalur koneksi [5].

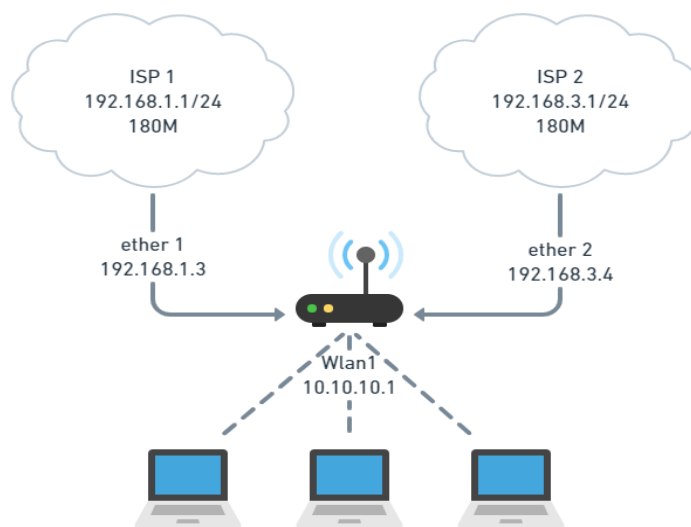
Load Balancing adalah teknik untuk menyeimbangkan beban lalu lintas pada dua atau lebih jalur koneksi sehingga bandwidth trafik dapat beroperasi secara optimal, meningkatkan throughput, mengurangi waktu respons, dan mencegah Overload pada jalur koneksi tertentu [5]. Dengan memiliki beberapa sumber daya internet, ini mengoptimalkan penggunaan sumber daya, throughput, dan waktu tanggap, terutama saat terjadi kegagalan jaringan, di mana beberapa jalur saling mendukung satu sama lain, dan juga mempercepat pemulihan ketika jaringan kembali normal. Ini sangat bermanfaat untuk memastikan tingkat koneksi yang sangat andal dengan uptime sekitar 99% dan menggunakan jalur upstream yang berbeda, yang dapat saling mendukung satu sama lain[11].

Pada dasarnya, *Net Balance* atau *Load balancer* mendistribusikan permintaan data yang bersalah dari LAN atau user dengan menggunakan metode tertentu ke beberapa *gateway* internet, Jika pada waktu tertentu ada satu pengguna LAN yang hanya membuat satu Koneksi TCP (misalnya ia melakukan satu

streaming dari Web), lalu lintas-nya akan melewati satu gateway dikarenakan koneksi yang dibuat belum mendukung multi koneksi, sehingga tidak mendapatkan manfaat dari Load Balancing ini.

Sebaliknya, Jika Koneksi dari LAN penuh dengan pengguna, maka setiap permintaan dari LAN menuju Wan diwaktu yang sama, secara keseluruhan, Koneksi mereka akan memiliki akses ke *Bandwidth* yang lebih tinggi, sama dengan jumlah *bandwidth* pada akses tunggal.

Dapat ditarik kesimpulan bahwa satu konektivitas ini tidak pernah memiliki lebih banyak *bandwidth* dari apa yang ditawarkan oleh satu konektivitas sedangkan beberapa koneksi simultan atau Multi koneksi, akan rata-rata, semuanya memiliki akses ke *bandwidth* yang lebih besar, yang akan melebarkan jalur pada jumlah *Bandwidth* internet semua link yang seimbang.



Gambar 2. 3. Load Balancing dengan Dua ISP

Dengan Konsep yang sederhana, sebuah *Load Balancing* yang diletakkan antara *client* dan ISP, seperti gambar 2.3, maka akan dapat menampung trafik yang datang dan membaginya ke dalam *request-request* per individual lalu menentukan server mana yang dapat menerima request tersebut, adapun beberapa keuntungan menggunakan *load balancing* antara lain:

- a. *High Availability* : *load balancing* akan secara terus menerus melakukan pemantauan terhadap ISP, jika terdapat ISP yang mati,

maka *load balancer* akan menghentikan *request* ke ISP dan mengalihkan ke ISP yang tersedia.

- b. *Scalability* : Ketika sistem mendapatkan beban yang meningkat, Kita dapat melakukan perubahan terhadap sistem agar dapat mengatasi beban sesuai kebutuhan.
- c. *Security* : Untuk semua koneksi yang melewati *loadbalancer*, aturan keamanan dapat diimplementasikan dengan mudah. Dengan Jaringan *private* digunakan dalam *server*, alamat IP address tidak dapat diakses secara langsung dari luar sistem dikarenakan ditahan oleh Security yang diterapkan.
- d. *Manageability* : Mudah di atur meskipun memiliki fisik sistem yang sangat besar.

Sebuah router mempunyai dua koneksi internet (sama atau memiliki ISP berbeda) *default gateway* di router tetap akan hanya bisa satu, jika ditambahkan pun yang bekerja tetap hanya satu gateway. Jadi misalnya *Router* terhubung ke ISP A melewati *interface 1* dan Gateway A, dan terhubung ke ISP B melewati *interface 2* dan *gateway B*, dan *default gateway* ke ISP A, maka Konektivitas *downlink* hanya akan datang dari ISP A saja, begitu juga sebaliknya jika dipasang *default gateway* ke ISP B. Penerapan teknik *load balancing* dapat menyelesaikan permasalahan tersebut dengan menggabungkan *traffic* ISP A dan ISP B, sehingga dapat diimplementasikan secara bersamaan.

Prinsip Kerja load balancing sebagai berikut:

- a. Lalu lintas koneksi yang terdistribusi berdasarkan probabilitas.
- b. Harus mengetahui seberapa besar tiap link yang dapat dilewatkan dan dilewatkan sesuai lalu lintas.
- c. Berdasarkan kecepatan pada keluaran dan masukan pada router, *load balance* dapat digambarkan sebagai berikut.

$$1 + 1 = 1 + 1$$

$$1 + 1 = \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \frac{1}{2}$$



$$1 + 1 = \frac{1}{4} + \frac{1}{4} + \frac{1}{4} + \frac{1}{4} + \frac{1}{4} + \frac{1}{4} + \frac{1}{4} + \frac{1}{4}$$

- d. Jika memiliki dua *gateway*, misalnya ISP A dan ISP B, A memiliki *bandwidth* 2 Mbps dan B memiliki *bandwidth* sebesar 3 Mbps. Maka lalu lintas yang akan dibagi ke dalam aliran dan mengirim 2 aliran ke ISP A dan 3 aliran ke ISP B.

Selama ini banyak berpikir bahwa dengan diterapkan *load balancing* dua jalur koneksi, maka kapasitas *bandwidth* yang didapatkan menjadi dua kali lipat besar dari *bandwidth* sebelum menggunakan *load balancing* (perhitungan dari total kedua *bandwidth*). Pada dasarnya *load balancing* tidak menambah besaran *bandwidth* yang diperoleh, tetapi bertugas membagi trafik dari kedua *bandwidth* agar dapat terkoneksi dan terpakai secara seimbang.

Ada berbagai metode *load balancing* yang dapat digunakan antara lain static route dengan address list, *Equal Cost MultiPath* (ECMP), *nth* dan *Per Connection Classifier* (PCC). Setiap metode *load balancing* memiliki kekurangan dan kelebihan tersendiri, namun lebih dari hal itu, hal yang paling penting dalam menentukan metode *load balancing* yang akan digunakan adalah harus terlebih dahulu karakteristik dari jaringan yang akan diimplementasikan. Dalam hal ini penelitian yang akan digunakan menggunakan *Mwan3* yang dimana sudah terdapat Metode *Load Balancing* dan *failover*.

