TESIS

ANALISIS MITIGASI *BUFFERBLOAT* UNTUK PENINGKATAN *QUALITY OF SERVICE* PADA JARINGAN PENDIDIKAN BERBASIS *MIKROTIK*

(Studi Kasus Di SMKS Al-Islam Joresan Mlarak Ponorogo)

disusun oleh

AZIB WIDAD ZUHAILY IMAM

23.55.1413

Konsentrasi : Digital Transformation Intelligence

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2026

TESIS

ANALISIS MITIGASI *BUFFERBLOAT* UNTUK PENINGKATAN *QUALITY OF SERVICE* PADA JARINGAN PENDIDIKAN BERBASIS *MIKROTIK*

(Studi Kasus Di SMKS Al-Islam Joresan Mlarak Ponorogo)

BUFFERBLOAT MITIGATION ANALYSIS TO IMPROVE QUALITY OF SERVICE ON MIKROTIK BASED EDUCATIONAL NETWORKS

(Case Study At Al-Islam Joresan Mlarak Vocational School Ponorogo)

Diajukan untuk memenuhi salah satu syarat mencapai derajat Pascasarjana

Program Studi Magister PJJ Informatika

disusun oleh

AZIB WIDAD ZUHAILY IMAM

23.55.1413

Konsentrasi : Digital Transformation Intelligence

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2026

HALAMAN PERSETUJUAN

ANALISIS MITIGASI *BUFFERBLOAT* UNTUK PENINGKATAN *QUALITY OF SERVICE* PADA JARINGAN PENDIDIKAN BERBASIS *MIKROTIK*

(Studi Kasus Di SMKS Al-Islam Joresan Mlarak Ponorogo)

BUFFERBLOAT MITIGATION ANALYSIS TO IMPROVE QUALITY OF SERVICE ON MIKROTIK BASED EDUCATIONAL NETWORKS

(Case Study At Al-Islam Joresan Mlarak Vocational School Ponorogo)

yang disusun dan diajukan oleh

Azib Widad Zuhaily Imam

23.55.1413

telah disetujui oleh Dosen Pembimbing Tesis
pada tanggal 20 Mei 2026

Dosen Pembimbing,

Hanif Al Fatta, S.Kom., M.Kom., Ph.D.
190302096

HALAMAN PENGESAHAN

ANALISIS MITIGASI *BUFFERBLOAT* UNTUK PENINGKATAN *QUALITY OF SERVICE* PADA JARINGAN PENDIDIKAN BERBASIS *MIKROTIK*

(Studi Kasus Di SMKS Al-Islam Joresan Mlarak Ponorogo)

BUFFERBLOAT MITIGATION ANALYSIS TO IMPROVE QUALITY OF SERVICE ON MIKROTIK BASED EDUCATIONAL NETWORKS

(Case Study At Al-Islam Joresan Mlarak Vocational School Ponorogo)

yang disusun dan diajukan oleh

Azib Widad Zuhally Imam

23.55.1413

Telah dipertahankan di depan Dewan Penguji
pada tanggal 11 Juni 2026

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Dhani Ariatmanto, S.Kom., M.Kom., Ph.D. **NIK. 190302197**	
Dr. Kumara Ari Yuana, S.T., M.T. **NIK. 190302575**	
Hanif Al Fatta, S.Kom., M.Kom., Ph.D. **NIK. 190302096**	

Tesis ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Magister Komputer
Tanggal 11 Juni 2026

DEKAN FAKULTAS ILMU KOMPUTER

Prof. Dr. Kusrini, M.Kom.
NIK. 190302106

HALAMAN PERNYATAAN KEASLIAN TESIS

Yang bertandatangan di bawah ini,

Nama mahasiswa : Azib Widad Zuhaily Imam
NIM : 23.55.1413

Menyatakan bahwa Tesis dengan judul berikut:

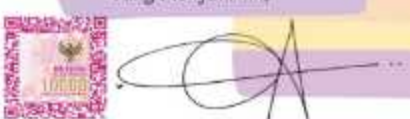
Analisis Mitigasi *Bufferbloat* Untuk Peningkatan *Quality Of Service* Pada Jaringan Pendidikan Berbasis *Mikrotik* (Studi Kasus Di SMKS Al-Islam Joresan Mlarak Ponorogo)

Dosen Pembimbing : Hanif Al Fatta, S.Kom., M.Kom., Ph.D.

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 11 Juni 2026

Yang Menyatakan,



Azib Widad Zuhaily Imam

HALAMAN PERSEMBAHAN

Alhamdulillahirabbil 'alamin, puji syukur penulis panjatkan kehadirat Allah SWT atas segala rahmat, hidayah, serta karunia-Nya sehingga penulis dapat menyelesaikan tesis yang berjudul "Analisis Mitigasi *Bufferbloat* Untuk Peningkatan *Quality Of Service* Pada Jaringan Pendidikan Berbasis *Mikrotik* (Studi Kasus Di SMKS Al-Islam Joresan Mlarak Ponorogo)" dengan baik.

Karya ini penulis persembahkan kepada kedua orang tua tercinta yang senantiasa memberikan doa, kasih sayang, pengorbanan, dukungan, motivasi, dan semangat tanpa henti kepada penulis dalam menempuh pendidikan hingga menyelesaikan tesis ini. Terima kasih atas segala perjuangan dan ketulusan yang tidak akan pernah dapat terbalaskan.

Penulis juga mempersembahkan tesis ini kepada keluarga besar yang selalu memberikan dukungan moral, semangat, dan doa terbaik selama proses penyusunan tesis. Kepada dosen pembimbing dan dosen penguji, penulis mengucapkan terima kasih atas segala arahan, bimbingan, masukan, serta ilmu yang diberikan sehingga tesis ini dapat tersusun dengan lebih baik dan sistematis.

Tesis ini juga penulis persembahkan kepada SMKS Al-Islam Joresan Mlarak Ponorogo yang telah memberikan kesempatan dan dukungan dalam pelaksanaan penelitian. Tidak lupa kepada sahabat, teman seperjuangan, serta semua pihak yang telah membantu penulis baik secara langsung maupun tidak langsung dalam proses penyusunan tesis ini.

Akhir kata, penulis mempersembahkan karya sederhana ini kepada almamater tercinta dan berharap semoga penelitian ini dapat memberikan manfaat, kontribusi, serta menjadi referensi dalam pengembangan ilmu pengetahuan khususnya di bidang jaringan komputer dan *Quality Of Service (QoS)*.

Yogyakarta, 01 Juni 2026

Penulis

MOTTO

Alloh Tidak Mengatakan Hidup Ini Mudah.

Tetapi Alloh Berjanji, Bahwa Sesungguhnya Bersama Kesulitan Ada Kemudahan.

(Q.S Al-Insyirah : 5-6)

Dan Satu Lagi,

Alloh Tidak Membebani Seseorang Melainkan Sesuai Dengan Kesanggupannya.

(Q.S Al-Baqarah : 286)

"Jika Bukan Karena Alloh Yang Mampukan, Aku Mungkin Sudah Lama Menyerah."

KATA PENGANTAR

Alhamdulillahirabbil 'alamin, segala puji dan syukur penulis panjatkan kehadirat Allah SWT atas limpahan rahmat, kasih sayang, kesehatan, kekuatan, serta kemudahan yang diberikan sehingga penulis dapat menyelesaikan tesis yang berjudul "Analisis Mitigasi *Bufferbloat* Untuk Peningkatan *Quality Of Service* Pada Jaringan Pendidikan Berbasis *Mikrotik* (Studi Kasus Di SMKS Al-Islam Joresan Mlarak Ponorogo)" sebagai salah satu syarat untuk menyelesaikan pendidikan Magister pada Program Studi Magister PJJ Informatika.

Perjalanan dalam menyelesaikan tesis ini bukanlah perjalanan yang mudah. Banyak proses, tantangan, rasa lelah, keraguan, serta pengorbanan yang harus dilalui. Namun di balik semua itu, penulis menyadari bahwa ada begitu banyak doa, dukungan, bantuan, dan ketulusan dari orang-orang baik yang senantiasa hadir menguatkan langkah penulis hingga sampai pada titik ini. Oleh karena itu, dengan segala kerendahan hati, penulis menyampaikan rasa hormat dan terima kasih yang sebesar-besarnya kepada:

1. Bapak Prof. Dr. Mohammad Suyanto, M.M. beserta seluruh civitas akademika yang telah memberikan kesempatan, fasilitas, dan lingkungan akademik yang sangat berarti selama penulis menempuh pendidikan.
2. Bapak Dhani Ariatmanto, M.Kom., Ph.D. selaku Ketua Program Studi Magister PJJ Informatika yang telah memberikan dukungan, arahan, perhatian, serta motivasi kepada penulis selama menjalani masa studi hingga terselesaikannya tesis ini.
3. Bapak Hanif Al Fatta, S.Kom., M.Kom., Ph.D. selaku dosen pembimbing yang dengan penuh kesabaran, ketulusan, dan keikhlasan telah meluangkan waktu, tenaga, serta pikiran dalam membimbing penulis. Setiap masukan, arahan, dan ilmu yang diberikan menjadi pelajaran yang sangat berharga bagi penulis, bukan hanya dalam penyusunan tesis ini, tetapi juga dalam perjalanan akademik dan kehidupan.
4. Seluruh dosen yang telah memberikan ilmu pengetahuan, pengalaman, dan wawasan selama masa perkuliahan. Semoga segala ilmu yang diberikan menjadi amal jariyah dan manfaat yang terus mengalir.

5. Pihak SMKS Al-Islam Joresan Mlarak Ponorogo yang telah memberikan izin, dukungan, serta kesempatan kepada penulis untuk melaksanakan penelitian ini dengan baik.
6. Kedua orang tua tercinta, yang menjadi alasan terbesar penulis untuk terus berjuang. Terima kasih atas setiap doa yang tidak pernah putus, kasih sayang yang tulus, pengorbanan yang tidak terhitung, serta dukungan yang selalu menguatkan penulis dalam setiap keadaan. Tidak ada kata yang mampu menggambarkan betapa besar rasa terima kasih dan cinta penulis kepada kalian.
7. Istri tercinta, yang selalu hadir dengan doa, kesabaran, pengertian, dan dukungan tanpa lelah. Terima kasih karena selalu menjadi tempat pulang, tempat menguatkan, dan alasan penulis untuk tetap bertahan menyelesaikan setiap proses hingga tesis ini dapat terselesaikan dengan baik.
8. Rekan-rekan mahasiswa, sahabat seperjuangan, dan semua pihak yang tidak dapat disebutkan satu per satu, yang telah membantu, mendukung, serta memberikan semangat kepada penulis baik secara langsung maupun tidak langsung selama proses penyusunan tesis ini.

Penulis menyadari bahwa tesis ini masih jauh dari sempurna dan masih memiliki berbagai kekurangan. Oleh karena itu, penulis dengan terbuka menerima kritik dan saran yang membangun demi perbaikan di masa mendatang.

Akhir kata, penulis berharap semoga tesis ini dapat memberikan manfaat, menambah wawasan, serta menjadi kontribusi kecil bagi perkembangan ilmu pengetahuan, khususnya di bidang jaringan komputer dan *Quality Of Service (QoS)*.

Yogyakarta, 01 Juni 2026

Penulis.

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

INTISARI

Kualitas layanan jaringan komputer merupakan salah satu faktor penting dalam mendukung kegiatan pembelajaran dan administrasi di lingkungan pendidikan. Permasalahan yang sering terjadi pada jaringan sekolah adalah penggunaan *bandwidth* yang tidak terkontrol, tingginya trafik jaringan, serta belum adanya mekanisme pengelolaan prioritas layanan terhadap jenis trafik tertentu. Kondisi tersebut menyebabkan menurunnya performa jaringan, terutama ketika banyak pengguna mengakses *internet* secara bersamaan sehingga layanan seperti video *conference*, *VoIP*, dan akses pembelajaran daring menjadi kurang optimal.

