BAB II

TINJAUAN PUSTAKA

2.1 Teori Dasar

2.1.1 Jaringan komputer

Jaringan komputer adalah kumpulan dua atau lebih komputer yang saling terhubung dengan tujuan untuk berbagi data, informasi, sumber daya, dan layanan. Jaringan komputer memungkinkan pengguna untuk saling berkomunikasi dan berinteraksi dengan perangkat lain di dalam jaringan, bahkan jika perangkat tersebut berada di lokasi yang berbeda. Jaringan komputer dapat dibentuk dengan berbagai jenis teknologi dan protokol, seperti *Ethernet*, *Wi-Fi*, *Bluetooth*, *TCP/IP*, dan lain-lain (Riska, Sugiartawan, & Wiratama, 2018).

Sedangkan menurut Aprilyano et al., jaringan komputer merupakan gabungan antara teknologi komputer dan teknologi komunikasi yang memungkinkan perangkat-perangkat komputer untuk saling terhubung dan berkomunikasi. Dalam jaringan komputer, komputer-komputer yang terhubung dapat berbagi data, sumber daya, dan informasi melalui berbagai media komunikasi, baik itu kabel maupun nirkabel. Teknologi komputer berperan dalam penyediaan perangkat keras dan perangkat lunak yang diperlukan, sementara teknologi komunikasi mendukung transfer data antar perangkat dalam jaringan tersebut. Dengan memadukan kedua teknologi ini, jaringan komputer memungkinkan terjadinya pertukaran informasi yang efisien dan cepat, yang mendukung berbagai aplikasi seperti berbagi file,

komunikasi jarak jauh, dan penggunaan perangkat bersama, seperti printer atau server penyimpanan (Aprilyano Ekklesia Tangkowit, Verry Ronny Palilingan, 2021).

2.1.2 Standar Jaringan Komputer

Standar jaringan dapat dikategorikan dalam dua cara, yaitu formal dan *de facto* (informal). Standarisasi formal adalah standar yang diakui dan disetujui oleh organisasi resmi atau badan pengatur internasional. Berikut adalah beberapa contoh standarisasi keamanan jaringan yang umum digunakan:

1. *ISO/IEC 27001* (Sistem Manajemen Keamanan Informasi)

   Standar internasional untuk sistem manajemen keamanan informasi (Information Security Management System/ISMS).
2. *NIST Cybersecurity Framework (CSF)*

   Kerangka kerja keamanan siber yang dikembangkan oleh *National Institute of Standards and Technology* (*NIST*), digunakan secara luas terutama di Amerika Serikat.
3. *PCI DSS (Payment Card Industry Data Security Standard)*

   Standar keamanan yang ditetapkan untuk perusahaan yang menangani data kartu pembayaran, seperti kartu kredit dengan melindungi data pemegang kartu dari ancaman seperti pencurian identitas dan penipuan.
4. *IEEE 802.1X (Network Access Control)*

   Standar untuk mengontrol akses ke jaringan berbasis port, biasanya digunakan dalam jaringan Wi-Fi.

5. *ITIL (Information Technology Infrastructure Library)* - Keamanan Informasi

   Framework untuk manajemen layanan TI yang mencakup praktik terbaik dalam keamanan informasi. Bertujuan untuk memastikan keamanan layanan TI melalui pengelolaan risiko, enkripsi, dan pemulihan bencana.

6. Tiphon (*Telecommunications and Internet Protocol Harmonization Over Networks*)

   Standar yang dikembangkan oleh ETSI (*European Telecommunications Standards Institute*) untuk memastikan kualitas layanan (*Quality of Service/QoS*) dalam jaringan telekomunikasi dan internet (Sitohang & Setiawan, 2018). Standar Tiphon bertujuan untuk menyatukan protokol telekomunikasi dan internet dalam satu framework, sehingga berbagai layanan seperti suara, data, dan video dapat disampaikan dengan kualitas yang terjamin. Beberapa elemen utama dalam standar Tiphon terkait dengan QoS meliputi:

a) *Latency*, waktu yang diperlukan untuk data berpindah dari satu titik ke titik lain di jaringan. Untuk layanan *real-time* seperti VoIP atau video streaming, latensi yang rendah sangat penting. Terdapat salah satu komponen latensi yang lebih spesifik yakni merujuk pada keterlambatan waktu dalam proses tertentu selama perjalanan paket, rumus standar menghitung delay tertera pada rumus 2.1 dan dapat disimpulkan dengan tabel standar QoS yang tertera pada tabel 2.1 (Alzi & Haeruddin, 2022).