#### 2.2.2.1. 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 *Load balancing* secara berdasarkan *interface* yang disetting.

*Mwan3* Menggunakan metode *Linux Policy routing* untuk menseimbangkan koneksi yang keluar dari *Multi Wan* tersebut, *Mwan* sendiri menggunakan *Load balancing Per-IP Connection basic*, yang dimana akan

menandai *packet* yang menuju *gateway* tertentu, dan ketika *packet* kembali akan melalui *gateway* yang dilewati (Mwan3 docs, 2022)

#### A. Cara Kerja Mwan3

Setiap *packet* data yang masuk (termasuk trafik yang berasal dari router) akan ditangani oleh iptables “mwan3\_hook”. Hook ini membutuhkan 5 langkah yaitu:

1. Menandai kembali tanda mark jika sebelumnya telah ditetapkan, jika berhasil ditandai *packet* tersebut, lanjut ke langkah 5.
2. Periksa apakah *packet* tiba di *gateway* mana, Jika berasal dari jaringan LAN yang terhubung, tandai *packet* dengan “iface\_id default”. Jika *packet* berasal dari jaringan lain (non-lokal) dan WAN, maka tandai dengan mark “iface\_id”. Jika berhasil ditandai pindah ke langkah 5.
3. Periksa apakah *packet* yang ditujukan untuk jaringan ip yang dikenal (non-default). Jika iya, *packet* tersebut akan ditandai dengan “iface\_id default” dan lanjut ke langkah 5.
4. Memeriksa apakah alamat sumber *packet* apakah alamat WAN atau bukan, jika benar gunakan Wan tersebut untuk routing tanpa mengikuti aturan yang dibuat oleh user dan *packet* tersebut ditandai mark “iface\_id” dari wan asalnya.
5. Terapkan aturan user dan tandai dengan mark “iface\_id” yang telah dikonfigurasi. Jika tidak ada yang cocok tidak ditandai.

#### B. Arsitektur Mwan3

1. Mwan3 bekerja berdasarkan “hotplug-event”, ketika *interface UP* atau muncul, maka Mwan3 akan membuat kustom *Routing table* dan *iptables 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.

2. Kemudian semua rute dan aturan yang sudah diatur, disini mwan3 akan berhenti bekerja dan Kernel (Router) yang akan menangani semua keputusan perutean. Jika terjadi peristiwa hotplug atau penambahan *interface* baru, maka Mwan3 akan bekerja kembali untuk menyesuaikan rute dan tabel sesuai kebutuhan.
3. Untuk memonitoring Jaringan *load balancing*, Mwan3 memiliki Mwan3track yang berjalan dilatar belakang untuk memeriksa apakah setiap *interface* WAN aktif menggunakan test konektivitas (Ping). Jika WAN tersebut mati, skrip Mwan3 akan menyesuaikan tabel perutean *Interface* yang mati.
4. Setiap perubahan tabel perutean secara konstan dipantau oleh mwan3rtmon yang dimana bertanggung jawab untuk menjaga tabel perutean utama tetap sinkron dengan tabel perutean *interface*.

### 2.2.3. Failover

Penerapan Load Balancing sangat rentang dengan putusnya salah satu jalur internet. Jika hal ini terjadi, sistem *load balancing* akan terganggu dan tidak akan berjalan dengan baik, dikarenakan beberapa *client* akan mendapatkan *connectionless* atau *packet* yang tidak sampai pada tujuan. Untuk menangani hal itu teknik *failover* merupakan solusi yang tepat.

*Failover* adalah kemampuan untuk beralih secara otomatis ke gateway lainnya yang masih aktif, *gateway* yang masih aktif akan mengambil alih tugas dari *gateway* yang mengalami putus koneksi, adapun teknik failover sudah termasuk ke dalam package Load Balancing Mwan3 (Mwan3 docs, 2022).

### 2.2.4. Bandwidth

Bandwidth adalah sejumlah besar data atau informasi yang dapat dipindahkan dari satu lokasi ke lokasi lain dalam jaringan pada waktu tertentu [12]. Manajemen bandwidth adalah alat yang digunakan untuk mengelola dan meningkatkan berbagai jenis koneksi jaringan dengan menerapkan layanan Quality of Service (QoS) untuk mengatur tipe lalu lintas jaringan[16].

### 2.2.4.1. Manajemen Bandwidth

*Bandwidth Management System* adalah suatu metode yang diterapkan untuk mengatur besarnya *bandwidth* yang akan digunakan oleh tiap user di sebuah jaringan, sehingga penggunaan *bandwidth* akan terdistribusi secara merata, Pengalokasian *bandwidth* yang tepat atau sesuai menjadi salah satu metode dalam memberikan jaminan kualitas suatu layanan internet [16]. Adapun Manajemen *Bandwidth* yang dapat digunakan dalam sistem OpenWrt sebagai berikut.

#### A. SQM

Smart Queue Management (SQM) adalah sebuah *Script* pada openwrt dengan teknik manajemen antrian yang cerdas dan adaptif yang digunakan untuk mengatur lalu lintas jaringan dengan cara mengendalikan dan mengatur penundaan (*latency*) pada jaringan [19]. SQM dapat meminimalkan dan mengelola bottleneck serta konflik lalu lintas yang terjadi dalam jaringan. Analisis ini memberikan pemahaman lebih dalam tentang penggunaan SQM dalam mengoptimalkan performa jaringan:

Konsep Dasar SQM:

1. SQM bekerja dengan menerapkan algoritma kontrol untuk mengatur laju pengiriman dan penerimaan *packet* dalam jaringan.
2. Tujuan utama SQM adalah untuk mengelola antrian *packet* dengan cara mengendalikan penundaan (*latency*) dan menjaga ketersediaan *bandwidth* secara adil bagi semua pengguna.
3. SQM mengidentifikasi dan mengurangi jenis-jenis penundaan yang umum terjadi, seperti penundaan yang disebabkan oleh antrian (*queuing delay*), penundaan akibat tumpang tindih *packet* (*packet interleaving delay*), dan penundaan yang disebabkan oleh buffer (*buffer delay*).

Tipe-tipe *Queueing Discipline* dalam SQM:

- a. FQ\_CODEL (Fair Queue Controlled Delay):

1. FQ\_CODEL merupakan tipe queueing discipline yang mengutamakan keadilan dan mengendalikan penundaan secara efisien.
  2. FQ\_CODEL mengelompokkan *packet* berdasarkan aliran (flow) dan memberikan penundaan yang proporsional terhadap setiap aliran.
  3. Dengan menggunakan algoritma CODEL (Controlled Delay), FQ\_CODEL dapat mengurangi dan mengelola penundaan secara optimal.
- b. Cake (Common Applications Kept Enhanced):
1. Cake adalah tipe queueing discipline yang dirancang untuk mengoptimalkan lalu lintas jaringan dalam berbagai situasi dan kebutuhan aplikasi.
  2. Cake mengatur antrian berdasarkan beberapa faktor, seperti prioritas (priority), bandwidth, *latency*, dan fairness.
  3. Dengan menggunakan teknik manajemen antrian yang adaptif, Cake dapat menghindari penundaan yang tidak perlu dan meningkatkan performa jaringan secara keseluruhan.