Penelitian ini bertujuan untuk menganalisis mitigasi *Bufferbloat* untuk peningkatan *Quality Of Service (QoS)* pada jaringan pendidikan berbasis *Mikrotik*, dengan studi kasus di SMKS Al-Islam Joresan Mlarak Ponorogo. Fokus penelitian diarahkan pada penerapan *Packet Filtering* berdasarkan *IP Address*, *Port*, dan protokol jaringan yang diintegrasikan dengan mekanisme *QoS* menggunakan *packet marking*, *Queue Tree*, dan metode *Per Connection Queue (PCQ)*. Penelitian ini menitikberatkan pada pengaruh *Packet Filtering* terhadap kualitas layanan jaringan dan manajemen trafik. Metode penelitian yang digunakan adalah *Network Development Life Cycle (NDLC)* yang terdiri dari tahap *analysis*, *design*, *simulation prototype*, *implementation*, *monitoring*, dan *management*. Pengujian sistem dilakukan melalui tiga skenario eksperimen, yaitu skenario *Baseline* (tanpa *Packet Filtering* dan *QoS*), skenario penerapan *Packet Filtering*, serta skenario integrasi *Packet Filtering* dan *QoS*. Parameter pengukuran yang digunakan meliputi *Throughput*, *Delay*, *Jitter*, dan *Packet Loss*.

Hasil penelitian menunjukkan bahwa penerapan *Packet Filtering* dan *QoS* berbasis *Mikrotik* mampu meningkatkan kualitas layanan jaringan secara signifikan. Implementasi *packet marking* dan *Queue Tree* berhasil memberikan prioritas terhadap trafik penting seperti *VoIP* dan video *conference* sehingga nilai *Delay*, *Jitter*, dan *Packet Loss* menjadi lebih rendah dibandingkan kondisi awal jaringan. Selain itu, penggunaan metode *PCQ* mampu mendistribusikan *bandwidth* secara lebih merata kepada pengguna jaringan sehingga performa jaringan menjadi lebih stabil. Berdasarkan hasil analisis yang dilakukan, *konfigurasi* optimal diperoleh melalui kombinasi *Packet Filtering*, *mangle*, *Queue Tree*, dan *PCQ* dengan pengaturan prioritas trafik berdasarkan jenis layanan jaringan. Penelitian ini membuktikan bahwa integrasi *Packet Filtering* dan *QoS* dapat meningkatkan performa dan kualitas layanan jaringan secara efektif pada lingkungan pendidikan.

Kata Kunci: *Quality Of Service (QoS), Packet Filtering, Mikrotik, Queue Tree, PCQ, Manajemen Bandwidth.*

ABSTRACT

The quality of computer network services is a crucial factor in supporting learning and administrative activities in educational settings. Frequent problems in school networks include uncontrolled bandwidth usage, high network traffic, and the lack of a mechanism for managing service priorities for certain types of traffic. These conditions lead to decreased network performance, especially when many users access the internet simultaneously, resulting in suboptimal services such as video conferencing, VoIP, and online learning.

This research aims to analyze Bufferbloat mitigation to improve the Quality Of Service (QoS) in a Mikrotik-based educational network (a case study at SMKS Al-Islam Joresan Mlarak Ponorogo). The research focuses on the implementation of Packet Filtering based on IP addresses, ports, and network protocols, integrated with QoS mechanisms using packet marking, Queue Trees, and the Per Connection Queue (PCQ) method. This research does not specifically address network security but instead focuses on the impact of Packet Filtering on network service quality and traffic management. The research method used is the Network Development Life Cycle (NDLC), which consists of analysis, design, simulation, prototype, implementation, monitoring, and management.

System testing was conducted using three experimental scenarios: a baseline scenario without Packet Filtering and QoS, a scenario implementing Packet Filtering, and an integrated scenario with Packet Filtering and QoS. Measurement parameters used in this study included Throughput, Delay, Jitter, and Packet Loss.

The results showed that implementing Mikrotik-based Packet Filtering and QoS significantly improved network service quality. The implementation of packet marking and Queue Tree successfully prioritized critical traffic such as VoIP and video conferencing, resulting in lower Delay, Jitter, and Packet Loss compared to the initial network conditions. Furthermore, the use of the PCQ method distributed bandwidth more evenly among network users, resulting in more stable network performance. Based on the analysis, the optimal configuration was obtained through a combination of Packet Filtering, mangle, Queue Tree, and PCQ, with traffic prioritization based on the type of network service. This study demonstrates that the integration of Packet Filtering and QoS can effectively improve network service performance and quality in educational environments.

***Keywords**: Quality Of Service (QoS), Packet Filtering, Mikrotik, Queue Tree, PCQ, Bandwidth Management.*

BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi jaringan komputer dan meluasnya akses *internet* di lembaga pendidikan telah membawa perubahan fundamental dalam pola pembelajaran modern. Penggunaan platform *e-learning*, video *conference*, dan layanan berbasis cloud kini menjadi bagian tak terpisahkan dari proses belajar mengajar. Namun di balik pertumbuhan infrastruktur jaringan yang pesat, terdapat permasalahan teknis mendasar yang belum banyak diteliti secara mendalam di konteks pendidikan Indonesia, yaitu fenomena *Bufferbloat*.

Bufferbloat merupakan fenomena jaringan yang terjadi ketika buffer (antrian paket) di dalam perangkat jaringan seperti router mengalami kelebihan kapasitas sehingga menimbulkan latensi tinggi, *Jitter*, dan penurunan *Throughput* secara signifikan. Fenomena ini pertama kali dideskripsikan secara sistematis oleh Jim Gettys pada tahun 2010 dan terbukti menjadi salah satu penyebab utama degradasi kualitas layanan jaringan (*Quality Of Service*/QoS) pada berbagai infrastruktur *internet* dunia. Ironisnya, *Bufferbloat* seringkali tidak teridentifikasi karena pengguna hanya melihat kapasitas bandwidth tanpa memperhatikan perilaku antrian paket di dalam router (Gettys & Nichols, 2012).

Dalam konteks jaringan pendidikan, masalah *Bufferbloat* memiliki dampak langsung terhadap kualitas pengalaman belajar (*Quality of Experience/QoE*) pengguna. Ketika banyak pengguna mengakses layanan real-time seperti Zoom, Google Meet, atau sistem *e-learning* secara bersamaan, buffer router yang tidak dikelola dengan baik akan terisi penuh oleh paket-paket yang menunggu transmisi. Kondisi ini mengakibatkan peningkatan *Delay* dan *Jitter* yang tajam, meskipun kapasitas bandwidth jalur tersebut secara nominal mencukupi. Fenomena inilah yang membedakan permasalahan *Bufferbloat* dari sekadar kekurangan bandwidth biasa.

Penelitian-penelitian terdahulu di bidang mitigasi *Bufferbloat* umumnya dilakukan pada konteks jaringan umum atau backbone ISP. *Active Queue Management (AQM)* seperti *CoDel (Controlled Delay)*, *FQ-CoDel* (Fair Queuing-CoDel), dan *CAKE (Common Applications Kept Enhanced)* telah terbukti efektif menekan latensi akibat *Bufferbloat* pada skala jaringan besar. Namun demikian, penelitian tentang penerapan mitigasi *Bufferbloat* secara spesifik pada jaringan pendidikan di Indonesia, khususnya menggunakan perangkat *Mikrotik* yang merupakan pilihan utama administrator jaringan sekolah di negeri ini, masih sangat terbatas (Nichols & Jacobson, 2012; Hoiland-Jørgensen et al., 2018).

Kesenjangan riset yang menjadi dasar penelitian ini adalah belum adanya studi empiris yang secara eksplisit mengidentifikasi dan mengukur fenomena *Bufferbloat* pada jaringan pendidikan berbasis *Mikrotik* di Indonesia. Kemudian belum diketahuinya efektivitas kombinasi *Packet Filtering*, packet marking, dan *Queue Tree* sebagai mekanisme mitigasi *Bufferbloat* dalam konteks jaringan sekolah menengah kejuruan. Serta ketiadaan framework operasional yang dapat dijadikan acuan praktis oleh administrator jaringan sekolah dalam menangani *Bufferbloat*. Penelitian ini hadir untuk mengisi kesenjangan tersebut dengan mengambil studi kasus di SMKS Al-Islam Joresan Mlarak Ponorogo sebagai representasi tipikal jaringan pendidikan menengah kejuruan di Indonesia.

SMKS Al-Islam Joresan Mlarak Ponorogo dipilih sebagai lokasi studi karena memiliki karakteristik jaringan yang representatif: menggunakan Router *Mikrotik* sebagai pusat manajemen jaringan, memiliki pengguna simultan dengan kebutuhan layanan yang heterogen (administrasi, pembelajaran daring, multimedia), serta mengalami gejala-gejala yang secara teknis dapat dikaitkan dengan fenomena *Bufferbloat*. Gejala tersebut meliputi ketidakstabilan koneksi pada jam padat, tingginya latensi pada layanan real-time, dan penurunan *Throughput* yang tidak proporsional terhadap penggunaan bandwidth total.

Dengan menempatkan permasalahan teknis jaringan di sekolah ini sebagai manifestasi konkret dari fenomena *Bufferbloat* yang telah banyak diteliti di literatur internasional, penelitian ini berupaya memberikan kontribusi empiris yang menjembatani teori mitigasi *Bufferbloat* dengan praktik administrasi jaringan pendidikan di Indonesia. Hasil penelitian diharapkan dapat digeneralisasikan ke institusi pendidikan lain dengan karakteristik jaringan yang serupa, mengingat dominasi penggunaan *Mikrotik* di sekolah-sekolah Indonesia.

1.2 Identifikasi Masalah

Berdasarkan kajian literatur tentang *Bufferbloat* dan kondisi jaringan di SMKS Al-Islam Joresan Mlarak Ponorogo sebagai representasi jaringan pendidikan, terdapat beberapa permasalahan yang diidentifikasi:

1. Fenomena *Bufferbloat* pada jaringan pendidikan berbasis *Mikrotik* belum mendapat perhatian riset yang memadai di Indonesia, padahal dampaknya langsung memengaruhi kualitas pembelajaran daring.
2. Belum terdapat studi empiris tentang efektivitas kombinasi *Packet Filtering* dan *Queue Tree* sebagai mekanisme mitigasi *Bufferbloat* pada infrastruktur *Mikrotik* di lingkungan pendidikan.
3. Ketiadaan benchmark kuantitatif yang dapat menjadi acuan pengukuran peningkatan QoS setelah penerapan mitigasi *Bufferbloat* pada jaringan sekolah.
4. Belum tersedianya framework praktis mitigasi *Bufferbloat* yang dapat diadopsi oleh administrator jaringan sekolah tanpa memerlukan infrastruktur yang kompleks.

1.3 Rumusan Masalah

Berdasarkan identifikasi masalah yang telah dijelaskan, penelitian ini difokuskan pada analisis pengaruh *Packet Filtering* terhadap *Quality Of Service (QoS)* pada jaringan *Mikrotik*. Adapun rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Bagaimana fenomena *Bufferbloat* termanifestasi pada parameter QoS (*Throughput*, *Delay*, *Jitter*, *Packet Loss*) jaringan pendidikan berbasis *Mikrotik* pada kondisi baseline?
2. Seberapa besar peningkatan parameter QoS yang dicapai melalui implementasi *Packet Filtering* sebagai tahap pertama mitigasi *Bufferbloat*?
3. Seberapa besar peningkatan parameter QoS yang dicapai melalui kombinasi QoS (packet marking + *Queue Tree* + PCQ) dan *Packet Filtering* sebagai mitigasi *Bufferbloat* yang komprehensif?
4. Bagaimana framework mitigasi *Bufferbloat* berbasis *Mikrotik* yang optimal untuk jaringan pendidikan menengah kejuruan di Indonesia?

1.4 Batasan Masalah

Agar penelitian lebih terarah dan tidak menyimpang dari tujuan yang telah ditentukan, maka penelitian ini dibatasi pada beberapa hal berikut:

1. Penelitian dilakukan pada jaringan *internet* SMKS Al-Islam Joresan Mlarak Ponorogo menggunakan Router *Mikrotik* sebagai representasi tipikal jaringan pendidikan.
2. Mekanisme mitigasi *Bufferbloat* yang diuji adalah *Packet Filtering*, packet marking, *Queue Tree*, dan *Per Connection Queue (PCQ)* pada platform RouterOS *Mikrotik*.
3. Parameter QoS yang diukur meliputi *Throughput*, *Delay*, *Jitter*, dan *Packet Loss* berdasarkan standar TIPHON.
4. Perbandingan kuantitatif dilakukan pada tiga skenario Baseline (tanpa mitigasi), Filtering, dan QoS+Filtering.