$$Delay\ (s) =$$

Rumus 2. 1 Rumus *Troughput*

$$\frac{\text{Jumlah delay}}{\text{Jumlah paket data yang diterima}}$$

Tabel 2. 1 Tabel Standar TIPHON *Delay*

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

(Sumber: Data Penelitian,2025)

b) *Jitter*, variasi waktu pengiriman data atau selisih delay. Jitter yang terlalu besar dapat mengganggu kualitas suara dan video (Alzi & Haeruddin, 2022) *Jitter* memiliki rumus standar yang tertera pada rumus 2.2 dan tabel standarisasi QoS yang tertera pada tabel 2.2.

$$Jitter = \frac{\text{Jumlah variasi delay}}{\text{Jumlah paket data yang diterima} - 1}$$

Rumus 2. 2 Rumus *Jitter*

Tabel 2. 2 Tabel Standar TIPHON *Jitter*

Kategori	*Jitter (ms)*	Indeks
Sangat Bagus	0 ms	4
Bagus	75 ms	3
Sedang	125 ms	2
Jelek	225 ms	1

(Sumber: Data Penelitian, 2025)

c) *Packet Loss* (kehilangan paket), rasio paket data yang hilang selama transmisi. Kehilangan paket yang tinggi akan mengurangi kualitas layanan, terutama pada aplikasi yang membutuhkan transmisi data *real-time* (Alzi & Haeruddin, 2022). *Packet loss* memiliki rumus standar yang terdapat pada rumus 2.3 dan tabel standarisasi QoS pada tabel 2.3.

$$Packet\ loss = \frac{(\text{Paket pengiriman data} - \text{Paket penerima data})}{\text{Paket data yang dikirim}} \text{ X } 100$$

Rumus 2. 3 Rumus *Packet Loss*

Tabel 2. 3 Tabel Standar TIPHON *Packet Loss*

Kategori	*Packet Loss (%)*	Indeks
Sangat Bagus	0%	4
Bagus	3%	3
Sedang	15%	2
Jelek	25%	1

(Sumber: Data Penelitian, 2025)

d) *Throughput*, kapasitas jaringan untuk mengirimkan data dalam jangka waktu tertentu. *Throughput* yang baik menjamin transfer data yang cepat dan konsisten. (Alzi & Haeruddin, 2022) Tiphon memiliki rumus standar untuk menghitung *throughput* yang tertera pada rumus 2.4 dan dapat dinyatakan melalui tabel sebagai standar *QoS* seperti pada tabel 2.4.

$$Throughput = \frac{\left(\frac{\text{Bytes}}{\text{Time span}} * 8\right)}{1000}$$

Rumus 2. 4 Rumus Troughput

Tabel 2. 4 Tabel Standar TIPHON *Throughput*

Kategori	*Throughput*	Indeks
Sangat Bagus	>2,1 Mbps	4
Bagus	700-1200 Kbps	3
Sedang	338-700 Kbps	2
Jelek	0-338 Kbps	1

Standar Tiphon menetapkan kriteria QoS ini agar layanan berbasis IP dan telekomunikasi dapat diakses dengan konsisten dan efisien oleh pengguna di seluruh dunia. Implementasi dari standar ini biasanya melibatkan berbagai teknik pengelolaan jaringan seperti *traffic shaping, priority queuing,* dan *bandwidth reservation*.

Sedangkan standar *de facto* (informal) adalah standar yang diterima secara luas dan digunakan secara umum meskipun belum ditetapkan secara resmi oleh organisasi standarisasi, contohnya *tcp/ip*, *html* dan *usb*.

2.1.3 Jenis Jaringan Komputer

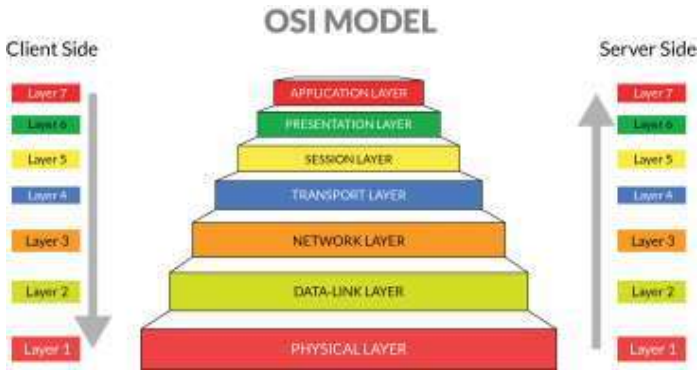
Jaringan komputer dapat dibedakan melalui areanya, LAN (*Local Area Network*), MAN (*Metropolitan Area Network*), WAN (*Wide Area Network*) berikut penjelasan lebih lanjut:

1. LAN (*Local Area Network*) adalah jaringan yang memiliki cakupan yang kecil, seperti jaringan pada sebuah divisi perusahaan atau didalam sebuah rumah. (Nasir, 2018)