Tipe-tipe Queue setup script dalam SQM:

- a. `layer_cake.qos`:
  1. Menggunakan `qdisc cake` sebagai pengganti `htb` sebagai shaper dan `fq_codel` sebagai leaf `qdisc`.
  2. Menggunakan profil `diffserv cake` sebagai "layer" prioritas yang berbeda.
  3. Membutuhkan `cake` sebagai `qdisc` yang dipilih dan memaksa penggunaannya.
- b. `piece_of_cake.qos`:
  1. Menggunakan `qdisc cake` sebagai pengganti `htb` sebagai shaper dan `fq_codel` sebagai leaf `qdisc`.

2. Konfigurasi yang sangat sederhana dan mudah, seperti namanya yang merupakan "piece of cake".
  3. Membutuhkan cake sebagai qdisc yang dipilih dan memaksa penggunaannya.
- c. simple.qos:
1. Skema prioritas tiga tingkat dengan pembatasan bandwidth menggunakan qdisc pada setiap antrian.
  2. Konfigurasi default.
- d. simplest.qos:
1. Konfigurasi yang paling sederhana: pembatasan bandwidth menggunakan HTB rate limiter dengan qdisc terpasang.
- e. simplest\_tbf.qos:
1. Konfigurasi yang paling sederhana (TBF): pembatasan bandwidth menggunakan TBF rate limiter dengan qdisc terpasang.
  2. Pada beberapa arsitektur, TBF dapat memberikan performa yang lebih baik dibandingkan dengan HTB.

## B. QoS Over Nftables

QoS over nftables adalah teknik manajemen lalu lintas jaringan yang digunakan untuk mengatur dan mengendalikan prioritas pengiriman *packet* dalam jaringan. Ini dilakukan dengan menggunakan nftables, sebuah framework firewall yang fleksibel dan kuat di sistem operasi Linux. Berikut ini adalah analisis lengkap tentang QoS over nftables:

Konsep Dasar QoS over nftables:

1. QoS over nftables bertujuan untuk memberikan prioritas yang sesuai kepada jenis lalu lintas yang berbeda dalam jaringan.
2. Prioritas diberikan berdasarkan aturan-aturan yang ditentukan, yang melibatkan identifikasi *packet* berdasarkan parameter tertentu seperti alamat sumber, alamat tujuan, port, atau jenis protokol.

3. Dengan memberikan prioritas, QoS over nftables dapat mengoptimalkan penggunaan bandwidth dan mengatur lalu lintas jaringan sesuai dengan kebutuhan dan kebijakan yang ditetapkan.

Mekanisme QoS over nftables:

1. Klasifikasi (Classification): *Packet-packet* dalam lalu lintas jaringan diklasifikasikan berdasarkan atribut-atribut tertentu seperti alamat sumber, alamat tujuan, atau jenis protokol.
2. Penandaan (Marking): Setelah diklasifikasikan, *packet-packet* diberi tanda (mark) untuk menunjukkan prioritas yang harus diberikan.
3. Pengaturan (Policing/Shaping): Setelah tanda diberikan, aturan QoS diterapkan untuk mengendalikan laju pengiriman *packet* (policing) atau mengatur laju pengiriman *packet* (shaping) sesuai dengan prioritas yang ditentukan.

### 2.2.5. 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*. Dan Openwrt juga didukung dengan kernel linux yang lebih baru daripada kebanyakan distribusi lainnya, Openwrt juga disediakan secara gratis melalui lisensi *General Public License (GPL)*, yang dimana banyak kontributor sukarela membantu mengembangkan openwrt dan openwrt juga tidak dikenakan biaya langganan atau lisensi [22]

Openwrt juga menyediakan *filesystem* yang dapat ditulis dengan sesuka hati pengguna, dimana pengguna dibebaskan dari batasan pemilihan fitur dan konfigurasi yang disediakan vendor atau memungkinkan pengguna menyesuaikan fitur yang digunakan agar sesuai dengan aplikasi yang digunakan.

### 2.2.5.1. Perangkat yang didukung OpenWrt

OpenWrt Dapat Diinstall pada berbagai jenis perangkat jaringan, seperti router, access point, switch, dan embedded device lainnya, adapun beberapa produsen yang didukung oleh OpenWrt antara lain: asus, Tp-link, Linksys, D-Link, Netgear, Ubiquiti, Raspberry Pi, reyee. Selain itu Openwrt juga mendukung banyak perangkat jaringan yang dirancang secara khusus untuk embedded system, seperti: ARM, MIPS64, MIPS, PPC, x86, x86\_64 [22].

### 2.2.5.2. Fitur-fitur Openwrt

Secara bawaan Openwrt hanya memiliki beberapa fitur yang diinstall, fitur yang diinstall secara default antara lain sebagai berikut:

- |                                   |                                |
|-----------------------------------|--------------------------------|
| a. Firewall dan NAT               | g. Network                     |
| b. Routing                        | h. Management Software         |
| c. <i>Policy by Routing</i> (PBR) | i. IP sets                     |
| d. VPN Client                     | j. <i>Monitoring Interface</i> |
| e. NTP Server                     | k. Diagnostics                 |

### 2.2.6. PC Router

Dari pengertian *Router* yang disampaikan sebelumnya dapat dikatakan bahwa *PC Router* adalah perangkat pengatur jaringan lalu lintas data antar segmen jaringan yang memanfaatkan *Personal Computer* sebagai perangkat atau *device*. Dengan kata lain *PC Router* adalah PC yang dimodifikasi sedemikian rupa sehingga memiliki fungsi sebagai sebuah *Router* yang mengatur lalu lintas data. Dengan penggunaan PC sebagai *Router* jaringan, maka kita dapat memanfaatkan PC yang tidak terpakai untuk dijadikan sebuah *Router* sehingga dapat menekan biaya, dibandingkan dengan pembelian *dedicated router* yang digunakan sebagai router, selain harganya yang relatif mahal, *maintenance* terhadap jenis router ini cukup sulit.



### **2.2.7. Internet Service Provider (ISP)**

*Internet Service Provider (ISP)* merupakan perusahaan atau badan usaha yang menjual koneksi internet atau sejenisnya kepada pelanggan. ISP identik dengan jaringan telepon karena ISP menjual koneksi atau *access* internet melalui jaringan telepon. Seperti salah satunya adalah Biznet, Perkembangan ISP tidak hanya dengan menggunakan jaringan telepon tetapi dapat menggunakan teknologi lain seperti Media *Fiber optic*, *Wireless*, ISP juga mempunyai jaringan secara domestic maupun internasional sehingga pelanggan dapat terhubung ke jaringan internet global [9].