1.5 Tujuan Penelitian

Penelitian ini bertujuan untuk menganalisis dan meningkatkan kualitas layanan jaringan menggunakan metode *Packet Filtering* dan *QoS* berbasis *Mikrotik*. Adapun tujuan penelitian ini adalah sebagai berikut:

1. Mengidentifikasi dan mengukur dampak *Bufferbloat* terhadap parameter QoS pada jaringan pendidikan berbasis *Mikrotik* dalam kondisi baseline.
2. Menganalisis dan mengkuantifikasi efektivitas *Packet Filtering* sebagai mekanisme mitigasi *Bufferbloat* tahap pertama.

3. Menganalisis dan mengkuantifikasi efektivitas kombinasi QoS+Filtering sebagai mitigasi *Bufferbloat* yang komprehensif.
4. Membangun framework mitigasi *Bufferbloat* berbasis *Mikrotik* yang dapat digeneralisasikan pada jaringan pendidikan lain.

1.6 Manfaat Penelitian

Penelitian mengenai pengaruh *Packet Filtering* terhadap *Quality Of Service (QoS)* pada jaringan *Mikrotik* ini diharapkan dapat memberikan manfaat baik secara teoritis maupun praktis. Adapun manfaat penelitian ini adalah sebagai berikut:

1. Memberikan bukti empiris tentang fenomena *Bufferbloat* pada jaringan pendidikan Indonesia dan menguji efektivitas mekanisme mitigasinya yang dapat memperkaya literatur jaringan komputer berbahasa Indonesia.
2. Mengembangkan protokol pengukuran *Bufferbloat* yang terstandar untuk konteks jaringan pendidikan berbasis *Mikrotik*.
3. Menyediakan framework mitigasi *Bufferbloat* yang dapat diadopsi oleh administrator jaringan di berbagai institusi pendidikan menengah di Indonesia.

1.7 Hipotesis

Berdasarkan rumusan masalah yang telah ditetapkan, maka hipotesis dalam penelitian ini adalah sebagai berikut:

1. Penerapan *Packet Filtering* dan QoS berbasis *Mikrotik* tidak memberikan perbaikan yang signifikan terhadap parameter QoS yang berkaitan dengan *Bufferbloat Throughput*, *Delay*, *Jitter*, *Packet Loss*.
2. Penerapan *Packet Filtering* dan QoS berbasis *Mikrotik* memberikan perbaikan yang signifikan terhadap parameter QoS yang berkaitan dengan *Bufferbloat*, dengan peningkatan *Throughput* minimal 20%, penurunan *Delay* minimal 10%, penurunan *Jitter* minimal 15%, dan penurunan *Packet Loss* minimal 40% dibandingkan kondisi baseline.

BAB II
TINJAUAN PUSTAKA

2.1 Tinjauan Pustaka

Bufferbloat adalah fenomena jaringan di mana buffer yang terlalu besar pada perangkat jaringan router, switch menyebabkan latensi yang tidak wajar tinggi dan penurunan *Throughput* ketika terjadi kongest. Fenomena ini secara teknis disebabkan oleh mekanisme TCP congestion avoidance yang terganggu: ketika buffer router terisi penuh, paket TCP menunggu terlalu lama dalam antrian sebelum akhirnya dibuang, sehingga sinyal kongesti yang dibutuhkan TCP untuk menyesuaikan window size datang terlambat. Akibatnya, pengirim terus menyuntikkan paket ke jaringan yang sudah jenuh, menciptakan siklus umpan balik negatif yang memperparah latensi (Gettys, 2011).

Penelitian yang dilakukan oleh Fani Nabhan Zaki dan Lukman pada tahun 2021 membahas analisis perbandingan *QoS* pada layanan video *streaming* menggunakan metode *Per Connection Queue (PCQ)* dan *Hierarchical Token Bucket (HTB)* pada *Router Mikrotik*. Penelitian ini menitikberatkan pada pengelolaan *bandwidth* untuk meningkatkan kualitas layanan video *streaming* pada jaringan wireless. Parameter *QoS* yang dianalisis meliputi *Delay*, *Throughput*, *Jitter*, dan *Packet Loss*. Hasil penelitian menunjukkan bahwa metode *HTB* dan *PCQ* mampu meningkatkan stabilitas distribusi *bandwidth* sehingga performa video *streaming* menjadi lebih optimal dan efisien dalam penggunaan jaringan *internet*. Penelitian ini juga menjelaskan bahwa pengaturan lalu lintas data melalui mekanisme manajemen *bandwidth* memiliki hubungan erat dengan konsep *Packet Filtering* karena sistem melakukan pengendalian terhadap trafik yang melewati *Router* berdasarkan aturan tertentu (Zaki & Lukman, 2021).

Pada jaringan universitas menggunakan AQM berbasis panjang antrian menunjukkan bahwa kehadiran mekanisme manajemen antrian aktif dapat secara signifikan menurunkan latensi meskipun jaringan beroperasi mendekati kapasitas penuh. Studi ini dilaksanakan di jaringan nyata kampus dengan mengukur performansi sebelum dan sesudah implementasi AQM, memberikan

baseline empiris yang relevan dengan konteks penelitian ini (Barczyk & Chydzinski, 2022).

Selanjutnya, penelitian yang dilakukan oleh Nurnaningsih, Riskayani, dan Anniar Husnang pada tahun 2022 membahas analisis keamanan jaringan *hotspot* menggunakan parameter *QoS* pada Kantor Dinas Komunikasi dan Informatika Kabupaten Soppeng. Penelitian ini berfokus pada pengukuran kualitas keamanan jaringan *hotspot* melalui parameter *QoS* seperti *latency* dan *Throughput*. Hasil penelitian menunjukkan bahwa kualitas jaringan *hotspot* pada jam sibuk maupun tidak sibuk masih tergolong baik serta sistem keamanan jaringan mampu mencegah tindakan *sniffing*. Penelitian ini menegaskan bahwa pengamanan jaringan tidak hanya bergantung pada sistem autentikasi, tetapi juga pada pengaturan lalu lintas paket data yang baik melalui teknik *Packet Filtering* untuk mencegah akses ilegal dan serangan terhadap jaringan *hotspot* (Husnang Anniar, 2022).

Pada tahun 2023, Rizal Abdul Rosid, Martanto, dan Irfan Ali melakukan penelitian mengenai analisis performa jaringan *internet* menggunakan parameter *QoS* di lingkungan SMK Al-Ma'rifah. Penelitian ini menggunakan aplikasi *Wireshark* untuk melakukan proses *capture packet* dan analisis terhadap parameter *Throughput*, *Delay*, *Packet Loss*, dan *Jitter* berdasarkan standar TIPHON. Hasil penelitian menunjukkan bahwa jaringan *internet* yang dianalisis memiliki kategori sangat baik dengan nilai *Throughput* tinggi, *Packet Loss* sebesar 0%, dan nilai *Delay* yang rendah. Penelitian ini menunjukkan bahwa monitoring lalu lintas jaringan menggunakan *Wireshark* dapat membantu administrator jaringan dalam melakukan pengawasan trafik sekaligus mendeteksi paket data yang tidak sesuai, sehingga konsep *PACKET FILTERING* dapat diterapkan untuk mengontrol paket-paket tertentu agar kualitas jaringan tetap stabil (Rosid et al., 2023).

Masih pada tahun 2023, penelitian yang dilakukan oleh Valia Yoga Pudya Ardhana dan M. Dermawan Mulyodiputro membahas analisis *QoS* jaringan *internet* universitas menggunakan metode *HTB*. Penelitian ini menitikberatkan pada penerapan manajemen *bandwidth* menggunakan metode

HTB untuk mengoptimalkan distribusi *bandwidth* pada lingkungan kampus. Parameter *QoS* yang digunakan terdiri dari *Delay*, *Jitter*, *Packet Loss*, dan *Throughput*. Hasil penelitian menunjukkan bahwa penerapan *HTB* menghasilkan nilai *QoS* sebesar 3,67 dengan kategori memuaskan berdasarkan standar TIPHON. Penelitian ini juga menjelaskan bahwa metode *HTB* bekerja dengan teknik antrean dan pembagian *bandwidth* berdasarkan prioritas pengguna, sehingga secara tidak langsung menerapkan mekanisme *Packet Filtering* terhadap lalu lintas jaringan sesuai aturan yang telah ditentukan administrator jaringan (Valia Yoga Pudya Ardhana & Mulyodiputro, 2023).

Penelitian terbaru dilakukan oleh Mas Nurul Hamidah, Rahmawati Febrifyaning Tias, dan Rifki Fahrial Zainal pada tahun 2024 mengenai analisis *QoS* menggunakan *Wireshark* pada jaringan LAN di SMA An Najiyah Surabaya. Penelitian ini menggunakan parameter *QoS* berupa *Throughput*, *Delay*, dan *Packet Loss* untuk mengukur kualitas jaringan LAN yang digunakan dalam kegiatan pembelajaran daring. Hasil penelitian menunjukkan bahwa jaringan memiliki kualitas sangat baik dengan nilai *Throughput* sebesar 2,6 Mbps, *Packet Loss* 0%, dan *Delay* sebesar 0,12 ms. Penelitian ini menegaskan bahwa monitoring jaringan menggunakan *Wireshark* sangat efektif dalam mengidentifikasi kualitas layanan jaringan serta mendukung implementasi *Packet Filtering* dalam pengendalian trafik jaringan agar distribusi data lebih stabil dan terhindar dari kemacetan lalu lintas data (*network congestion*) (Wardhana et al., 2024).

Di Indonesia, perkembangan riset tentang *Bufferbloat* pada jaringan pendidikan mulai tampak. Menerapkan PCQ dan FQ_CoDel pada jaringan berbasis *Mikrotik* dan membuktikan peningkatan QoS yang signifikan. Penelitian serupa dilakukan oleh Tiawan et al. (2024) pada jaringan WiFi hotspot sekolah. Namun demikian, mayoritas penelitian tersebut belum secara eksplisit mengidentifikasi dan mengukur *Bufferbloat* sebagai variabel independen—penelitian ini hadir untuk mengisi gap tersebut (Gumeular & Akbi, 2025).

Penelitian mengenai *Quality Of Service (QoS)* dan *Packet Filtering*

berkembang pesat seiring meningkatnya kebutuhan akan kualitas jaringan *internet* yang stabil, aman, dan efisien. *QoS* digunakan sebagai metode untuk mengukur performa jaringan berdasarkan parameter seperti *Throughput, Delay*, *Jitter*, dan *Packet Loss*, sedangkan *Packet Filtering* digunakan untuk mengatur, menyaring, dan mengontrol lalu lintas paket data agar kualitas jaringan tetap optimal. Berbagai penelitian terdahulu menunjukkan bahwa penerapan *QoS* yang dikombinasikan dengan teknik pengelolaan trafik dan *Packet Filtering* mampu meningkatkan stabilitas jaringan serta efisiensi penggunaan *bandwidth* (Hawari, 2025).

Penelitian yang dilakukan oleh Frans Boy Laim, Djami Olii, dan Rudy Harijadi Wibowo Pardanus pada tahun 2025 membahas analisis *Quality Of Service (QoS)* pada jaringan *internet* di SMK Kristen 1 Tomohon menggunakan metode *NDLC (Network Development Life Cycle)*. Penelitian ini menggunakan parameter *Throughput*, *Packet Loss*, *Delay*, dan *Jitter* untuk menganalisis kualitas jaringan *internet* di laboratorium komputer sekolah. Hasil penelitian menunjukkan bahwa nilai *Packet Loss* berada pada kategori sangat baik, sedangkan nilai *Throughput* berada pada kategori cukup. Penelitian ini juga menegaskan bahwa proses monitoring jaringan menggunakan *Wireshark* sangat membantu dalam mendeteksi gangguan jaringan sehingga administrator dapat melakukan pengelolaan trafik dan *Packet Filtering* untuk menjaga kestabilan jaringan *internet* di lingkungan sekolah (Hawari, 2025).