2. MAN (*Metropolitan Area Network)* terdiri dari 2 atau lebih jaringan LAN yang berada dalam area geografis yang sama, contohnya perusahaan cabang dapat terhubung dengan perusahaan pusat yang berada pada daerah yang sama. (Nasir, 2018)
3. WAN (*Wide Area Network)* adalah jaringan komputer dengan cakupan luas dimana ia dapat menghubungkan jaringan antar negara bahkan antar benua.(Nasir, 2018)

2.1.4 Model *Operating System Interconnect* (OSI) *Layer*

Model OSI terdiri dari tujuh lapisan atau partisi berupa tumpukan vertikal. Tujuan dibuatnya adalah menjadi rujukan untuk vendor dan developer yang dapat bersifat *interporate* artinya dapat bekerja dengan system atau produk tanpa harus melakukan upaya khusus dari pengguna. Setiap layer memiliki peran yang saling berkaitan seperti pada gambar 2.1. Berikut penjelasan singkat dari ketujuh lapisan tersebut:



Gambar 2. 1 Model *OSI Layer*
Sumber: (https:/sites.google.com)

1. Lapisan fisik

Lapisan pertama dan terendah dari model OSI. lapisan yang berfungsi untuk mentransmisikan bit data digital dari *physical layer* pengirim ke *physical layer* penerima. Data ditansmisikan menggunakan sinyal dan media fisik, seperti tegangan listrik, kabel, frekuensi radio, atau *infrared* (Irawan, 2011).

2. Lapisan datalink

   Lapisan yang berfungsi sebegai pemeriksa kesalahan yang mungkin terjadi pada transmisi data lalu mengubah bit menjadi data frame. Selain itu, datalink mengelola pengalamatan fisik seperti alamat *MAC* pada jaringan. lapisan in terbagi menjadi dua bagian yaitu *MAC* dan *LLC*. *MAC* berfungsi untuk mengendalikan perangkat untuk memperoleh akses ke medium dan izin melakukan transmisi data. *LLC* berfungsi untuk mengidentifikasi dan membungkus protokol *network layer* dan mengontrol pemeriksaan kesalahan (Irawan, 2011).

3. *Network* layer

   Lapisan ini berfungsi untuk menetapkan jalur yang akan digunakan atau bisa disebut *routing*. Lapisan ini menyimpan alamat *IP* untuk setiap perangkat pada jaringan melalui *ARP* (Irawan, 2011).

4. *Transport* layer

   Transport layer mengirimkan pesan dua atau lebih host didalam jaringan juga menangani pemecahan dan penggabungan pesan dan juga mengontrol kehandalan jalur koneksi yang diberikan. Protokol *TCP* merupakan contoh yang paling sering digunakan pada *transport layer* (Kristianto, Najoan, 2017).

5. *Session* layer

   Session layer bertanggung jawab untuk mengendalikan sesi koneksi dialog seperti menetapkan, mengelola dan memutuskan koneksi antar komputer. Untuk dapat membentuk sebuah sesi komunikasi yang menggunakan sirkuit virtual yang dibuat oleh *transport layer* (Irawan, 2011).

6. *Presentation* layer

   Presentation layer bertanggung jawab untuk mendefinisikan sintaks yang digunakan host jaringan untuk berkomunikasi. *Presentation layer* juga melakukan proses enkripsi/dekripsi informasi atau data sehingga mampu digunakan pada lapisan aplikasi (Irawan, 2011).

7. *Application* layer

   Application layer merupakan lapisan paling atas dari model OSI dan bertanggung jawab untuk menyediakan sebuah *interface* antara protokol jaringan dengan aplikasi yang ada pada komputer. Lapisan ini menyediakan layanan yang dibutuhkan oleh aplikasi, seperti menyediakan sebuah interface untuk *Simple Mail Transfer Protocol (SMTP)*, *telnet* dan *File Transfer Protocol (FTP)*. Pada bagian sinilah dimana aplikasi saling terkait dengan jaringan (Irawan, 2011).

2.1.5 Router

Router adalah alat yang digunakan untuk menghubungkan antar jaringan yang berbeda satu sama lain, selain itu *router* dapat memilih jalan terbaik untuk sampai ketujuan dengan melihat alamat asal dan alamat tujuan dari paket (Purwanto, 2015). Dalam kehidupan sehari-hari *router* tergolong masih mahal oleh

karena itu sulit untuk dijangkau oleh kalangan masyarakat biasa. Solusi dari penggunaan *router* yaitu dengan menggunakan *router* mikrotik yang khusus digunakan untuk membuat *router* dan membantu administrasi jaringan untuk membuat jaringan berskala kecil. Fungsi lain dari *router* adalah sebagai keamanan atau *firewall* yang dapat melakukan pemeriksaan paket dan memblokir lalu lintas yang berbahaya.