#### **2.2.7.1. Multi ISP**

Multi ISP pada ISP (*Internet Service Provider*) mengacu pada penggunaan beberapa koneksi internet dari beberapa penyedia layanan internet (ISP) untuk memperluas ketersediaan layanan internet dan meningkatkan keandalan dan kecepatan jaringan. Untuk mengimplementasikan Multi ISP, Dapat menggunakan Teknologi *Load Balancing* untuk membagi lalu lintas jaringan secara merata ke setiap koneksi yang tersedia, adapun keunggulan Multi ISP dari single ISP yaitu:

1. Meningkatkan ketersediaan dan kecepatan layanan internet bagi pelanggan
2. Menjaga kestabilan dan kinerja jaringan pada saat salah satu ISP mengalami gangguan atau downtime

### **2.2.8. Arsitektur Protocol TCP/IP**

Arsitektur Protokol TCP/IP merupakan sebuah hasil penelitian dan pengembangan protokol yang dilaksanakan pada jaringan jaringan, ARPANET yang dibiayai oleh DARA (*defense Advanced Research Project Agency*) dan umumnya ditunjuk sebagai *packet* protokol yang telah diterbitkan sebagai standar Internet dan IAB (*Internet Architecture Board*) [24]. Model TCP/IP memiliki empat lapisan (*layer*) yang membantu dalam pengiriman data yang terstruktur dan terstandarisasi. Keempat lapisan tersebut adalah:

1. Lapisan Akses Jaringan (Data Link Layer): Lapisan ini bertanggung jawab atas pengiriman data di dalam satu jaringan fisik. Protokol yang terkait dengan lapisan ini adalah Ethernet, Wi-Fi, dan lainnya.
2. Lapisan Antar Jaringan (Network Layer): Lapisan ini mengatur pengiriman data antara jaringan yang berbeda. Protokol yang terkait dengan lapisan ini adalah Internet Protocol (IP), yang memberikan alamat IP kepada setiap perangkat dalam jaringan.
3. Lapisan Antar Host ke Host (Transport Layer): Lapisan ini memastikan pengiriman data yang andal antara host sumber dan host tujuan. Protokol yang terkait dengan lapisan ini adalah Transmission Control Protocol (TCP) yang memastikan pengiriman data yang handal dan User Datagram Protocol (UDP) yang menyediakan pengiriman data tanpa koneksi.
4. Lapisan Aplikasi (Application Layer): Lapisan ini berhubungan dengan aplikasi yang digunakan oleh pengguna akhir. Protokol yang terkait dengan lapisan ini meliputi Hypertext Transfer Protocol (HTTP) untuk akses web, Simple Mail Transfer Protocol (SMTP) untuk pengiriman email, dan protokol lainnya.

Pengalamatan IP address adalah sistem yang digunakan dalam arsitektur TCP/IP untuk memberikan alamat logis kepada setiap perangkat dalam jaringan. IP address digunakan untuk mengidentifikasi perangkat secara unik dalam jaringan dan memungkinkan pengiriman data antara perangkat-perangkat tersebut[31]. Dalam pengalamatan IP address IPv4, terdapat konsep kelas yang digunakan untuk mengorganisir dan mengelompokkan alamat IP ke dalam rentang yang lebih besar. Pada awalnya, sistem kelas digunakan dalam IPv4 untuk menentukan bagian dari alamat IP yang digunakan untuk identifikasi jaringan (Network ID) dan bagian yang digunakan untuk mengidentifikasi perangkat dalam jaringan (Host ID) [21, 31]. Terdapat tiga kelas utama dalam sistem kelas IPv4:

1. Kelas A: Kelas A mencakup rentang alamat IP yang dimulai dari 1.0.0.0 hingga 126.0.0.0. Kelas A memiliki 8 bit untuk identifikasi jaringan dan 24 bit untuk identifikasi perangkat dalam jaringan. Kelas A umumnya digunakan oleh organisasi besar atau ISP (Internet Service Provider) karena dapat menampung jumlah perangkat yang sangat besar.
2. Kelas B: Kelas B mencakup tentang alamat IP yang dimulai dari 128.0.0.0 hingga 191.0.0.0. Kelas B memiliki 16 bit untuk identifikasi jaringan dan 16 bit untuk identifikasi perangkat dalam jaringan. Kelas B digunakan oleh organisasi menengah yang memerlukan jumlah perangkat yang sedang.
3. Kelas C: Kelas C mencakup tentang alamat IP yang dimulai dari 192.0.0.0 hingga 223.0.0.0. Kelas C memiliki 24 bit untuk identifikasi jaringan dan 8 bit untuk identifikasi perangkat dalam jaringan. Kelas C umumnya digunakan oleh organisasi kecil karena memiliki jumlah perangkat yang terbatas.

Selain ketiga kelas utama di atas, terdapat juga kelas khusus seperti Kelas D (224.0.0.0 hingga 239.255.255.255) yang digunakan untuk multicast, dan Kelas E (240.0.0.0 hingga 255.255.255.255) yang digunakan untuk penggunaan khusus.

### **2.2.9. NAT (Network Address Translator)**

*Network address Translation* atau biasa disebut NAT adalah suatu metode untuk menghubungkan lebih dari satu komputer ke jaringan internet dengan menggunakan satu alamat IP address yang terbatas. Banyak yang menggunakan metode ini disebabkan karena ketersediaan alamat IP yang terbatas, kebutuhan akan keamanan juga, serta fleksibilitas dalam administrasi jaringan.

Dikarenakan keterbatasan inilah ISP (*Internet Service Provider*) yang hanya akan memberikan satu alamat IP untuk satu pengguna dan alamat ini bersifat dinamik atau *dynamic*, yang artinya alamat IP yang diberikan akan berbeda setiap kali user melakukan koneksi ke internet. Dengan NAT *gateway* yang dijalankan di salah satu Router, Satu alamat IP tersebut dapat dibagikan ke

beberapa komputer lain dan dapat melakukan koneksi internet secara bersamaan. Adapun beberapa jenis NAT, yaitu :

#### **2.2.9.1.Static NAT**

Static NAT adalah teknik NAT dimana sebuah alamat IP dan Port External ditetapkan secara manual dan tetap untuk suatu alamat IP internal pada suatu jaringan. Dengan menggunakan Static NAT, lalu lintas jaringan publik dapat diarahkan ke alamat IP internal tertentu, sehingga membuat host yang terhubung dapat diakses dari internet dengan menggunakan alamat IP Publik yang diberikan. Static NAT sering digunakan untuk layanan Public seperti Web Server, Email Server atau Server Game yang terhubung ke jaringan internal, sehingga dapat diakses pengguna diluar jaringan.

#### **2.2.9.2.Dynamic NAT**

Dinamic NAT adalah teknik NAT dimana sebuah alamat IP dan Port diberikan secara dinamis oleh server NAT ketika koneksi pertama kali dibuat. Dalam dinamic NAT, alamat IP publik dapat dipakai secara bergantian oleh koneksi yang berbeda pada waktu yang sama, tergantung dengan ketersediaan IP publik di server NAT. dynamic NAT biasanya digunakan pada jaringan dengan banyak user yang membutuhkan akses ke internet, karena teknik ini memungkinkan beberapa host untuk menggunakan satu alamat IP public yang sama.

#### **2.2.9.3.Masquerading NAT**

Masquerading NAT ini menerjemahkan semua IP address yang tidak terdaftar pada jaringan lokal yang dapat dipetakan kepada satu IP address terdaftar dan port. Agar banyak *client* bisa mengakses internet secara bersamaan *router*, NAT menggunakan nomor *port* untuk membedakan antara *packet-packet* yang dihasilkan oleh atau diarahkan ke komputer-komputer yang berbeda.

#### **2.2.10. Jaringan Komputer**

Jaringan komputer adalah kumpulan perangkat keras dan perangkat lunak yang terhubung satu sama lain untuk berbagi data, sumber daya, dan informasi.