Selanjutnya, penelitian yang dilakukan oleh Rizki Dwi Sanjaya, Dian Syamdova, Muhammad Farhan, dan Ryan Putra Laksana pada tahun 2025 membahas analisis parameter *QoS* pada jaringan *internet* di Perpustakaan Universitas Esa Unggul Tangerang. Penelitian ini berfokus pada pengukuran parameter *Throughput*, *Packet Loss*, *Delay*, dan *Jitter* guna mengevaluasi kualitas layanan jaringan *internet* di lingkungan akademik. Hasil penelitian menunjukkan bahwa nilai *Throughput* masih tergolong buruk, sedangkan *Packet Loss*, *Delay*, dan *Jitter* berada pada kategori sangat baik. Penelitian ini menyimpulkan bahwa rendahnya *Throughput* menjadi kendala utama sehingga

diperlukan optimalisasi *bandwidth* dan pengaturan lalu lintas jaringan melalui mekanisme *QoS* dan *Packet Filtering* untuk meningkatkan kualitas layanan *internet* di perpustakaan universitas (Unggul, 2025).

Penelitian berikutnya dilakukan oleh Dimas Arya Mukhti, Yasinta Bella Fitrianan, Doddy Teguh Yuwono, dan Yunanri W. pada tahun 2025 mengenai analisis kinerja layanan *RT/RW.Net* Robby Media berbasis *hotspot* menggunakan metode *QoS*. Penelitian ini menggunakan metode NDLC untuk menganalisis kualitas jaringan *RT/RW.Net* berdasarkan parameter *QoS*. Hasil penelitian menunjukkan bahwa nilai *Throughput* jaringan tergolong sangat baik, tetapi *Packet Loss* masih berada pada kategori sedang hingga buruk sehingga memengaruhi stabilitas koneksi *internet* pengguna. Penelitian ini menekankan pentingnya penerapan *QoS* dan pengelolaan *bandwidth* melalui teknik *Packet Filtering* serta penjadwalan trafik jaringan untuk mengurangi gangguan koneksi dan meningkatkan kualitas layanan *internet* pada jaringan *RT/RW.Net* (Mukhti et al., 2025).

Penelitian lain dilakukan oleh Indar Kusmanto, Hidayat, dan Zaid Al Khair pada tahun 2025 yang membahas analisis perbandingan kualitas jaringan *internet IndiHome* dan Iconnet berdasarkan metode *QoS*. Penelitian ini menggunakan parameter *Throughput*, *Delay*, *Jitter*, dan *Packet Loss* untuk membandingkan kualitas layanan kedua ISP. Hasil penelitian menunjukkan bahwa *IndiHome* memiliki performa jaringan yang lebih stabil dibandingkan Iconnet, terutama pada parameter *Jitter*. Selain itu, kedua ISP memiliki kualitas sangat baik pada parameter *Throughput*, *Packet Loss*, dan *Delay*. Penelitian ini menjelaskan bahwa pengelolaan lalu lintas data menggunakan *QoS* dapat membantu proses pengaturan paket data melalui *Packet Filtering* sehingga distribusi *bandwidth* menjadi lebih stabil dan efisien sesuai kebutuhan pengguna jaringan (Kusmanto & Al, 2025).

Penelitian yang dilakukan oleh Ramadhani Bagus Satrio Wibowo dan Yuli Komalasari pada tahun 2025 membahas penerapan *Quality Of Service* menggunakan metode *Hierarchical Token Bucket (HTB)* pada jaringan *internet* di PT. Triwall Indonesia. Penelitian ini bertujuan untuk mengoptimalkan

pembagian *bandwidth* menggunakan metode *HTB* pada *Router Mikrotik*. Hasil penelitian menunjukkan bahwa metode *HTB* mampu mengatur distribusi *bandwidth* secara lebih adil dan terstruktur sehingga kualitas jaringan menjadi lebih stabil. Penelitian ini juga menjelaskan bahwa teknik *Queue Tree* dan packet mark pada *Mikrotik* berfungsi sebagai mekanisme *Packet Filtering* yang dapat mengatur prioritas paket data berdasarkan jenis trafik tertentu sehingga performa jaringan dapat dipertahankan dalam kondisi optimal (Wibowo & Komalasari, 2025).

Selanjutnya, penelitian yang dilakukan oleh Agil Saputra, Yunanri W., dan I Made Widiarta pada tahun 2025 membahas analisis perbandingan jaringan *internet* pada layanan ISP menggunakan metode *QoS*. Penelitian ini membandingkan performa layanan *internet IndiHome* dan *NetHome* berdasarkan parameter *QoS* seperti *Throughput*, *Delay*, dan *Packet Loss*. Hasil penelitian menunjukkan bahwa *NetHome* memiliki nilai *Packet Loss* lebih rendah, sedangkan *IndiHome* memiliki *Throughput* yang lebih stabil. Penelitian ini menyatakan bahwa penerapan *QoS* yang baik perlu didukung oleh pengaturan trafik jaringan dan *Packet Filtering* agar lalu lintas data dapat berjalan lebih optimal dan mampu meminimalkan gangguan koneksi *internet* pengguna (Saputra et al., 2025).

Penelitian terbaru dilakukan oleh O.K. Muhammad Majid Maulana, Asrianda, dan Muhammad Fikry pada tahun 2025 mengenai analisis perbandingan algoritma antrean tradisional dan modern pada *Mikrotik RouterOS* v7 untuk optimasi *QoS* jaringan broadband. Penelitian ini membandingkan algoritma SFQ, *PCQ*, *FQ-CoDel*, dan *CAKE* menggunakan parameter *QoS* berupa *Throughput*, *Delay*, *Jitter*, dan *Packet Loss*. Hasil penelitian menunjukkan bahwa algoritma modern seperti *FQ-CoDel* dan *CAKE* mampu menghasilkan kualitas jaringan yang lebih baik dibandingkan algoritma tradisional karena mampu menjaga latensi tetap rendah dan mengurangi *Packet Loss*. Penelitian ini juga menegaskan bahwa implementasi *Active Queue Management (AQM)* dan web filtering merupakan bentuk *Packet Filtering* modern yang efektif dalam mengontrol lalu lintas data serta

mengurangi kemacetan jaringan (*Bufferbloat*) pada jaringan broadband (Safira Safra, 2025).

Quality Of Service (QoS) merupakan suatu metode yang digunakan untuk mengukur, mengontrol, dan mengevaluasi kualitas layanan pada jaringan komputer berdasarkan beberapa parameter utama, yaitu *Throughput, Delay*, *Jitter*, dan *Packet Loss*. *QoS* digunakan untuk memastikan bahwa proses pengiriman data pada jaringan dapat berjalan dengan baik, stabil, cepat, dan sesuai dengan kebutuhan pengguna maupun aplikasi yang digunakan. Berdasarkan penjelasan tersebut dapat disimpulkan bahwa *Quality Of Service (QoS)* merupakan mekanisme penting dalam jaringan komputer yang digunakan untuk mengukur dan menjaga kualitas layanan jaringan agar tetap stabil, efisien, dan mampu mendukung berbagai kebutuhan komunikasi digital secara optimal (Samosir et al., 2026).

2.2 Keaslian Penelitian

Tabel 2.2 Matriks Literatur Review Dan Posisi Penelitian

Analisis Mitigasi *Bufferbloat* Untuk Peningkatan *Quality Of Service* Pada Jaringan Pendidikan Berbasis *Mikrotik* (Studi Kasus Di SMKS Al-Islam Joresan Mlarak Ponorogo)

No	Judul	Peneliti, Media Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
1	Analisis Perbandingan *QoS* Video *Streaming* Menggunakan Metode *PCQ* dan *HTB* pada *Router Mikrotik*	Fani Nabhan Zaki & Lukman, Jurnal Jaringan Komputer, 2021	Menganalisis perbandingan metode *PCQ* dan *HTB* terhadap kualitas layanan video *streaming* pada jaringan wireless.	Metode *HTB* dan *PCQ* mampu meningkatkan stabilitas *bandwidth* serta mengoptimalkan layanan video *streaming*.	Belum membahas *Bufferbloat* dan mitigasinya.	Penelitian ini berfokus pada mitigasi *Bufferbloat* dan pengaruhnya terhadap QoS jaringan pendidikan.
2	AQM Based on the Queue Length: A Real-Network Study	Marek Barczyk dan Andrzej Chydzinski, Jurnal PLoS ONE, 2022	Menganalisis efektivitas berbagai algoritma *Active Queue Management (AQM)* berbasis queue length dalam mengurangi *Buffierbloat* pada jaringan kampus nyata.	Implementasi AQM mampu menurunkan queue length, *Delay*, dan burst loss secara signifikan dibandingkan FIFO tanpa AQM. Seluruh fungsi dropping non-trivial (d1–d7) memberikan peningkatan performa jaringan yang signifikan.	Penelitian hanya berfokus pada implementasi AQM berbasis dropping function dan belum mengkaji mekanisme QoS lain seperti traffic classification, packet marking, *Queue Tree*, maupun PCQ. Penulis juga menyarankan pengujian pada jaringan lain dan analisis per-flow.	Penelitian ini menggunakan AQM pada perangkat Linux-DPDK dalam jaringan kampus. Sedangkan tesis yang diusulkan menggunakan perangkat *Mikrotik* pada jaringan pendidikan sekolah menengah dan menerapkan mitigasi *Bufferbloat* secara bertahap melalui *Packet Filtering*, packet marking, *Queue Tree*, dan PCQ. Selain mengukur queue length dan loss, tesis juga mengevaluasi

No	Judul	Peneliti, Media Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
						QoS berdasarkan *Throughput*, *Delay*, *Jitter*, dan *Packet Loss* sesuai standar TIPHON.
3	Analisis Keamanan Jaringan *Hotspot* Menggunakan Parameter *QoS* pada Diskominfo Kabupaten Soppeng	Nurnaningsih, Riskayani, & Anniar Husnang, Jurnal Teknologi Informasi, 2022	Mengukur kualitas keamanan jaringan *hotspot* menggunakan parameter *QoS*.	Kualitas jaringan *hotspot* tergolong baik dan mampu mencegah *sniffing* pada jaringan.	Fokus pada keamanan jaringan, bukan *Bufferbloat*.	Penelitian ini fokus pada peningkatan QoS melalui mitigasi *Bufferbloat*.
4	Analisis Performa Jaringan *Internet* Menggunakan Parameter *QoS* di SMK Al-Ma'rifah	Rizal Abdul Rosid, Martanto, & Irfan Ali, Jurnal Sistem Informasi, 2023	Menganalisis performa jaringan *internet* menggunakan parameter *QoS* dengan bantuan *Wireshark*.	Jaringan memiliki *Throughput* tinggi, *Delay* rendah, dan *Packet Loss* 0% sehingga termasuk kategori sangat baik.	Hanya monitoring QoS tanpa optimasi jaringan.	Penelitian ini tidak hanya mengukur QoS tetapi juga menerapkan mitigasi *Bufferbloat*.
5	Analisis *QoS* Jaringan *Internet* Universitas Menggunakan Metode *HTB*	Valia Yoga Pudya Ardhana & M. Dermawan Mulyodiputro, Jurnal Informatika, 2023	Mengoptimalkan distribusi *bandwidth* menggunakan metode *HTB* pada jaringan universitas.	*HTB* menghasilkan kualitas jaringan memuaskan berdasarkan standar TIPHON.	Tidak membahas *Bufferbloat* maupun antrean jaringan.	Penelitian ini mengkaji *Bufferbloat* sebagai penyebab utama penurunan QoS.
6	Analisis *QoS* Menggunakan *Wireshark* pada	Mas Nurul Hamidah, Rahmawati	Mengukur kualitas jaringan LAN menggunakan	Jaringan memiliki kualitas sangat baik dengan *Throughput*	Tidak melakukan perbaikan atau mitigasi jaringan.	Penelitian ini melakukan analisis sekaligus mitigasi *Bufferbloat*.