Router juga memiliki kekurangan diantaranya adalah kompleksitas konfigurasi, mahal, *Single Point Of Failure*(*SPOF*) dimana jika *router* bermasalah maka lalu lintas yang melalui *router* tersebut dapat terganggu dan memerlukan protocol yang sesuai untuk berkomunikasi dengan jaringan lain. Berikut adalah beberapa jenis *router* yang umum digunakan:

1. *Router Residensial*

   Router yang digunakan di rumah atau kantor kecil. Mereka biasanya memiliki beberapa port *ethernet* untuk menghubungkan perangkat kabel, dan juga menyediakan koneksi nirkabel (*Wi-Fi*) untuk menghubungkan perangkat secara nirkabel yang menghubungkan jaringan lokal dengan internet.

2. *Router* Jaringan Nirkabel (*Wireless Router*)

   Router ini memiliki fungsi serupa dengan *router* residensial, tetapi fokusnya adalah pada pengaturan dan manajemen koneksi nirkabel. Mereka menyediakan akses *Wi-Fi* kepada perangkat nirkabel seperti laptop, *smartphone*, atau tablet, sambil juga menghubungkan jaringan lokal dengan internet.

3. *Router Edge*

   Router tepi adalah *router* yang ditempatkan di tepi jaringan, menghubungkan jaringan perusahaan ke internet atau jaringan lain di luar. Router ini sering digunakan di *ISP* atau pusat data.

2.1.6 *Bandwidth*

Pengertian *Bandwidth* sendiri bisa diartikan sebagai jumlah nilai konsumsi transfer data yang dihitung dalam hitungan *bit*/detik atau yang biasanya di sebut dengan *bit per second (bps)*, antara *server* dan *client* dalam waktu tertentu (Pamungkas, 2016). *Bandwith* bisa diartikan juga kapasitas maksimum dari suatu jalur komunikasi yang dipakai untuk mentransfer data dalam hitungan detik. *Bandwidth* biasanya dinyatakan dalam bit per detik , seperti 60 Mbps atau 60 Mbps, untuk menjelaskan laju transfer data 60 juta bit (megabits) per detik. (Firmansyah, 2020)

2.1.7 Manajemen *bandwidth*

Manajemen *bandwidth* adalah proses mengukur dan mengontrol komunikasi pada link jaringan untuk menghindari kemacetan jaringan dan kinerja buruk. Maksud dari manajemen *bandwidth* ini adalah menerapkan pengalokasian atau pengaturan *bandwidth* menggunakan PC *router* mikrotik dengan memberikan kemampuan dalam pengaturan *bandwidth* jaringan dan memberikan level layanan seseuai dengan kebutuhan dan prioritas dari jaringan salah satu cara untuk manajemen *bandwidth* adalah dengan menggunakan metode *radius* (Supendar & Handrianto, 2017).

2.1.7.1 Radius authentication

Radius Server adalah sebuah server autentikasi yang digunakan untuk mengatur akses ke jaringan atau sumber daya lainnya dalam suatu jaringan komputer. Kata radius sendiri adalah singkatan dari *Remote Authentication Dial-In User Service* (Muttaqin, Rochim, & Widianto, 2016). Fungsi utama dari radius adalah untuk memastikan bahwa hanya pengguna yang memiliki hak akses yang diberikan oleh administrator jaringan yang dapat mengakses jaringan atau sumber daya lainnya. Saat seorang pengguna mencoba untuk terhubung ke jaringan, radius akan memverifikasi identitas pengguna dengan menghubungkan ke database yang berisi informasi login pengguna seperti nama pengguna dan kata sandi. Jika informasi login valid, radius akan memberikan akses ke jaringan atau sumber daya lainnya yang diizinkan.

Selain otentikasi, radius juga dapat digunakan untuk mengatur manajemen *bandwidth* pada jaringan. Saat seorang pengguna terhubung ke jaringan, Radius dapat menetapkan tingkat *bandwidth* tertentu untuk pengguna berdasarkan kriteria seperti jenis pengguna, waktu akses, dan jenis aplikasi yang digunakan. Radius server dapat diimplementasikan pada server yang berbeda-beda atau pada perangkat jaringan seperti *router* atau switch. Implementasi radius dapat membantu meningkatkan keamanan jaringan dan memudahkan manajemen akses pengguna pada jaringan.

Kelebihan dari metode radius sendiri adalah memungkinkan manajemen autentikasi pengguna, memudahkan administrasi, ideal untuk jaringan besar,

mendukung enkripsi data autentikasi, dan dapat mengontrol pengelolaan kebijakan akses pengguna dengan lebih mudah dan terperinci.

2.1.8 Mikrotik

Mikrotik adalah sebuah perusahaan di Latvia yang memproduksi perangkat keras jaringan (*network hardware*) dan *software* untuk keperluan manajemen jaringan (*network management*) (Sitohang, Pangaribuan, & Maslan, 2023). Mikrotik adalah perangkat jaringan komputer yang berupa *hardware* dan *software* yang dapat difungsikan sebagai *router*, sebagai alat *filtering*, *switching* maupun yang lainnya (Amarudin, 2018) Secara umum, Mikrotik *RouterOS* dan perangkat keras jaringan Mikrotik digunakan oleh para administrator jaringan untuk membangun dan mengelola jaringan komputer yang handal, aman, dan efisien.