Ini memungkinkan komunikasi antara komputer dan perangkat lainnya[29], baik dalam jarak yang sangat dekat (seperti di dalam satu gedung) maupun di seluruh dunia melalui internet. Berikut adalah beberapa komponen utama dan konsep dalam jaringan komputer:

1. **Node (Node):** Node adalah perangkat dalam jaringan, seperti komputer, server, printer, router, atau perangkat lainnya yang terhubung ke jaringan. Setiap node memiliki alamat unik yang disebut alamat MAC (Media Access Control) atau alamat IP (Internet Protocol) untuk mengidentifikasinya dalam jaringan.
2. **Perangkat Keras (Hardware):** Ini mencakup perangkat keras fisik seperti komputer, kabel jaringan, router, switch, hub, dan perangkat keras lain yang digunakan untuk menghubungkan dan mentransfer data antara node dalam jaringan.
3. **Perangkat Lunak (Software):** Perangkat lunak jaringan termasuk sistem operasi jaringan, protokol komunikasi, dan aplikasi yang memungkinkan komunikasi dan berbagi sumber daya antara node dalam jaringan.
4. **Media Transmisi:** Ini adalah media fisik atau nirkabel yang digunakan untuk mengirim data antara node dalam jaringan. Contohnya termasuk kabel tembaga (seperti Ethernet), serat optik, dan gelombang radio.
5. **Topologi Jaringan:** Topologi jaringan menggambarkan cara node dalam jaringan diatur dan terhubung satu sama lain. Beberapa topologi jaringan umum termasuk topologi bintang, topologi lingkaran (ring), topologi mesh, topologi pohon, dan topologi bus.
6. **Protokol Jaringan:** Protokol adalah aturan dan standar komunikasi yang digunakan dalam jaringan. Ini mencakup protokol TCP/IP yang digunakan di internet, serta banyak protokol lainnya seperti HTTP untuk World Wide Web, FTP untuk File Transfer Protocol, dan SMTP untuk Simple Mail Transfer Protocol.

7. **Internet:** Internet adalah jaringan global terbesar yang menghubungkan jutaan jaringan komputer di seluruh dunia. Ini memungkinkan komunikasi dan akses ke berbagai sumber daya dan informasi.
8. **Aplikasi Jaringan:** Aplikasi jaringan adalah perangkat lunak yang memungkinkan pengguna untuk berkomunikasi dan berbagi data melalui jaringan. Ini termasuk email, web browsing, pesan instan, dan banyak lagi.

### 2.2.11. Firewall

*Firewall* adalah sistem yang digunakan untuk menjalankan kontrol akses pada sebuah jaringan internal terhadap jaringan untrusted seperti internet. Umumnya sebuah *firewall* diimplementasikan dalam sebuah *router* yang berjalan pada gateway antara jaringan lokal dan jaringan lainnya.

Firewall pada umumnya juga digunakan untuk mengontrol akses terhadap akses jaringan luar ataupun jaringan dalam. Fungsi-fungsi umum dari *firewall* sebagai berikut:

- a. Melindungi jaringan dari serangan dan ancaman yang tidak diinginkan.
- b. Memantau dan mengatur lalu lintas data yang masuk dan keluar jaringan.
- c. Menolak akses dari pengguna atau program tertentu.
- d. Mengatur kebijakan keamanan dan hak akses pengguna.
- e. Membatasi akses Internet kepada pengguna.

#### 2.2.11.1. OpenWrt sebagai firewall

OpenWrt Selain dapat digunakan sebagai gateway Internet, OpenWrt juga dapat berfungsi sebagai *firewall* bagi komputer lain dan memberikan prioritas bagi komputer lain agar bisa mengakses data internet maupun data lokal [23].

Dalam fitur *firewall Openwrt* terdapat direktori, yaitu

- a. General Settings, untuk konfigurasi awal jika tidak ada konfigurasi yang ditetapkan pada Zones.
- b. Routing/Nat Offloading, untuk meningkatkan performa router dengan memindahkan beban pengolahan data dari CPU ke Hardware khusus yang mendukung *Hardware* akselerasi.

- c. Zones, Mengatur dan memisahkan lalu lintas jaringan antar dua atau lebih jaringan yang berbeda, setiap Zones mewakili jaringan yang berbeda seperti LAN, WAN, DMZ.
- d. Port Forwards, Untuk mengatur dan mengarahkan lalu lintas jaringan dari port tertentu pada router menuju perangkat di jaringan lokal.
- e. Traffic Rules, merupakan aturan untuk mengontrol lalu lintas jaringan yang masuk dan keluar dari router, aturan ini digunakan untuk membatasi akses ke jaringan dan perangkat di dalamnya.
- f. Ip Sets, untuk mengelompokkan alamat ip atau jangkauan alamat ip dalam satu set dan menggunakannya dalam aturan firewall.

#### 2.2.11.2.Nftables

nftables menggantikan {ip,ip6,arp,eb}tables yang populer. nftables ini menyediakan framework klasifikasi *packet* di dalam kernel yang didasarkan pada *Virtual Machine* (VM) yang khusus untuk jaringan dan baris perintah pengguna nft yang baru. nftables menggunakan kembali subsistem Netfilter yang sudah ada, seperti infrastruktur hook yang sudah ada, sistem pelacakan koneksi, NAT, penggunaan queueing, dan subsistem pencatatan [netfilter, 2023].

#### 2.2.12. Quality of Service (QoS)

*Quality of service* merupakan sebuah layanan untuk menjamin performa dan merupakan parameter untuk mengukur kualitas dari sebuah layanan. Parameter QoS mengacu pada performa tingkat kecepatan dan kehandalan penyampaian berbagai jenis data dalam komunikasi[28]. Parameter QoS sebagai berikut:

- a. Delay

Delay atau *latency* adalah waktu tunda suatu *packet* yang dikirimkan diakibatkan oleh proses transmisi dari satu titik menuju titik lain yang menjadi tujuannya. Delay dapat dipengaruhi oleh jarak, Media fisik, Kongesti atau waktu proses yang lama.

Tabel 2. 1. Standar Delay TIPHON

Kategori Latensi	Besar Delay	Indeks
Sangat Bagus	< 150 ms	4
Bagus	150 s/d 300 ms	3
Sedang	300 s/d 450 ms	2
Jelek	> 450 ms	1

(TIPHON, 1999)

b. Packet Loss

*Packet Loss* merupakan banyaknya *packet* yang hilang atau gagal dikirim pada suatu jaringan yang disebabkan oleh tabrakan (*collision*) dan *congestion*. Pada jaringan, hal ini berpengaruh pada semua aplikasi karena retransmisi akan mengurangi efisiensi jaringan secara keseluruhan meskipun jumlah bandwidth cukup untuk aplikasi tersebut. Di dalam implementasi jaringan IP, diharapkan Nilai *packet loss* ini mempunyai nilai yang minimum. Secara umum terdapat empat kategori penurunan performa jaringan berdasarkan nilai *packet loss* sesuai dengan standar TIPHON, sebagai berikut:

Tabel 2. 2. Standar Packet LOSS TIPHON

Kategori Degradasi	Packet LOSS	Indeks
Sangat Bagus	$X \leq 3 \%$	4
Bagus	$X \leq 15 \%$	3
Sedang	$X \leq 25 \%$	2
Jelek	$X \geq 25 \%$	1

(TIPHON, 1999)

c. Jitter

*Jitter* atau variasi kedatangan *packet* yang diakibatkan oleh variasi – variasi dalam panjang antrian, dalam waktu pengolahan data dan dalam waktu



penghimpunan ulang paket-paket di akhir perjalanan jitter. Jitter biasanya disebut variasi delay pada transmisi data di jaringan. Delay antrian pada router dan switch dapat menyebabkan jitter.