No	Judul	Peneliti, Media Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
	Jaringan LAN di SMA An Najiyah Surabaya	Febrifyaning Tias, & Rifki Fahrial Zainal, Jurnal Komputer dan Jaringan, 2024	*Wireshark* berdasarkan parameter *QoS*.	tinggi dan *Packet Loss* 0%.		
7	Optimalisasi QoS Manajemen Bandwidth Menggunakan PCQ dan FQ_Codel Berbasis *Mikrotik*	Muhammad Jihan Gumcular dan Denar Regata Akbi, Jurnal REPOSITOR Vol. 7 No. 2, 2025	Mengoptimalkan *Quality Of Service* (QoS) pada jaringan *internet* menggunakan metode PCQ dan FQ_Codel berbasis *Mikrotik* untuk mengatasi distribusi bandwidth yang tidak merata dan koneksi *internet* lambat.	Implementasi PCQ dan FQ_Codel berhasil meningkatkan kualitas layanan *internet*. *Throughput* meningkat dari 2.500 Kbps menjadi 3.258 Kbps, *Packet Loss* turun dari 0,75% menjadi 0,2%, *Jitter* turun dari 8,8 ms menjadi 2–3 ms, dan latency turun dari 9,9 ms menjadi 2,5 ms. QoS jaringan masuk kategori sangat baik.	Penelitian berfokus pada optimalisasi bandwidth di lingkungan kost dan belum menganalisis fenomena *Bufferbloat* secara khusus. Tidak dilakukan pengukuran kondisi baseline *Bufferbloat* maupun mitigasi bertahap. Pengujian hanya membandingkan sebelum dan sesudah penerapan PCQ-FQ_Codel.	Penelitian ini secara khusus mengukur dan memitigasi *Bufferbloat* melalui beberapa tahapan konfigurasi *Mikrotik*.
8	Kajian Perkembangan *QoS* dan *Packet Filtering* pada Jaringan Komputer	Hawari, Artikel Ilmiah Teknologi Jaringan, 2025	Mengkaji perkembangan implementasi *QoS* dan *Packet Filtering* pada jaringan modern.	*QoS* dan *Packet Filtering* terbukti mampu meningkatkan stabilitas jaringan dan efisiensi *bandwidth*.	Tidak ada implementasi dan pengujian nyata.	Penelitian ini melakukan implementasi langsung pada jaringan sekolah.

No	Judul	Peneliti, Media Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
9	Analisis *QoS* pada Jaringan *Internet* di SMK Kristen 1 Tomohon Menggunakan Metode NDLC	Frans Boy Laim, Djami Olii, & Rudy Harijadi Wibowo Pardanus, Jurnal Teknologi Informasi, 2025	Menganalisis kualitas jaringan *internet* sekolah menggunakan metode NDLC.	*Packet Loss* sangat baik, namun *Throughput* masih cukup.	Belum melakukan optimasi jaringan berbasis *Bufferbloat*.	Penelitian ini menerapkan strategi mitigasi *Bufferbloat* dan mengukur hasilnya.
10	Analisis Parameter *QoS* pada Jaringan *Internet* di Perpustakaan Universitas Esa Unggul Tangerang	Rizki Dwi Sanjaya, Dian Syamdova, Muhammad Farhan, & Ryan Putra Laksana, Jurnal Sistem Komputer, 2025	Mengevaluasi kualitas jaringan *internet* perpustakaan menggunakan parameter *QoS*.	*Throughput* masih rendah sedangkan parameter lainnya sangat baik.	Tidak dilakukan tindakan optimasi jaringan.	Penelitian ini mengevaluasi sekaligus meningkatkan QoS melalui mitigasi *Bufferbloat*.
11	Analisis Kinerja Layanan *RT/RW.Net* Robby Media Menggunakan Metode *QoS*	Dimas Arya Mukhti, Yasinta Bella Fitrianan, Doddy Teguh Yuwono, & Yunanri W., Jurnal Telekomunikasi, 2025	Menganalisis kualitas jaringan *RT/RW.Net* berbasis *hotspot* menggunakan *QoS*.	*Throughput* sangat baik namun *Packet Loss* masih tinggi sehingga koneksi kurang stabil.	Tidak membahas *Bufferbloat* maupun mekanisme mitigasi.	Penelitian ini berfokus pada mitigasi *Bufferbloat* sebagai solusi peningkatan QoS.
12	Analisis Perbandingan Kualitas Jaringan	Indar Kusmanto, Hidayat, & Zaid	Membandingkan kualitas layanan dua	*IndiHome* lebih stabil dibandingkan Iconnet	Tidak melakukan konfigurasi atau optimasi jaringan.	Penelitian ini melakukan konfigurasi *Mikrotik* untuk mengurangi *Bufferbloat*.

No	Judul	Peneliti, Media Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
	Internet IndiHome dan Iconnet Berdasarkan *QoS*	Al Khair, Jurnal Teknologi Komunikasi, 2025	ISP menggunakan parameter *QoS*.	terutama pada parameter *Jitter*.		
13	Penerapan *QoS* Menggunakan Metode *HTB* pada Jaringan *Internet* PT. Triwall Indonesia	Ramadhani Bagus Satrio Wibowo & Yuli Komalasari, Jurnal Informatika Industri, 2025	Mengoptimalkan pembagian *bandwidth* menggunakan metode *HTB* pada *Mikrotik*.	*HTB* mampu mengatur *bandwidth* lebih adil dan stabil.	Tidak membahas *Bufferbloat* dan AQM.	Penelitian ini mengintegrasikan mitigasi *Bufferbloat* dengan manajemen trafik *Mikrotik*.
14	Analisis Perbandingan Jaringan *Internet* pada Layanan ISP Menggunakan *QoS*	Agil Saputra, Yunanri W., & I Made Widiarta, Jurnal Rekayasa Jaringan, 2025	Membandingkan performa jaringan *internet* beberapa ISP menggunakan *QoS*.	*NetHome* unggul pada *Packet Loss* sedangkan *IndiHome* lebih stabil pada *Throughput*.	Tidak mengimplementasikan solusi jaringan.	Penelitian ini menerapkan solusi teknis untuk meningkatkan QoS.
15	Analisis Perbandingan Algoritma Antrean Tradisional dan Modern pada *Mikrotik RouterOS* v7	O.K. Muhammad Majid Maulana, Asrianda, & Muhammad Fikry, Jurnal Broadband Network, 2025	Membandingkan algoritma SFQ, *PCQ*, *FQ-CoDel*, dan *CAKE* terhadap kualitas *QoS* jaringan broadband.	Algoritma modern seperti *FQ-CoDel* dan *CAKE* memberikan kualitas jaringan lebih baik dan mengurangi *Bufferbloat*.	Fokus pada algoritma antrean, bukan implementasi mitigasi *Bufferbloat* pada sekolah.	Penelitian ini mengimplementasikan mitigasi *Bufferbloat* pada lingkungan pendidikan nyata.
16	Konsep *Quality Of Service (QoS)* pada Jaringan Komputer	Samosir et al., Buku/Jurnal Teknologi Informasi, 2026	Menjelaskan konsep *QoS* sebagai metode pengukuran	*QoS* menjadi mekanisme penting untuk menjaga kualitas	Bersifat konseptual dan tidak melakukan implementasi.	Penelitian ini mengimplementasikan dan memvalidasi peningkatan

No	Judul	Peneliti, Media Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
			kualitas layanan jaringan komputer.	layanan jaringan tetap stabil dan efisien.		QoS melalui mitigasi *Bufferbloat*.

2.3 Landasan Teori

2.3.1 Jaringan Komputer

Jaringan komputer merupakan suatu sistem yang menghubungkan dua atau lebih perangkat komputer untuk memungkinkan proses komunikasi, pertukaran data, serta berbagi sumber daya secara efektif dan efisien. Jaringan komputer merupakan media utama dalam mendukung perkembangan teknologi informasi dan *internet* yang digunakan untuk memenuhi kebutuhan layanan komunikasi dan pertukaran informasi secara cepat. Jaringan komputer juga dimanfaatkan untuk mengelola akses *internet* melalui teknologi *hotspot* dan manajemen *bandwidth* agar distribusi koneksi *internet* dapat berjalan secara optimal dan merata kepada setiap pengguna (Gustiawan et al., 2021).

Dalam perkembangannya, jaringan komputer menjadi bagian penting dalam mendukung aktivitas manusia di berbagai bidang, seperti pendidikan, bisnis, pemerintahan, industri, hingga layanan publik berbasis digital. Pemanfaatan jaringan komputer memungkinkan pengguna untuk melakukan akses informasi, komunikasi jarak jauh, transfer data, dan penggunaan layanan *internet* secara bersama-sama melalui media komunikasi tertentu (Randy Ikhsan Ramadhan & Siti Madinah Ladjamuddin, 2022).

Selain itu jaringan komputer tidak hanya berfungsi sebagai media komunikasi data, tetapi juga memiliki peran penting dalam menjaga keamanan informasi. Dalam implementasinya, jaringan komputer memerlukan sistem keamanan seperti *firewall* untuk melindungi kerahasiaan, integritas, dan ketersediaan data dari ancaman akses yang tidak sah. Oleh karena itu, pengelolaan keamanan jaringan menjadi salah satu aspek penting dalam pengembangan sistem jaringan komputer modern (Pratomo, 2024).

Perkembangan jaringan komputer dalam konsep jaringan nirkabel atau *Wireless Sensor Network (WSN)*. Berdasarkan penelitian Zulkarnaen dan Qolbi, WSN merupakan sistem jaringan yang terdiri dari sejumlah node sensor yang saling terhubung secara nirkabel untuk mengumpulkan, memproses, dan mengirimkan data ke pusat pengendali. Teknologi ini banyak

dimanfaatkan dalam pengembangan *Internet of Things (IoT)* karena mampu mendukung komunikasi data secara *real-time* dengan biaya infrastruktur yang relatif lebih rendah (Samosir et al., 2026).

Dalam konteks perkembangan teknologi modern, jaringan komputer juga menjadi fondasi utama dalam implementasi *Internet of Things (IoT)*. Menjelaskan bahwa jaringan komputer berfungsi sebagai infrastruktur utama yang mendukung komunikasi antarperangkat IoT melalui berbagai protokol komunikasi seperti *Wi-Fi, LoRaWAN*, dan *NB-IoT*. Jaringan komputer tidak lagi hanya berperan sebagai media transmisi data, tetapi telah berkembang menjadi ekosistem yang mendukung interoperabilitas sistem, keamanan data, *cloud computing*, serta pengelolaan *bandwidth* pada berbagai sektor industri (Suryaningtyas et al., 2026).

Perkembangan jaringan komputer juga ditandai dengan evolusi protokol komunikasi *internet*, yaitu dari *IPv4* menuju *IPv6*. Merupakan fondasi utama dalam jaringan komputer yang berfungsi untuk melakukan pengalamatan, pengiriman, dan pengaturan jalur paket data antarperangkat jaringan. Kehadiran *IPv6* menjadi solusi atas keterbatasan *IPv4* dengan menyediakan ruang alamat yang lebih luas, keamanan yang lebih baik, serta efisiensi *routing* yang lebih optimal untuk mendukung perkembangan jaringan komputer modern dan *Internet* of Things (Rahman, 2026).

Berdasarkan berbagai penelitian tersebut, dapat disimpulkan bahwa jaringan komputer merupakan sistem komunikasi data yang menghubungkan berbagai perangkat untuk melakukan pertukaran informasi, berbagi sumber daya, dan mendukung berbagai layanan digital secara efektif. Jaringan komputer terus berkembang mengikuti kemajuan teknologi, mulai dari jaringan kabel, jaringan nirkabel, sistem keamanan jaringan, hingga integrasi dengan teknologi IoT dan *cloud computing* guna mendukung kebutuhan komunikasi dan informasi di era digital.

2.3.1.1 *Local Area Network (LAN)*

Local Area Network (LAN) merupakan jaringan komputer yang menghubungkan beberapa perangkat dalam area terbatas, seperti rumah,

sekolah, laboratorium, kantor, maupun organisasi tertentu. LAN digunakan untuk mendukung komunikasi data, berbagi sumber daya, dan akses *internet* antar pengguna dalam satu lingkungan lokal sehingga proses pertukaran informasi dapat berlangsung lebih cepat dan efisien. Jaringan LAN umumnya memanfaatkan perangkat seperti *switch*, *Router*, *access point*, dan kabel UTP sebagai media penghubung antar perangkat komputer.

Local Area Network (LAN) merupakan jaringan lokal yang berfungsi untuk menunjang aktivitas organisasi melalui koneksi *internet* yang cepat dan stabil. Dalam penelitian tersebut dijelaskan bahwa kualitas jaringan LAN dipengaruhi oleh *latency* dan *Throughput* karena kedua aspek tersebut menentukan kecepatan transfer data pada jaringan lokal. Penelitian ini juga menjelaskan bahwa LAN menggunakan perangkat seperti *Routerboard Mikrotik*, *switch*, dan kabel UTP untuk mengatur lalu lintas komunikasi data antar pengguna jaringan (Novianto et al., 2023).