Dalam penggunaannya, Mikrotik dapat diaplikasikan dalam berbagai jenis jaringan, mulai dari jaringan kecil seperti di rumah atau kantor kecil hingga jaringan yang lebih kompleks seperti di perusahaan besar atau provider layanan internet (ISP). Mikrotik memiliki berbagai jenis, diantaranya adalah :

1. Mikrotik RouterOS

   Mikrotik *router*os adalah mikrotik dengan jenis *software* yang dapat diunduh di www.mikrotik.com. Mikrotik jenis ini dapat digunakan pada komputer rumah yang berfungsi untuk mengubah komputer menjadi *router*.

2. Mikrotik *RouterBOARD*

   Mikrotik *RouterBoard* adalah mikrotik dalam bentuk perangkat keras yang didalamnya sudah terinstal *Mikrotik RouterOS*. Jenis dari mikrotik ini

banyak sekali, diantaranya *RouterBoard RB011*, *RouterBoard RB3011*, *RouterBoard RB4011*, *RouterBoard RB1100AHx4*, *RouterBoard CCR1009*, *RouterBoard hAP ac2,* dan lain sebagainya.

Untuk mengakses perangkat MikroTik, ada beberapa cara yang dapat dilakukan, tergantung pada kebutuhan dan perangkat yang digunakan, misalnya melalui Winbox (GUI), Webfig (Web Interface), SSH (Command Line Interface), Telnet (PuTTY) dan Mobile (MikroTik App).

2.2 Penelitian Terdahulu

Pada penelitian ini akan memaparkan penelitian terdahulu yang relavan dengan topik yang diangkat peneliti, adapun penelitian sebelumnya adalah sebagai berikut:

1. Artikel berjudul "*Simple solution for low cost bandwidth management*" yang diterbitkan di TELKOMNIKA (Vol. 19, No. 4, Agustus 2021) terindeks di Scopus dengan peringkat Q2 dalam kategori *Electrical and Electronic Engineering* membahas solusi manajemen bandwidth dengan biaya rendah menggunakan *RADIUS server* dan Mikrotik *RouterBoard*. Penelitian ini mengatasi masalah penggunaan *bandwidth* yang tidak efisien pada jaringan, terutama untuk aktivitas yang tidak produktif seperti streaming video. Metode yang digunakan untuk mengatur bandwidth menggunakan fitur *Queue Tree*, dengan data klien yang disimpan dalam *MySQL* dan pengelolaan kuota menggunakan *PHP scripts*. Hasil uji coba menunjukkan bahwa *PHP scripts* lebih efektif dalam mengelola bandwidth dibandingkan modul *SQL counter*. Sistem ini juga dilengkapi dengan

antarmuka berbasis web untuk memudahkan monitoring penggunaan bandwidth. Penelitian ini menawarkan solusi manajemen bandwidth yang lebih efisien dan terjangkau bagi organisasi yang membangun jaringan *hotspot* (Sukarsa et al., 2021).

2. Artikel yang berjudul "*A Novel Network Optimization Framework Based on Software-Defined Networking (SDN) and Deep Learning (DL) Approach*" yang diterbitkan dalam *International Journal on Informatics Visualization* (Vol. 8, No. 4, Desember 2024) terindeks di Scopus dengan peringkat Q4 membahas tentang solusi untuk mengelola bandwidth dan meningkatkan kualitas layanan (QoS) pada jaringan menggunakan pendekatan *Software-Defined Networking* (SDN) dan *Deep Learning* (DL). Penelitian ini mengatasi keterbatasan mekanisme QoS konvensional yang statis dan tidak mampu beradaptasi dengan permintaan jaringan yang dinamis. Dalam penelitian ini, SDN digunakan untuk memantau jaringan secara global dan mengelola perangkat jaringan secara terpusat, sedangkan algoritma DL meningkatkan kemampuan sistem dalam menentukan konfigurasi bandwidth yang tepat untuk trafik sensitif. Sistem ini dapat menyesuaikan alokasi bandwidth secara dinamis sesuai kebutuhan, tanpa intervensi manual (Fendi, Rizal, Isa, & Adib, 2024).
3. Artikel berjudul "*Dynamic QoS: Automatically Modifying QoS Queue's Maximum Bandwidth Rate-Limit of Network Devices for Network Improvement*" yang diterbitkan di IJASET (Vol. 13, No. 6, 2023) terindeks di Scopus dengan peringkat Q4 dalam kategori *Engineering* (*miscellaneous*)