Besaran nilai jitter akan sangat dipengaruhi oleh variasi beban trafik dan besarnya tumpukan antara *packet* yang berada dalam jaringan. Semakin besar beban trafik dalam jaringan maka akan menyebabkan semakin besar juga peluang terjadinya *congestion* dengan demikian nilai *jitter* akan semakin besar, semakin besar nilai jitter maka semakin kecil nilai QoS,

Adapun empat kategori penurunan performa jaringan berdasarkan nilai *peak jitter* sesuai dengan standar TIPHON.

Tabel 2. 3. Standar Jitter TIPHON

Kategori Latensi	Peak Jitter	Indeks
Sangat Bagus	0 ms	4
Bagus	1 s/d 75 ms	3
Sedang	76 s/d 125 ms	2
Jelek	126 s/d 225 ms	1

(TIPHON, 1999)

Rumus yang digunakan untuk menghitung jitter:

$$Jitter = \frac{\text{Total variasi delay}}{\text{Total paket diterima}-1}$$

Total variasi delay diperoleh dari penjumlahan:

$$(\text{Delay 2} - \text{delay 1}) + (\text{delay 3} - \text{delay 2}) + \dots + (\text{delay n} - \text{delay}(n-1))$$

d. Throughput

Throughput, yaitu kecepatan (*rate*) transfer data efektif yang diukur dalam bps. Throughput merupakan jumlah total kedatangan *packet* yang berhasil dan

dilihat pada destinasi selama interval waktu tertentu dibagi oleh durasi interval waktu tersebut.

Secara umum terdapat lima kategori penurunan performasi jaringan berdasarkan nilai *Throughput* sesuai dengan standar TIPHON, yaitu sebagai berikut:

Tabel 2. 4. Standar *Throughput* TIPHON

Kategori	Throughput	Indeks
Terbagus	> 2.1 Mbps	4
Sangat Bagus	1200 kbps- 2.1 Mbps	3
Bagus	700-1200 kbps	2
Sedang	338-700 kbps	1
Jelek	0-338 kbps	0

(TIPHON, 1999)

Acuan Konversi satuan

1 Byte = 8 bit (ISO/IEC 2382-1:1993)

Rumus yang digunakan untuk mencari *Throughput* adalah:

$$\text{Throughput} = \frac{\text{Jumlah Bit yang dikirimkan}}{\text{Total Waktu pengiriman}}$$

### 2.2.13. Sistem Konfigurasi

Sistem Konfigurasi adalah suatu proses pengaturan dan penyesuaian perangkat lunak atau perangkat keras sehingga dapat beroperasi dengan kebutuhan dan preferensi pengguna. Sistem Konfigurasi seringkali dilakukan pada Sistem Operasi, Aplikasi, atau perangkat jaringan seperti Router atau switch.

Sistem konfigurasi dapat dilakukan melalui berbagai cara, seperti melalui antarmuka grafis (GUI) atau melalui antarmuka baris perintah (CLI). Proses konfigurasi sistem yang efektif dan efisien memerlukan pemahaman yang baik

tentang sistem yang akan dikonfigurasi serta penggunaan perintah-perintah atau tools yang tepat untuk melakukan konfigurasi yang diperlukan.

Pada Umumnya Sistem konfigurasi dilakukan dengan cara melakukan perubahan atau modifikasi beberapa pengaturan yang terdapat dalam konfigurasi suatu sistem, beberapa hal yang dapat dikonfigurasi dalam sebuah sistem antara lain:

1. Jaringan: Pengaturan alamat IP, subnet mask, gateway, DNS, DHCP, vlan, dan lainnya
2. Keamanan: pengaturan firewall, VPN, SSL, Akses control (ACL)
3. Server: pengaturan *web server*, mail server, database server, dan lainnya
4. Sistem operasi: pengaturan kernel, driver, pengguna, grub, hak akses, dan lain-lain.
5. Aplikasi: pengaturan database, file konfigurasi, plugin, dan lain-lain.

#### **2.2.14. Monitoring Jaringan**

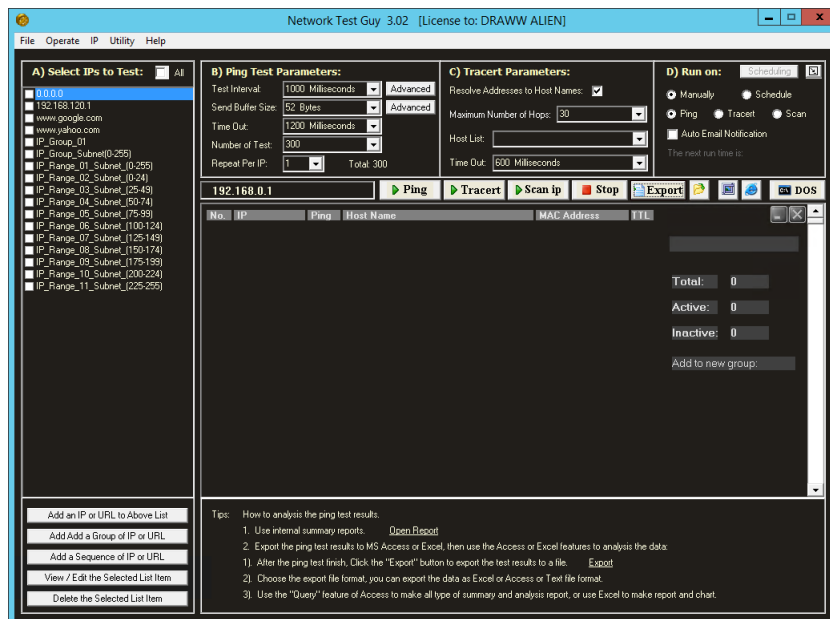
Monitoring Jaringan merupakan sebuah fungsi dari management yang berguna untuk menganalisa apakah suatu jaringan masih cukup layak untuk digunakan atau perlu menambahkan kapasitas atau perbaikan. Hasil monitoring juga dapat membantu jika admin ingin mendesain ulang jaringan yang telah ada. Untuk melakukan *monitoring*, sudah banyak tools yang tersebar luas di internet untuk melakukan *monitoring* secara gratis. Salah satu diantaranya yang dapat di monitoring adalah *Cpu usage* pada sebuah router. Monitoring dapat dilakukan dengan SNMP, collectd. Selain itu kondisi jaringan pun harus dimonitoring, misalnya status perangkat.

Dimana Monitoring Jaringan akan terdapat Akses Log, Akses log pada pemantauan jaringan adalah proses memeriksa dan menganalisis catatan aktivitas jaringan yang telah terjadi. Log jaringan berisi informasi penting tentang apa yang terjadi dalam jaringan, seperti koneksi yang dibuat, akses pengguna, aktivitas perangkat, dan lebih banyak lagi[33]. Akses log jaringan penting untuk:

1. **Keamanan Jaringan:** Log jaringan membantu mengidentifikasi aktivitas mencurigakan atau serangan yang mungkin terjadi pada jaringan. Ini memungkinkan tim keamanan untuk mengambil tindakan yang tepat untuk melindungi jaringan.
2. **Pemecahan Masalah:** Ketika terjadi masalah jaringan, log dapat membantu dalam pemecahan masalah. Dimana dapat melacak aktivitas yang mungkin menjadi penyebab masalah dan mengambil langkah-langkah perbaikan.
3. **Kepatuhan dan Audit:** Dalam beberapa kasus, organisasi harus mematuhi peraturan tertentu yang mengharuskan mereka untuk menyimpan dan menganalisis log jaringan. Log ini digunakan untuk audit dan verifikasi kepatuhan.
4. **Pemantauan Kinerja:** Log jaringan juga dapat digunakan untuk memantau kinerja jaringan secara keseluruhan. untuk melacak penggunaan bandwidth, latensi, dan masalah kinerja lainnya.
5. **Pelaporan:** Informasi dari log jaringan dapat digunakan untuk menghasilkan laporan aktivitas jaringan yang berguna untuk pemangku kepentingan dalam organisasi.