Selain itu LAN berfungsi sebagai media distribusi akses *internet* dalam suatu organisasi melalui pengelolaan jaringan yang terstruktur. Pada implementasinya, perangkat pengguna akan terhubung ke *switch* sebagai konsentrator jaringan, kemudian diteruskan menuju *Routerboard Mikrotik* untuk diproses dan diatur jalur komunikasinya. Penggunaan metode Fasttrack pada jaringan LAN dinilai mampu meningkatkan performa koneksi *internet* dengan mengurangi *latency* dan meningkatkan *Throughput* jaringan sehingga koneksi *internet* menjadi lebih optimal.

Local Area Network (LAN) merupakan jaringan lokal yang dapat diintegrasikan dengan teknologi keamanan jaringan seperti *Virtual Private Network (VPN)*. Dalam penelitian tersebut dijelaskan bahwa jaringan LAN memungkinkan pengguna untuk melakukan komunikasi data secara aman melalui implementasi *WireGuard VPN* yang dihubungkan dengan jaringan publik menggunakan perangkat *Mikrotik*. Teknologi ini memungkinkan pengguna untuk melakukan kontrol dan monitoring jaringan lokal dari luar jaringan utama dengan tetap menjaga keamanan data melalui proses enkripsi komunikasi jaringan (Ikhwandi et al., 2025).

Selain itu LAN memerlukan berbagai perangkat pendukung seperti *Router*board, *switch*, *access point*, kabel UTP, dan perangkat lunak jaringan untuk membangun komunikasi antar perangkat. Infrastruktur LAN yang baik sangat berpengaruh terhadap stabilitas jaringan, efisiensi *bandwidth*, keamanan akses data, serta kualitas komunikasi antar pengguna dalam jaringan komputer. Oleh karena itu, pemilihan perangkat jaringan yang sesuai menjadi faktor penting dalam menjaga performa dan kestabilan jaringan LAN pada suatu organisasi atau instansi.

Berdasarkan berbagai penelitian tersebut dapat disimpulkan bahwa *Local Area Network (LAN)* merupakan jaringan komputer dalam area terbatas yang digunakan untuk menghubungkan berbagai perangkat agar dapat saling bertukar data, berbagi sumber daya, dan mengakses layanan *internet* secara bersama-sama. Seiring perkembangan teknologi, LAN tidak hanya digunakan sebagai media komunikasi lokal, tetapi juga telah berkembang menjadi sistem jaringan yang mendukung keamanan data, manajemen *bandwidth*, serta integrasi dengan teknologi *VPN* dan jaringan modern lainnya.

2.3.1.2 *TCP/IP*

Transmission Control Protocol/Internet Protocol (*TCP/IP*) merupakan sekumpulan protokol komunikasi yang digunakan untuk menghubungkan perangkat komputer dalam jaringan agar dapat saling bertukar data dan informasi. *TCP/IP* menjadi standar utama dalam komunikasi jaringan komputer modern karena mampu mengatur proses pengiriman data, pengalamatan perangkat, serta pengelolaan jalur komunikasi antar jaringan komputer. Sistem protokol ini banyak digunakan pada jaringan lokal (LAN), *internet*, maupun jaringan berskala luas lainnya untuk memastikan proses komunikasi data berjalan secara efektif dan terstruktur.

TCP/IP merupakan protokol komunikasi yang digunakan pada implementasi Ethernet Over IP (EoIP) Tunnel di *Mikrotik RouterOS*. Dalam penelitian tersebut dijelaskan bahwa *TCP/IP* digunakan sebagai dasar

komunikasi antar *Router* untuk membangun koneksi jaringan melalui proses tunneling. Protokol *TCP/IP* memungkinkan perangkat jaringan saling berkomunikasi dengan menggunakan pengalamatan *IPv4* sehingga proses pertukaran data antar jaringan dapat berlangsung secara terintegrasi (Widodo, 2024).

Disisi lain *TCP/IP* memiliki peran penting dalam proses *routing* dan pengiriman paket data antar jaringan komputer. Pada implementasinya, *Router* berfungsi untuk meneruskan paket data dari satu jaringan ke jaringan lainnya menggunakan protokol *routing* seperti *Open* Shortest Path First (OSPF). Sistem komunikasi *TCP/IP* memungkinkan *Router* saling berbagi informasi jaringan sehingga perangkat dalam jaringan yang berbeda tetap dapat melakukan komunikasi data secara efisien dan aman.

Selain itu, penelitian Bongga Arifwidodo menjelaskan bahwa *TCP/IP* mendukung teknologi *Virtual Private Network (VPN)* dan tunneling pada jaringan komputer. Teknologi tunneling bekerja dengan cara melakukan enkapsulasi paket data ke dalam format protokol lain agar komunikasi data dapat berjalan melalui jaringan publik seperti *internet* tanpa mengurangi keamanan informasi. Dengan adanya *TCP/IP*, proses pengiriman data pada jaringan *VPN* dapat berlangsung secara aman melalui mekanisme pengalamatan dan *routing* paket data yang terstruktur.

Pada tahun 2024, penelitian yang dilakukan oleh Rafif Abyakto, Naif Baihaqi, M. Aldi Firdaus, Salsabila Aulia, dan Didik Aribowo menjelaskan bahwa *TCP/IP* merupakan protokol utama yang digunakan dalam proses komunikasi data pada jaringan komputer berbasis topologi bus. Penelitian tersebut menjelaskan bahwa *TCP/IP* berfungsi untuk mengatur komunikasi data selama proses transfer data dari satu komputer ke komputer lainnya melalui jaringan komputer. *TCP/IP* terdiri dari dua protokol utama, yaitu *Transmission Control Protocol* (*TCP*) yang bertugas mengatur proses pengiriman data, serta *Internet Protocol* (IP) yang berfungsi mengatur alamat perangkat dan proses *routing* jaringan (Rafif Abyakto et al., 2024).

TCP/IP memiliki layanan aplikasi yang mendukung komunikasi data

berbasis *internet* dan intranet. Pada implementasinya, setiap perangkat komputer dalam jaringan diberikan alamat *IP* (*IP Address*) sebagai identitas unik agar perangkat dapat saling mengenali dan berkomunikasi satu sama lain. Port pada protokol *TCP/IP* juga berfungsi sebagai mekanisme yang memungkinkan sebuah komputer menjalankan beberapa layanan atau koneksi aplikasi secara bersamaan dalam jaringan komputer.

Selain itu *TCP/IP* mendukung perkembangan berbagai teknologi jaringan modern, seperti *Wi-Fi, Virtual Private Network (VPN), cloud computing*, dan *Internet of Things (IoT)*. Protokol *TCP/IP* memungkinkan komunikasi data dilakukan secara aman dan efisien melalui penerapan teknologi keamanan jaringan seperti *firewall*, enkripsi data, SSL/TLS, dan *IPSec*. Dengan demikian, *TCP/IP* tidak hanya berfungsi sebagai protokol komunikasi data, tetapi juga menjadi fondasi utama dalam perkembangan teknologi jaringan komputer modern (Wagimin, 2024).

Berdasarkan berbagai penelitian tersebut dapat disimpulkan bahwa *TCP/IP* merupakan sekumpulan protokol komunikasi jaringan yang berfungsi untuk mengatur proses pengiriman data, pengalamatan perangkat, *routing*, dan komunikasi antar komputer dalam jaringan. *TCP/IP* menjadi fondasi utama dalam perkembangan jaringan komputer modern karena mampu mendukung berbagai layanan jaringan seperti *internet*, intranet, *VPN*, *routing*, hingga komunikasi data berbasis *client-server* secara efektif, aman, dan terstruktur.

2.3.1.3 *Bandwidth*

Bandwidth merupakan kapasitas atau kemampuan suatu jaringan komputer dalam mentransmisikan data dalam jumlah tertentu pada periode waktu tertentu. *Bandwidth* biasanya diukur dalam satuan *bit per second (bps), Kbps, Mbps,* atau *Gbps* yang menunjukkan besarnya data yang dapat dikirim maupun diterima melalui jaringan komputer. Dalam implementasinya, *bandwidth* menjadi salah satu faktor penting yang memengaruhi kecepatan akses *internet*, kualitas komunikasi data, serta stabilitas koneksi jaringan komputer.

Bandwidth memiliki peran penting dalam menjaga kualitas layanan jaringan atau *Quality Of Service (QoS)*. Dalam penelitian tersebut dijelaskan bahwa manajemen *bandwidth* diperlukan untuk menghindari perebutan *bandwidth* antar client sehingga setiap pengguna memperoleh pembagian *bandwidth* yang adil dan optimal. Penelitian ini juga menunjukkan bahwa metode *Queue Tree* pada *Mikrotik* mampu memberikan performa *Throughput, Delay*, dan *Jitter* yang lebih baik dibandingkan metode lainnya dalam pengelolaan *bandwidth* jaringan komputer (Paskal, 2024).

Selain itu *bandwidth* merupakan bagian penting dalam proses transmisi data pada jaringan komputer karena memengaruhi kecepatan upload dan download data. Penelitian tersebut menjelaskan bahwa permasalahan yang sering terjadi pada penggunaan *internet* adalah manajemen *bandwidth* yang tidak teratur sehingga menyebabkan perebutan *bandwidth*, *Delay*, dan lagging antar pengguna jaringan. Oleh karena itu, diperlukan pengelolaan *bandwidth* yang baik menggunakan perangkat *Mikrotik* dan metode *Queue Tree* agar distribusi *bandwidth* menjadi lebih stabil dan efisien (Aminah, 2022).

Bandwidth merupakan kapasitas atau kemampuan suatu jaringan komputer dalam mentransmisikan data dalam jumlah tertentu pada periode waktu tertentu. *Bandwidth* biasanya diukur dalam satuan *bit per second (bps)* dan digunakan untuk menentukan besarnya data yang dapat dikirim maupun diterima melalui jaringan komputer. Semakin besar *bandwidth* yang dimiliki suatu jaringan, maka semakin besar pula kapasitas transfer data yang dapat dilakukan dalam proses komunikasi jaringan (Herawan et al., 2023).

Berdasarkan berbagai penelitian tersebut dapat disimpulkan bahwa *bandwidth* merupakan kapasitas transmisi data dalam jaringan komputer yang sangat memengaruhi kualitas koneksi *internet* dan performa komunikasi data. Pengelolaan *bandwidth* yang baik diperlukan untuk menjaga stabilitas jaringan, meningkatkan kecepatan akses *internet*, mengurangi gangguan komunikasi data, serta memastikan pembagian akses

jaringan yang adil dan efisien kepada seluruh pengguna jaringan komputer.

2.4 *Mikrotik*

Mikrotik merupakan sistem operasi dan perangkat jaringan yang digunakan untuk mengelola serta membangun jaringan komputer, baik jaringan kabel maupun jaringan nirkabel. *Mikrotik* banyak digunakan sebagai *Router* network karena memiliki berbagai fitur yang mendukung pengelolaan jaringan seperti *routing*, *firewall*, *hotspot*, *bandwidth* management, monitoring jaringan, hingga pengamanan akses *internet*. Penggunaan *Mikrotik* dinilai mampu membantu administrator jaringan dalam mengatur lalu lintas data agar jaringan komputer dapat berjalan secara lebih stabil, aman, dan efisien.

Mikrotik RouterOS merupakan sistem operasi berbasis Linux yang banyak digunakan oleh *Internet Service Provider (ISP)* untuk keperluan *firewall* maupun *Router* network. Dalam penelitian tersebut dijelaskan bahwa *Mikrotik* menjadi *Router* network yang handal karena dilengkapi dengan berbagai fitur dan tools yang mendukung pengelolaan jaringan kabel maupun wireless. *Mikrotik* juga mampu digunakan untuk membangun sistem *hotspot*, *routing*, serta pengaturan *bandwidth* pada jaringan komputer (Sundara et al., 2022).

Mikrotik digunakan dalam implementasi jaringan *Virtual Private Network (VPN)* untuk meningkatkan keamanan komunikasi data antar jaringan komputer. Dalam penelitian tersebut dijelaskan bahwa *Mikrotik* mampu mendukung proses transmisi data secara aman melalui teknologi tunneling dan enkripsi jaringan sehingga komunikasi data antar lokasi yang berbeda dapat dilakukan secara lebih aman dan stabil (Arfind et al., 2023).