membahas mengenai solusi *Dynamic QoS* untuk mengelola *bandwidth* secara otomatis pada perangkat jaringan, khususnya untuk trafik sensitif seperti video konferensi dan VoIP. Penelitian ini mengatasi masalah keterbatasan QoS konvensional dalam jaringan besar yang mengalami kemacetan dan trafik heterogen. Dengan menggunakan *Software-Defined Networking* (SDN), sistem ini dapat memonitor *jitter* dan *bandwidth*, serta menyesuaikan kapasitas *bandwidth* secara dinamis dengan mengubah *QoS Queue's Maximum Bandwidth Rate-Limit* pada router. Pengujian dilakukan menggunakan *Mininet* untuk mensimulasikan jaringan dan mengukur kinerja sistem. Hasilnya menunjukkan bahwa sistem ini dapat meningkatkan throughput dan mengurangi *jitter* pada trafik sensitif, meskipun penerapan *Deep Learning* (DL) masih dalam tahap pengembangan untuk penelitian lanjutan (Osman et al., 2023) .

4. Artikel "Metode PCQ dan Queue Tree untuk Implementasi Manajemen Bandwidth Berbasis Mikrotik" yang diterbitkan dalam Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi) Vol. 5 No. 2 (2021) terakreditasi SINTA 2. Membahas penggunaan dua metode manajemen bandwidth, yaitu PCQ (*Per Connection Queue*) dan *Queue Tree* untuk mengoptimalkan penggunaan bandwidth terbatas di jaringan berbasis Mikrotik. Permasalahan utama yang dibahas adalah penurunan kualitas layanan (QoS) akibat penggunaan bandwidth yang tidak efisien di jaringan dengan banyak perangkat terhubung. Peneliti menggunakan metode PCQ untuk membagi bandwidth secara otomatis dan merata sesuai jumlah

perangkat yang terhubung, serta *Queue Tree* untuk melakukan antrian lebih kompleks yang memprioritaskan trafik tertentu seperti streaming dan browsing. Metode yang digunakan meliputi perancangan jaringan, implementasi Mikrotik RouterOS, serta pengujian QoS melalui pengukuran parameter seperti *jitter*, *ping*, *throughput*, dan *packet loss*. Algoritma yang diterapkan termasuk penggunaan PCQ untuk optimasi QoS pada jaringan besar dan *Queue Tree* untuk pengelolaan trafik berbasis prioritas. Hasil yang diharapkan dari penelitian ini adalah pengoptimalan bandwidth yang memungkinkan seluruh perangkat di jaringan memanfaatkan internet secara maksimal tanpa peningkatan kapasitas bandwidth. Kendala yang dihadapi meliputi pengaturan konfigurasi Mikrotik yang kompleks, serta tantangan dalam mengelola banyak perangkat dengan kebutuhan yang berbeda-beda. Namun, hasil pengujian menunjukkan perbaikan signifikan pada QoS, dengan jitter rata-rata 1.64 ms, ping 36.8 ms, throughput stabil di angka 2 Mbps, dan packet loss 0.1%, yang menunjukkan keberhasilan sistem manajemen bandwidth yang diterapkan (Christanto, Daru, & Kurniawan, 2021).

5. Artikel berjudul "Analisa QoS dengan *Simple Queue*, *Queue Tree*, dan *Hierarchical Token Bucket*" diterbitkan dalam Jurnal Inovtek Polbeng - Seri Informatika terakreditasi SINTA 3. Membahas pengelolaan manajemen *bandwidth* pada jaringan menggunakan metode *Simple Queue, Queue Tree,* dan *Hierarchical Token Bucket* (HTB) untuk mengoptimalkan distribusi *bandwidth* pada jaringan Warnet Pro Net Bangkinang. Peneliti menganalisis

dan membandingkan hasil *Quality of Service* (QoS) antara ketiga metode tersebut dengan perangkat Mikrotik dan Linux Ubuntu. Permasalahan yang dihadapi adalah distribusi bandwidth yang tidak merata, yang menyebabkan beberapa pengguna mengalami penurunan kinerja, terutama saat banyak pengguna aktif secara bersamaan. Metode yang digunakan mencakup penerapan *Simple Queue*, *Queue Tree*, dan HTB pada perangkat Mikrotik dan sistem berbasis Linux Ubuntu, untuk mengatur alokasi bandwidth dan memprioritaskan jenis trafik tertentu. *Simple Queue* digunakan untuk pengaturan yang lebih sederhana, sedangkan *Queue Tree* dan HTB mengatur *bandwidth* dengan lebih kompleks dan terstruktur. Algoritma yang digunakan termasuk pembagian *bandwidth* berdasarkan peraturan yang diatur dalam *Queue Tree* dan pembatasan trafik pada HTB. *Output* yang diharapkan adalah peningkatan kinerja jaringan dengan distribusi bandwidth yang lebih adil dan terkontrol, yang tercermin pada parameter *throughput*, *delay*, *jitter*, dan *packet loss* yang diukur selama pengujian. Kendala yang dihadapi mencakup perbedaan dalam kinerja masing-masing metode, serta tantangan dalam mengoptimalkan konfigurasi Mikrotik dan Linux Ubuntu agar lebih efisien. Hasil penelitian menunjukkan bahwa *Queue Tree* pada Mikrotik memberikan kinerja QoS yang terbaik, dengan nilai throughput lebih tinggi dibandingkan *Simple Queue* dan HTB pada Linux Ubuntu. Sistem manajemen bandwidth yang optimal dapat mengatasi masalah akses jaringan yang lambat dan mengurangi masalah kemacetan,