Tingkat akses log jaringan dapat bervariasi, dan mungkin melibatkan perangkat keras dan perangkat lunak tertentu. Berikut adalah beberapa contoh cara mengakses log jaringan

### 2.2.14.1. Ping Tester



Gambar 2. 4. Software Ping Tester

*Ping Tester* adalah aplikasi yang berfungsi sebagai *network analyzer* (penganalisa jaringan) dengan cara melakukan Ping dan menangkap paket-paket data di jaringan melalui *network interface card* (NIC). Software ini mudah digunakan karena tampilan menggunakan *graphical user interface* (GUI) atau tampilan grafis yang sederhana. Berikut adalah beberapa fitur utama dari Ping Tester:

1. **Pengujian Koneksi:** Ping Tester memungkinkan pengguna untuk menguji koneksi jaringan dengan mengirimkan *packet* pesan ke alamat IP atau nama host tujuan. Ini membantu dalam memeriksa ketersediaan dan kestabilan jaringan.
2. **Pengukuran Latensi:** Dengan melakukan ping ke alamat IP tujuan, Ping Tester dapat mengukur waktu respons atau latensi antara pengirim dan penerima. Ini membantu dalam menentukan kecepatan dan keandalan koneksi jaringan.
3. **Grafik dan Statistik:** Ping Tester menyajikan hasil pengujian dalam bentuk grafik dan memberikan statistik tentang waktu respons, rata-rata,

maksimum, minimum, dan *packet* yang hilang. Ini membantu dalam menganalisis kinerja jaringan.

4. Pilihan Pengaturan: Pengguna dapat mengatur pengaturan ping tester, seperti ukuran *packet*, jumlah pengujian, dan interval antar ping. Hal ini memungkinkan pengguna untuk mengkustomisasi pengujian sesuai kebutuhan mereka.
5. Log dan Riwayat: Ping Tester menyimpan log dan riwayat hasil pengujian sebelumnya, memungkinkan pengguna untuk melacak perubahan koneksi dari waktu ke waktu.
6. Antarmuka Pengguna yang Sederhana: Ping Tester menyediakan antarmuka pengguna yang sederhana dan mudah digunakan. Pengguna dapat dengan mudah memasukkan alamat IP atau nama host tujuan dan memulai pengujian dengan beberapa klik.

#### **2.2.13.2.XDM**

XDM singkatan dari Xtreme Download Manager, adalah perangkat lunak pengelola unduh yang dirancang untuk meningkatkan kecepatan, pengaturan, dan pengelolaan unduh. XDM adalah aplikasi open-source yang berfungsi sebagai pengganti manajer unduh bawaan pada browser web.

#### **2.2.13.3.NetData**

Netdata adalah sebuah perangkat lunak pemantauan waktu nyata (real-time monitoring) yang dirancang untuk memberikan informasi dan visualisasi kinerja sistem yang cepat, akurat, dan terperinci. Dengan menggunakan Netdata, pengguna dapat memonitor berbagai parameter kritis dalam lingkungan komputasi mereka, termasuk penggunaan CPU, memori, jaringan, disk, serta berbagai aplikasi dan layanan. Fitur utama Netdata meliputi:

1. Real time Monitoring: Netdata memberikan pemantauan secara real-time dengan update frekuensi tinggi, memungkinkan pengguna untuk melihat data kinerja sistem secara langsung.

2. Visualisasi yang banyak: Netdata menyajikan data pemantauan dalam bentuk grafik dan tampilan yang interaktif, memungkinkan pengguna untuk dengan mudah memahami dan menganalisis kinerja sistem.
3. Konfigurasi sederhana: Netdata dapat diinstal dan dikonfigurasi dengan mudah tanpa memerlukan pengetahuan teknis yang mendalam. Pengguna dapat mengaktifkan pemantauan untuk berbagai komponen sistem dengan konfigurasi yang minimal.
4. Skalabilitas dan fleksibilitas: Netdata dirancang untuk bekerja pada berbagai sistem operasi dan platform, dan dapat digunakan untuk memantau lingkungan yang kompleks dan berukuran besar dengan ribuan server.
5. Open-source dan gratis: Netdata merupakan perangkat lunak sumber terbuka yang dapat digunakan secara gratis, sehingga dapat diakses dan dikembangkan oleh komunitas pengguna.

#### **2.2.15. UCI**

Unified Configuration *Interface* (UCI) sistem konfigurasi yang digunakan dalam OpenWrt untuk mengatur dan mengelola konfigurasi pada perangkat. UCI menyediakan antarmuka yang konsisten dan terstruktur untuk mengkonfigurasi berbagai aspek sistem dan aplikasi dalam OpenWrt [25], adapun Format konfigurasi dan Perintah yang dapat dilakukan sebagai berikut :

1. Struktur dan Format Konfigurasi UCI
  - a. File Konfigurasi: Konfigurasi UCI disimpan dalam file teks dengan ekstensi ".uci". Setiap file konfigurasi UCI mengatur pengaturan untuk suatu aplikasi atau bagian sistem tertentu.
  - b. Bagian (Section): Setiap file konfigurasi UCI terdiri dari beberapa bagian, yang disebut "section". Setiap section berisi pengaturan spesifik yang berhubungan dengan fitur atau aspek yang sama.
  - c. Opsi (Option): Setiap section memiliki beberapa opsi yang mengatur nilai-nilai konfigurasi yang spesifik untuk section tersebut.
2. Perintah UCI

- a. 'uci show': Perintah ini digunakan untuk melihat konfigurasi yang sedang berjalan pada perangkat.
- b. 'uci get': Perintah ini digunakan untuk mendapatkan nilai dari suatu opsi konfigurasi tertentu.
- c. 'uci set': Perintah ini digunakan untuk mengatur nilai dari suatu opsi konfigurasi tertentu.
- d. 'uci add': Perintah ini digunakan untuk menambahkan section baru ke file konfigurasi UCI.
- e. 'uci delete': Perintah ini digunakan untuk menghapus section atau opsi dari file konfigurasi UCI.
- f. 'uci commit': Perintah ini digunakan untuk menyimpan perubahan konfigurasi yang telah dilakukan ke dalam file konfigurasi UCI.

Ketika pengguna melakukan perubahan pada konfigurasi menggunakan perintah **uci set**, perubahan tersebut belum langsung diterapkan pada perangkat. Perubahan konfigurasi yang dilakukan dengan **uci set** dianggap sebagai perubahan yang belum disimpan (*uncommitted changes*). Untuk menyimpan perubahan tersebut ke dalam file konfigurasi UCI, pengguna perlu menjalankan perintah **uci commit**. Dengan melakukan **uci commit**, perubahan konfigurasi akan diterapkan secara permanen pada perangkat dan disimpan dalam file konfigurasi UCI.