Selain itu *Mikrotik* merupakan perangkat jaringan berbasis *RouterOS* yang digunakan untuk membangun jaringan komputer berbasis kabel maupun wireless. *Mikrotik* memiliki kemampuan untuk melakukan *routing*, *firewall*, *proxy server*, *hotspot*, dan manajemen jaringan sehingga banyak digunakan pada sekolah, kantor, warnet, maupun penyedia layanan *internet* (ISP) (Nursobah, Pitrasacha Aditya, 2023).

Berdasarkan berbagai penelitian tersebut dapat disimpulkan bahwa

Mikrotik merupakan sistem operasi dan perangkat jaringan berbasis Linux yang digunakan untuk membangun dan mengelola jaringan komputer. *Mikrotik* memiliki berbagai fitur seperti *routing*, *firewall*, *hotspot*, *bandwidth* management, *VPN*, monitoring jaringan, dan *QoS* yang mampu mendukung pengelolaan jaringan komputer secara lebih aman, stabil, efisien, dan terstruktur pada berbagai lingkungan jaringan komputer.

2.4.1 *RouterOS*

RouterOS merupakan sistem operasi jaringan yang digunakan untuk mengubah komputer atau perangkat jaringan menjadi sebuah *Router* yang mampu mengelola lalu lintas data pada jaringan komputer. *RouterOS* banyak digunakan dalam pengelolaan jaringan karena memiliki berbagai fitur seperti *routing*, *firewall*, *hotspot*, *bandwidth management*, *wireless access point*, *Virtual Private Network (VPN)*, dan monitoring jaringan sehingga mampu mendukung pembangunan jaringan komputer secara lebih efektif dan efisien.

RouterOS merupakan sistem operasi jaringan yang digunakan untuk mengelola, mengatur, dan mengontrol komunikasi data pada jaringan komputer. *RouterOS* berfungsi untuk menghubungkan berbagai perangkat jaringan melalui proses *routing* sehingga paket data dapat dikirim dari sumber menuju tujuan secara efektif dan efisien. Selain itu, *RouterOS* juga mendukung berbagai fitur jaringan seperti *firewall*, *bandwidth* management, *hotspot*, *Virtual Private Network (VPN)*, wireless network, dan monitoring jaringan yang membantu administrator dalam mengelola infrastruktur jaringan komputer modern (Subowo, 2023).

Selain itu, *RouterOS* digunakan dalam implementasi *VPN* Server menggunakan protokol *L2TP* dan *IPSec* sebagai sistem keamanan jaringan. Dalam penelitian tersebut dijelaskan bahwa *RouterOS* berfungsi sebagai sistem operasi jaringan yang mampu melakukan *Konfigurasi routing*, pengalamatan *IP Address*, serta pengamanan komunikasi data antar jaringan komputer melalui proses tunneling dan enkripsi data (Ikhwandi et al., 2025).

Berdasarkan berbagai penelitian tersebut dapat disimpulkan bahwa *RouterOS* merupakan sistem operasi jaringan yang digunakan untuk

membangun, mengatur, dan mengelola komunikasi data pada jaringan komputer melalui fitur *routing*, *firewall*, *bandwidth* management, *VPN*, monitoring jaringan, dan pengaturan lalu lintas data. *RouterOS* berperan penting dalam mendukung pengelolaan jaringan komputer modern karena mampu meningkatkan fleksibilitas, efisiensi, keamanan, serta stabilitas komunikasi data pada berbagai jenis infrastruktur jaringan komputer.

2.4.2 *Firewall*

Firewall merupakan sistem keamanan jaringan yang digunakan untuk mengatur, memantau, dan mengendalikan lalu lintas data yang masuk maupun keluar dari suatu jaringan komputer berdasarkan aturan keamanan tertentu. *Firewall* berfungsi sebagai pelindung jaringan dari berbagai ancaman siber seperti akses ilegal, malware, spoofing, Distributed Denial of Service (DDoS), ransomware, dan berbagai bentuk serangan jaringan lainnya sehingga keamanan data dan sistem dapat tetap terjaga.

Firewall generasi awal bekerja menggunakan metode *Packet Filtering* dengan melakukan pemeriksaan paket data berdasarkan alamat IP dan nomor port. *Firewall* jenis ini mampu melakukan pengendalian lalu lintas dasar pada jaringan komputer, namun masih memiliki keterbatasan dalam mendeteksi ancaman yang bekerja pada tingkat aplikasi. Penelitian tersebut juga menjelaskan perkembangan *firewall* menuju *Next Generation Firewall* (*NGFW*) yang memiliki kemampuan inspeksi lalu lintas data secara lebih mendalam dibandingkan *firewall* tradisional (Tarina et al., 2026).

Selain itu *firewall* merupakan komponen penting dalam sistem keamanan jaringan modern yang berfungsi untuk memantau, menyaring, dan mengendalikan lalu lintas data berdasarkan kebijakan keamanan tertentu. Penelitian tersebut menjelaskan bahwa perkembangan *firewall* telah menghasilkan *application layer firewall* yang mampu melakukan penyaringan berdasarkan aplikasi dan protokol tertentu seperti *HTTP* dan *SMTP* sehingga ancaman berbasis aplikasi dapat dideteksi dengan lebih baik dibandingkan *firewall* tradisional.

Sistem keamanan jaringan modern mendukung pengelolaan lalu lintas

data secara terpusat melalui konsep *Software-Defined Networking (SDN)* menggunakan protokol *Open*Flow. Dalam implementasinya, *firewall* digunakan untuk melakukan pengaturan lalu lintas jaringan dan pengendalian komunikasi data antar perangkat jaringan sehingga administrator dapat memonitor dan mengendalikan keamanan jaringan secara lebih fleksibel dan efisien (Kurniawan & Setiawan, 2025).

Firewall dan sistem keamanan jaringan modern mendukung implementasi *Network Intrusion Detection System (NIDS)* berbasis virtualisasi fungsi jaringan. Dalam penelitian tersebut dijelaskan bahwa *firewall* digunakan untuk melakukan monitoring lalu lintas jaringan, mendeteksi ancaman secara *real-time*, serta meningkatkan keamanan komunikasi data melalui pengelolaan aturan keamanan yang lebih dinamis dan skalabel pada jaringan komputer modern (Mahbub & Srisulistiowati, 2026).

Berdasarkan berbagai penelitian tersebut dapat disimpulkan bahwa *firewall* merupakan sistem keamanan jaringan yang digunakan untuk melindungi jaringan komputer melalui proses filtering, monitoring, dan pengendalian lalu lintas data berdasarkan aturan keamanan tertentu. *Firewall* terus berkembang dari sistem keamanan tradisional menjadi sistem keamanan modern berbasis *Software-Defined Networking (SDN)*, *cloud computing*, dan otomatisasi jaringan yang mampu meningkatkan keamanan, fleksibilitas, efisiensi, serta stabilitas komunikasi data pada jaringan komputer modern.

2.4.3 *Mangle*

Mangle merupakan salah satu fitur pada *firewall Mikrotik* yang digunakan untuk melakukan penandaan (*marking*) terhadap paket data yang melewati jaringan komputer. Penandaan tersebut digunakan untuk membantu proses manajemen *bandwidth*, *routing*, *Packet Filtering*, dan pengaturan lalu lintas data sehingga administrator jaringan dapat mengontrol distribusi trafik jaringan secara lebih efektif dan terstruktur. *Mangle* bekerja dengan memberikan tanda tertentu pada paket data berdasarkan alamat IP, port, protokol, maupun jenis koneksi yang digunakan dalam jaringan komputer.

Firewall mangle adalah salah satu fitur pada *RouterOS Mikrotik* yang berfungsi untuk melakukan proses *marking* atau penandaan terhadap paket data tertentu. Paket data yang telah diberi tanda kemudian dapat digunakan oleh berbagai fitur jaringan lainnya, seperti pengaturan *bandwidth*, monitoring trafik, dan pengelompokan jalur koneksi. *Firewall mangle* memiliki lima chain utama, yaitu pre*routing*, input, output, forward, dan post*routing* yang masing-masing memiliki fungsi tersendiri dalam proses lalu lintas paket data (Hamza, 2022).

Mangle digunakan dalam implementasi metode *Queue Tree* pada *bandwidth management Mikrotik*. Dalam penelitian tersebut dijelaskan bahwa *mangle* berfungsi untuk melakukan packet *marking* terhadap trafik upload dan download sebelum proses pembagian *bandwidth* dilakukan menggunakan *Queue Tree*. Dengan adanya proses penandaan paket data tersebut, administrator jaringan dapat mengatur distribusi *bandwidth* secara lebih adil dan terstruktur kepada setiap pengguna jaringan komputer (Andesita Prihantara, Antonius Agung Hartono, 2026).

Selain itu *firewall mangle* merupakan pusat pengaturan jalur packet data yang memanfaatkan fitur *Mark Connection, Mark Packet, dan Mark Routing*. Mark Connection berfungsi untuk memberikan tanda pada koneksi paket pertama yang keluar dari client atau respon dari *server, Mark Packet* digunakan untuk menandai seluruh paket yang memiliki koneksi tertentu, sedangkan Mark *Routing* digunakan untuk menentukan jalur *routing internet*, terutama pada penggunaan lebih dari satu ISP. Dengan penerapan *firewall mangle*, pengelolaan *bandwidth* dan distribusi trafik jaringan dapat dilakukan secara lebih seimbang dan efisien.

Berdasarkan beberapa penelitian dan jurnal yang telah dibahas, dapat disimpulkan bahwa *mangle* merupakan fitur pada *firewall Mikrotik* yang digunakan untuk melakukan penandaan (*marking*) terhadap paket data, koneksi, maupun jalur *routing* pada jaringan komputer. Fitur ini berperan penting dalam proses manajemen *bandwidth*, pengaturan lalu lintas data, monitoring jaringan, serta pengendalian distribusi trafik agar penggunaan

jaringan menjadi lebih optimal dan seimbang.

Selain itu, *mangle* juga mendukung proses pengaturan kualitas layanan jaringan (*Quality Of Service*/*QoS*) melalui fungsi *Mark Connection, Mark Packet, dan Mark Routing*. Dengan adanya fitur tersebut, administrator jaringan dapat mengelompokkan paket data berdasarkan jenis koneksi, menentukan prioritas trafik, serta mengatur jalur *routing* menggunakan lebih dari satu ISP sehingga koneksi *internet* dapat berjalan lebih stabil, efisien, dan merata bagi seluruh pengguna jaringan.

2.4.4 *Queue Tree*

Queue Tree merupakan metode manajemen *bandwidth* pada *Router Mikrotik* yang digunakan untuk mengatur dan membatasi aliran trafik data dalam jaringan komputer. Metode ini bekerja dengan cara membagi *bandwidth* berdasarkan jenis koneksi atau pengguna sehingga penggunaan jaringan dapat lebih terkontrol dan merata.

Queue Tree adalah salah satu metode manajemen antrian (*queue management*) yang diterapkan pada perangkat jaringan seperti *Router* atau *firewall* untuk mengatur prioritas serta alokasi *bandwidth* terhadap berbagai jenis layanan maupun pengguna jaringan. Metode ini memungkinkan administrator jaringan melakukan pengendalian lalu lintas data agar kualitas layanan jaringan tetap terjaga (nasir et al., 2023).

Selain itu metode *Queue Tree* digunakan pada *Router Mikrotik* untuk meningkatkan *Quality Of Service (QoS)* melalui pengaturan *bandwidth* yang lebih terstruktur. Penerapan *Queue Tree* memungkinkan distribusi *bandwidth* dilakukan secara adil sehingga koneksi *internet* menjadi lebih stabil dan mampu mengurangi terjadinya gangguan pada pengguna lain di dalam jaringan.

2.4.5 *PCQ* (*Per Connection Queue*)

Peer Connection Queue (*PCQ*) merupakan metode manajemen *bandwidth* yang digunakan untuk membagi kapasitas *bandwidth* secara otomatis dan merata kepada setiap pengguna atau koneksi pada jaringan komputer. Metode *PCQ* bekerja dengan cara mengelompokkan lalu lintas

data berdasarkan koneksi pengguna sehingga setiap klien memperoleh alokasi *bandwidth* yang adil tanpa harus bersaing dengan pengguna lainnya (Mufrot & Sobari, 2023).