memberikan QoS yang lebih baik di jaringan (Toresa, Lisnawita, & Renadi, 2020).

6. Artikel berjudul "Sistem *Autentikasi Hotspot* Menggunakan LDAP dan *RADIUS* pada Jaringan Internet Wireless Prodi Teknik Sistem Komputer" diterbitkan dalam Jurnal Teknologi dan Sistem Komputer (Vol. 4 No. 2 April 2016) yang terakreditasi SINTA 3. Penelitian ini membahas pengelolaan akses pengguna pada jaringan *hotspot* menggunakan sistem otentikasi berbasis LDAP dan RADIUS untuk meningkatkan keamanan dan efisiensi. Masalah yang diangkat adalah pengelolaan akses pengguna yang tidak terstruktur, yang dapat menurunkan keamanan dan penggunaan bandwidth. Untuk mengatasi hal ini, peneliti mengusulkan penggunaan LDAP untuk manajemen data pengguna dan RADIUS untuk otentikasi dan otorisasi pengguna jaringan wireless. Metode yang digunakan adalah implementasi sistem dengan mengintegrasikan kedua teknologi ini, di mana LDAP mengelola data pengguna dan RADIUS bertanggung jawab atas proses otentikasi dan otorisasi akses. Sistem ini menggunakan algoritma autentikasi berbasis *username* dan *password* yang diverifikasi melalui LDAP dan dikendalikan oleh RADIUS. Hasilnya adalah sistem dapat meningkatkan keamanan jaringan hotspot dengan memastikan bahwa hanya pengguna yang terautentikasi yang dapat mengakses jaringan, serta menyediakan laporan penggunaan bandwidth yang dapat membantu manajemen jaringan lebih efisien. Kendala yang dihadapi termasuk kompleksitas dalam mengonfigurasi dan mengintegrasikan LDAP dengan

RADIUS, serta pengelolaan data pengguna dalam jaringan besar. Peneliti juga menyoroti penerapan sistem ini dalam mengurangi masalah keamanan di jaringan hotspot serta pentingnya sistem ini dalam lingkungan pendidikan atau perusahaan untuk mengelola akses jaringan secara aman dan terkontrol (Muttaqin et al., 2016).

7. Artikel berjudul "Manajemen *Autentikasi User* Menggunakan Metode *RADIUS Server* pada RS Jantung Hasna Medika" diterbitkan dalam Jurnal Ilmiah Manajemen Informatika dan Komputer (Vol. 06 No. 02 Juni 2022) terakreditasi SINTA 3. Penelitian ini membahas penerapan metode *RADIUS server* untuk manajemen autentikasi pengguna di RS Jantung Hasna Medika. Masalah yang diangkat adalah pengelolaan akses jaringan yang aman dan efisien di rumah sakit untuk memastikan hanya pengguna yang terautentikasi yang dapat mengakses jaringan dan aplikasi penting. Metode yang digunakan adalah implementasi *RADIUS server*, yang berfungsi untuk otentikasi, otorisasi, dan akuntansi (AAA) pengguna. Teknik yang digunakan dalam penelitian ini adalah *RADIUS server* dengan protokol standar untuk menjaga keamanan proses otentikasi. Hasilnya adalah sistem yang dapat meningkatkan keamanan dan kontrol akses jaringan rumah sakit, serta mengurangi risiko kebocoran data dan akses yang tidak sah. Kendala yang dihadapi meliputi tantangan dalam mengintegrasikan *RADIUS server* dengan sistem yang ada dan pengelolaan data pengguna yang cukup besar. Penelitian ini juga menekankan pentingnya pengelolaan akses yang aman untuk melindungi kerahasiaan data pasien dan aplikasi medis yang

digunakan di rumah sakit (Haris Abdul Hadi, Iin, Gifthera Dwilestari, Ahmad Faqih, & Nisa Dienwati Nuris, 2022).