#### 2.2.14.1.Luci

Luci (*Lighttpd User Interface*) adalah antarmuka pengguna berbasis web yang digunakan untuk mengelola dan mengkonfigurasi perangkat keras jaringan yang menjalankan sistem operasi OpenWrt. Luci menyediakan antarmuka yang intuitif dan mudah digunakan, memungkinkan pengguna untuk mengatur berbagai pengaturan dan fitur jaringan[27, 30]. Adapun fitur dan fungsi dari Luci sebagai berikut.

1. Konfigurasi Jaringan: LuCI memungkinkan pengguna untuk mengatur pengaturan jaringan seperti IP address, subnet mask, gateway, DNS, VLAN, dan pengaturan protokol seperti DHCP dan PPPoE.



2. Pengaturan Keamanan: Melalui LuCI, pengguna dapat mengkonfigurasi fitur keamanan seperti firewall, VPN (Virtual Private Network), pengaturan akses jaringan, pengaturan protokol keamanan seperti WPA2 pada Wi-Fi, dan lain-lain.
3. Manajemen Pengguna dan Akses: LuCI menyediakan fitur untuk mengelola pengguna, membuat akun pengguna, mengatur akses hak akses, dan mengatur otorisasi terhadap berbagai fitur dan pengaturan.
4. Manajemen Paket: Pengguna dapat menggunakan LuCI untuk mengelola paket perangkat lunak, menginstal, menghapus, dan memperbarui paket melalui antarmuka web.
5. Monitoring Jaringan: LuCI menyediakan fitur pemantauan untuk melihat status jaringan, kinerja perangkat, penggunaan bandwidth, dan statistik jaringan lainnya.
6. Konfigurasi Layanan dan Aplikasi: Pengguna dapat mengkonfigurasi berbagai layanan dan aplikasi seperti server web (Apache), server file (Samba), server FTP, DNS, dan banyak lagi melalui antarmuka web LuCI.

UCI dan LuCI saling terhubung dan bekerja bersama untuk mengatur konfigurasi pada perangkat OpenWrt. UCI digunakan untuk mengelola konfigurasi pada tingkat sistem, sementara LuCI menyediakan antarmuka grafis untuk mengakses dan mengatur konfigurasi menggunakan UCI. Ketika pengguna melakukan perubahan pada konfigurasi melalui LuCI, LuCI akan menggunakan perintah UCI seperti **uci set** untuk menerapkan perubahan tersebut ke dalam konfigurasi UCI. Kemudian, pengguna dapat menyimpan perubahan dengan menggunakan tombol "Save" dan mengaplikasikannya dengan tombol "Apply" di LuCI, yang akan menjalankan perintah **uci commit** untuk menyimpan perubahan ke dalam file konfigurasi UCI dan menerapkannya pada perangkat OpenWrt.

### **2.2.16. Interface**

*Interface* pada jaringan mengacu pada titik persimpangan antara dua atau lebih perangkat atau jaringan yang memungkinkan pertukaran data dan komunikasi antara host. *Interface* dapat berupa fisik atau virtual dan berfungsi

sebagai batas antara perangkat atau jaringan yang berbeda [24], Adapun Jenis *Interface* sebagai berikut:

1. *Interface* Fisik / Hardware

*Interface* fisik mengacu pada konektor fisik yang menghubungkan perangkat ke jaringan. Contoh *interface* fisik meliputi port Ethernet, konektor RJ-45, Fiber Optic, atau konektor USB

2. *Interface* logis/Virtual

*Interface* logis atau virtual dibuat di atas atau didalam *interface* fisik dan dapat digunakan untuk membagi satu *interface* fisik menjadi beberapa *interface* logis / virtual. Contoh *interface* virtual meliputi VLAN (Virtual Local Area Network), loopback *interface*, atau tunneling *interface*.

### 2.2.16.1.VLAN

VLAN (Virtual Local Area Network) adalah teknologi yang memungkinkan pemisahan Jaringan dari jaringan fisik menjadi beberapa jaringan virtual yang terisolasi. VLAN digunakan untuk mengatur dan mengelompokkan perangkat dalam jaringan berdasarkan kebutuhan dan kebijakan tertentu, meskipun mereka terhubung ke jaringan yang sama secara fisik[25], Adapun Fungsi Vlan dan Jenis Vlan sebagai berikut

A. Fungsi Vlan

1. Segregasi Jaringan: Dengan VLAN, jaringan fisik dapat dibagi menjadi beberapa jaringan virtual yang terisolasi. Ini memungkinkan pemisahan dan segmentasi jaringan berdasarkan kebutuhan organisasi, sehingga memungkinkan pengelompokan perangkat sesuai dengan kebijakan dan kebutuhan khusus.
2. Keamanan dan Pengaturan Akses: VLAN memungkinkan implementasi kebijakan keamanan yang lebih ketat. Dengan menggunakan VLAN, administrator jaringan dapat mengontrol akses perangkat ke jaringan lain dan mengatur pengaturan keamanan yang berbeda untuk setiap VLAN.

3. Efisiensi Lalu Lintas: Dengan VLAN, lalu lintas jaringan dapat dikendalikan dan dikonfigurasi secara lebih efisien. VLAN memungkinkan penyesuaian prioritas lalu lintas, pengaturan QoS (Quality of Service), dan pemisahan broadcast domain, yang dapat meningkatkan kinerja dan efisiensi jaringan.

#### B. Jenis Vlan

1. Port-Based VLAN: VLAN jenis ini mengatur perangkat ke dalam VLAN berdasarkan nomor port fisik pada switch. Setiap port switch ditempatkan ke dalam satu VLAN tertentu.
2. Tagged VLAN: Dalam tagged VLAN, setiap frame data diberi tag dengan informasi VLAN yang sesuai saat melewati switch. Ini memungkinkan satu kabel fisik untuk membawa lalu lintas dari beberapa VLAN secara bersamaan.
3. Protocol-Based VLAN: VLAN jenis ini mengelompokkan perangkat berdasarkan protokol jaringan tertentu. Setiap protokol ditempatkan ke dalam VLAN tertentu.
4. Dynamic VLAN: Dynamic VLAN memungkinkan perangkat otomatis ditugaskan ke VLAN berdasarkan atribut tertentu seperti identitas pengguna atau alamat MAC perangkat.

#### **2.2.17. Batch Programming**

Batch programming adalah salah satu teknik yang digunakan untuk melakukan sederetan proses yang sudah dikonfigurasi pada sebuah file. Dimana terdapat file batch yang berisi perintah-perintah untuk mengatur, memilih, dan mengeksekusi[32]. File batch ini kemudian dijalankan dengan menggunakan CronJob. Dengan demikian, perintah perintah yang sudah di konfigurasi dapat berjalan secara otomatis sesuai waktu yang ditentukan tanpa perlu mengoperasikan secara manual[32].

Batch programming pada OpenWrt atau sistem berbasis Linux mirip dengan penulisan skrip di sistem operasi Linux lainnya menggunakan bahasa seperti Bash (Bourne Again Shell) atau bahasa skrip lainnya. Dalam konteks

OpenWrt, peneliti dapat membuat skrip batch untuk melakukan berbagai tugas, seperti otomatisasi konfigurasi, pemantauan sistem, atau tugas-tugas lainnya.