8. Artikel yang berjudul "Manajemen *Bandwidth* dan Manajemen Pengguna pada Jaringan *Wireless Mesh Network* dengan Mikrotik" diterbitkan dalam Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer (Vol. 1 No. 11 November 2017) terakreditasi sinta 4. Penelitian ini membahas penerapan manajemen bandwidth dan manajemen pengguna dalam jaringan Wireless Mesh Network menggunakan perangkat Mikrotik untuk meningkatkan kinerja jaringan. Masalah yang diangkat adalah bagaimana mengelola bandwidth dan akses pengguna secara efisien dalam jaringan wireless mesh, yang sering kali mengalami kendala terkait dengan pengalokasian sumber daya dan pengelolaan akses yang tidak terkontrol dengan baik. Metode yang digunakan dalam penelitian ini adalah eksperimen dan implementasi pada jaringan *Wireless Mesh Network* dengan menggunakan Mikrotik untuk mengatur *bandwidth* dan mengelola akses pengguna. Peneliti mengintegrasikan beberapa fitur Mikrotik, seperti *Queue Simple* dan *Hotspot*, untuk membatasi *bandwidth* dan mengelola koneksi pengguna sesuai dengan kebijakan yang ditentukan. Teknik yang digunakan termasuk *Traffic Shaping* dan *Bandwidth Management* menggunakan Mikrotik RouterOS untuk memastikan distribusi *bandwidth* yang optimal dan pengelolaan akses pengguna yang efisien. Hasilnya adalah peningkatan kinerja jaringan dengan pengelolaan bandwidth yang lebih baik dan pengaturan akses pengguna yang adil. Kendala yang dihadapi dalam

penelitian ini mencakup keterbatasan pada perangkat keras yang digunakan dan tantangan dalam menyinkronkan konfigurasi Mikrotik dengan kebutuhan jaringan yang lebih kompleks. Selain itu, peneliti juga membahas tentang penerapan sistem dalam konteks jaringan *Wireless Mesh Network* yang sering digunakan dalam lingkungan yang membutuhkan jaringan yang fleksibel dan skalabel, seperti kampus atau area publik (Ardiansa & Primananda, 2017).

9. Artikel berjudul "Sistem *Autentikasi Hotspot* Menggunakan *RADIUS Server Mikrotik Router*" oleh Herman Kuswanto, diterbitkan dalam Jurnal *Informatics For Educators and Professionals* (Vol. 2 No. 1 Desember 2017) terakreditasi SINTA 4. Penelitian ini membahas penerapan *RADIUS server* Mikrotik Router untuk sistem *autentikasi hotspot* guna meningkatkan keamanan jaringan di area publik, seperti di sekolah atau kampus. Masalah yang diangkat adalah pentingnya pengelolaan akses yang aman pada jaringan hotspot, yang sering kali terabaikan, menyebabkan potensi risiko penyalahgunaan akses dan kebocoran data. Penelitian ini mengusulkan penggunaan *RADIUS server* yang terintegrasi dengan Mikrotik Router untuk memastikan hanya pengguna yang *terautentikasi* yang bisa mengakses jaringan hotspot. Metode yang digunakan adalah implementasi sistem autentikasi menggunakan *RADIUS server* dan Mikrotik Router untuk mengontrol akses pengguna. Teknik yang digunakan mencakup penggunaan *RADIUS server* untuk otentikasi dan otorisasi, serta Mikrotik Router untuk pengaturan lalu lintas data dan kebijakan akses yang diterapkan. Hasilnya

adalah sistem autentikasi yang efisien dan aman, yang dapat mencegah penyalahgunaan akses dan menyediakan laporan penggunaan jaringan. Kendala yang dihadapi dalam penelitian ini termasuk tantangan dalam integrasi sistem dan pengelolaan data pengguna dalam jaringan dengan banyak pengguna. Peneliti juga menekankan pentingnya pengamanan akses untuk memastikan kerahasiaan data dan keamanan pengguna (Kuswanto, Mandiri, Jl, Damai, & Barat, 2017).

2.3 Kerangka Pemikiran

Berdasarkan teori yang telah diperoleh dan dijelaskan, kerangka penelitian ini bisa digambarkan seperti pada gambar 2.2.

Gambar 2. 2 Kerangka Pemikiran
(Sumber: Data Penelitian, 2025)

Terdapat 3 tahapan yang terdapat pada kerangka pemikiran peneliti, yaitu:

1. Input berupa kebutuhan internet yang meningkat yang memungkinkan siapapun dapat mengakses internet secara berlebihan sehingga terdapat pengambilan *bandwidth* yang tidak merata.

2. Proses dengan melakukan konfigurasi pada *router* untuk pembagian *bandwidth* yang merata menggunakan *radius server* sebagai autentikasinya dan *packages userman* untuk membatasi *bandwidth*.
3. Output berupa setiap pengguna dapat menggunakan internet dengan *bandwidth* yang telah ditetapkan dan *radius server* bekerja dengan baik dalam menjalankan tugasnya.