Metode pembagian *bandwidth* yang diterapkan pada *Router Mikrotik* dengan memanfaatkan *Queue Tree* untuk meningkatkan *Quality Of Service (QoS)* dalam jaringan. Metode ini digunakan untuk mengatasi ketidakmerataan distribusi *bandwidth* yang sering menyebabkan sebagian pengguna memperoleh koneksi *internet* lebih cepat dibandingkan pengguna lain. Dengan penerapan *PCQ*, seluruh klien yang terhubung ke jaringan akan mendapatkan pembagian *bandwidth* yang lebih merata dan stabil.

Dalam implementasinya, *PCQ* bekerja dengan cara membatasi dan mengatur *bandwidth* berdasarkan sumber atau tujuan koneksi sehingga penggunaan *internet* dapat dibagi secara otomatis sesuai jumlah pengguna aktif. Metode ini sangat efektif diterapkan pada jaringan yang memiliki banyak pengguna karena mampu menjaga kestabilan koneksi *internet* saat proses *browsing*, *streaming*, upload, maupun download berlangsung secara bersamaan.

Selain itu, penerapan metode *PCQ* terbukti mampu meningkatkan kualitas layanan jaringan karena setiap pengguna memperoleh hak akses *bandwidth* yang sama sesuai aturan manajemen jaringan yang telah ditentukan. Dengan demikian, metode *PCQ* dapat menciptakan penggunaan *bandwidth* yang lebih efisien, adil, dan optimal pada jaringan komputer berbasis *Mikrotik*.

2.5 *Quality Of Service (QoS)*

Quality Of Service (QoS) merupakan standar pengukuran kualitas layanan jaringan yang digunakan untuk menilai kemampuan suatu jaringan dalam memberikan performa komunikasi data yang baik. Penilaian *QoS* dilakukan melalui beberapa parameter, seperti *Throughput, Delay*, *Jitter*, dan *Packet Loss* untuk mengetahui tingkat kualitas layanan jaringan *internet* yang diterima oleh pengguna.

Quality Of Service (QoS) adalah metode pengukuran yang digunakan

untuk mengetahui seberapa baik kualitas suatu jaringan dalam memberikan layanan komunikasi data. *QoS* digunakan untuk mendefinisikan karakteristik layanan jaringan *internet* sehingga kualitas koneksi dapat diukur berdasarkan parameter tertentu, seperti *bandwidth*, *Throughput, Delay*, *Jitter*, dan *Packet Loss*. Semakin baik pengelolaan parameter tersebut, maka semakin baik pula kualitas lalu lintas jaringan yang dihasilkan (Hafizh Ridwan et al., 2024).

Selain itu *Quality Of Service (QoS)* merupakan metode pengukuran kualitas jaringan secara objektif yang dilakukan menggunakan parameter teknis, seperti *Throughput*, *Packet Loss*, *Delay*, dan *Jitter*. *QoS* digunakan untuk mengetahui tingkat kualitas layanan *internet*, khususnya pada aktivitas *streaming* video dan penggunaan jaringan wireless sehingga performa jaringan dapat dianalisis berdasarkan standar tertentu, seperti *TIPHON* (Zulkarnain et al., 2025).

Quality Of Service (QoS) adalah teknik pengelolaan jaringan yang digunakan untuk mengatur *bandwidth*, *Delay*, dan *Packet Loss* pada aliran data di dalam jaringan komputer. *QoS* bertujuan untuk meningkatkan kualitas layanan *internet* agar koneksi menjadi lebih stabil, cepat, dan optimal bagi pengguna, terutama dalam aktivitas *streaming*, video *conference*, *gaming*, dan *browsing* (Gumeular & Akbi, 2025).

Disisi lain *Quality Of Service (QoS)* adalah mekanisme pengelolaan jaringan yang bertujuan untuk meningkatkan kualitas layanan *internet* melalui pengaturan *bandwidth* secara terstruktur. *QoS* diterapkan menggunakan metode manajemen *bandwidth*, seperti Simple Queue, *Queue Tree*, dan *Hierarchical Token Bucket (HTB)* agar distribusi *bandwidth* menjadi lebih adil, stabil, dan sesuai kebutuhan pengguna jaringan (Wibowo & Komalasari, 2025).

Berdasarkan beberapa jurnal yang telah dibahas, dapat disimpulkan bahwa *Quality Of Service (QoS)* merupakan metode atau teknik pengelolaan jaringan yang digunakan untuk mengukur, mengatur, dan meningkatkan kualitas layanan pada jaringan komputer maupun *internet*. *QoS* berfungsi untuk memastikan distribusi *bandwidth*, pengendalian trafik, serta performa jaringan dapat berjalan secara optimal, stabil, dan merata bagi setiap pengguna.

Selain itu, *QoS* juga digunakan untuk menganalisis kualitas jaringan melalui beberapa parameter penting, seperti *Throughput, Delay, Jitter*, dan *Packet Loss*. Dengan penerapan metode manajemen *bandwidth*, seperti *Queue Tree*, *PCQ*, dan *Hierarchical Token Bucket (HTB)*, *QoS* mampu meningkatkan efisiensi penggunaan *bandwidth* serta menjaga kestabilan koneksi *internet* pada berbagai aktivitas jaringan, seperti *browsing*, *streaming*, video *conference*, *gaming*, dan transfer data.

2.5.1 *Throughput*

Throughput merupakan jumlah data yang berhasil dikirim dari sumber ke tujuan dalam satuan waktu tertentu. *Throughput* biasanya diukur dalam satuan *bit per second (bps), Kbps, Mbps,* atau *Gbps*. *Throughput* adalah kecepatan aktual transfer data yang diterima oleh pengguna dalam suatu jaringan komunikasi. Nilai *Throughput* dipengaruhi oleh kapasitas *bandwidth*, kepadatan trafik jaringan, dan kualitas perangkat jaringan yang digunakan.

Selain itu *Throughput* adalah parameter *QoS* yang digunakan untuk mengukur jumlah data yang berhasil dikirim dan diterima pada jaringan komputer dalam kurun waktu tertentu. *Throughput* digunakan untuk mengetahui kualitas jaringan *internet* berdasarkan tingkat keberhasilan transfer data sehingga dapat menjadi indikator performa jaringan sebelum dan sesudah penerapan manajemen *bandwidth* (Yehezkiel Saputra Wanggi, 2023).

Selain itu, nilai *Throughput* dipengaruhi oleh kondisi jaringan, kapasitas *bandwidth*, jumlah pengguna, serta efektivitas manajemen *bandwidth* yang diterapkan. Semakin besar nilai *Throughput* yang diperoleh, maka semakin baik pula kemampuan jaringan dalam melakukan proses komunikasi data secara stabil, cepat, dan efisien. Oleh karena itu, *Throughput* menjadi salah satu parameter penting dalam analisis kualitas jaringan komputer dan *internet*.

2.5.2 *Delay*

Delay atau *latency* merupakan waktu yang dibutuhkan oleh paket data untuk menempuh perjalanan dari sumber menuju tujuan pada jaringan

komputer. *Delay* digunakan sebagai salah satu parameter *Quality Of Service (QoS)* untuk mengetahui tingkat kecepatan respon jaringan dalam proses pengiriman data.

Selain itu *Delay* adalah waktu tunda yang terjadi pada saat proses pengiriman paket data dalam jaringan komunikasi. Besarnya nilai *Delay* dipengaruhi oleh kondisi jaringan, kapasitas *bandwidth*, media transmisi, serta kepadatan lalu lintas data yang berlangsung pada jaringan tersebut. *Delay* merupakan waktu tempuh yang dibutuhkan data untuk mencapai tujuan pengiriman dari sumber asal. Parameter *Delay* digunakan untuk mengukur kualitas jaringan *internet* karena semakin kecil nilai *Delay*, maka semakin cepat dan baik pula performa jaringan dalam melakukan komunikasi data.

Disisi lain *Delay* adalah parameter *Quality Of Service (QoS)* yang digunakan untuk mengukur lamanya waktu pengiriman data dari pengirim menuju penerima dalam jaringan komputer. *Delay* dapat dipengaruhi oleh jarak pengiriman, kepadatan trafik jaringan, serta kemampuan perangkat jaringan dalam memproses data sehingga nilai *Delay* menjadi indikator penting dalam menentukan kestabilan dan kualitas layanan jaringan *internet* (Pratama et al., 2022).

Dapat disimpulkan bahwa *Delay* atau *latency* merupakan waktu tunda yang dibutuhkan paket data untuk melakukan perjalanan dari sumber menuju tujuan pada jaringan komputer. *Delay* digunakan sebagai salah satu parameter *Quality Of Service (QoS)* untuk mengukur tingkat kecepatan respon dan kualitas layanan jaringan dalam proses komunikasi data.

Selain itu, nilai *Delay* dipengaruhi oleh berbagai faktor, seperti jarak pengiriman data, kepadatan trafik jaringan, kapasitas *bandwidth*, media transmisi, serta kemampuan perangkat jaringan dalam memproses paket data. Semakin kecil nilai *Delay* yang dihasilkan, maka semakin baik pula kualitas dan performa jaringan *internet* karena proses pengiriman data dapat berlangsung lebih cepat, stabil, dan efisien.

2.5.3 *Jitter*

Jitter merupakan variasi waktu tunda (*Delay variation*) yang terjadi

selama proses pengiriman paket data pada jaringan komputer. *Jitter* digunakan sebagai parameter *Quality Of Service (QoS)* untuk mengukur kestabilan waktu pengiriman data sehingga semakin kecil nilai *Jitter*, maka semakin baik kualitas jaringan yang digunakan (Pratama et al., 2022).

Selain itu *Jitter* adalah perubahan atau variasi selisih waktu *Delay* antar paket data yang dikirimkan melalui jaringan *internet*. *Jitter* berkaitan erat dengan *Delay* karena tingginya nilai *Jitter* dapat menyebabkan ketidakstabilan komunikasi data, terutama pada layanan *real-time* seperti *streaming*, video *conference*, *gaming*, dan *Voice over IP (VoIP)* (Gumeular & Akbi, 2025).

Disisi lain *Jitter* merupakan variasi panjang antrean, waktu pemrosesan data, serta waktu penghimpunan ulang paket data selama proses transmisi berlangsung. Parameter *Jitter* digunakan untuk mengetahui tingkat kestabilan jaringan karena nilai *Jitter* yang rendah menunjukkan bahwa proses pengiriman data dapat berjalan lebih stabil dan konsisten. Penerapan metode manajemen *bandwidth* seperti *PCQ* dan *FQ_Codel* mampu menurunkan nilai *Jitter* pada jaringan *internet* secara signifikan. Hal tersebut menunjukkan bahwa pengelolaan *bandwidth* yang baik dapat meningkatkan kualitas layanan jaringan sehingga koneksi *internet* menjadi lebih stabil dan optimal bagi pengguna.

2.5.4 *Packet Loss*

Packet Loss merupakan kondisi hilangnya paket data pada saat proses transmisi data di dalam jaringan komputer. *Packet Loss* terjadi ketika paket data yang dikirim tidak berhasil mencapai tujuan sehingga dapat memengaruhi kualitas komunikasi dan performa jaringan *internet*.

Dalam penerapan parameter *Quality Of Service (QoS)* yang digunakan untuk menggambarkan jumlah paket data yang hilang selama proses pengiriman data berlangsung. Hilangnya paket data tersebut dapat disebabkan oleh kepadatan trafik jaringan, tabrakan data (collision), gangguan media transmisi, maupun keterbatasan kapasitas *bandwidth* pada jaringan komputer.

Packet Loss digunakan sebagai salah satu parameter pengukuran

Quality Of Service (QoS) pada jaringan *VPN* berbasis *Mikrotik*. Parameter ini digunakan untuk menganalisis performa jaringan berdasarkan jumlah paket data yang hilang selama proses komunikasi data berlangsung sehingga kualitas layanan jaringan dapat diketahui secara lebih akurat (Adji Putra Pamungkas F, Muhammad Reza Putra, 2021).

Selain itu *Packet Loss* merupakan indikator kualitas jaringan yang digunakan untuk mengetahui tingkat keberhasilan pengiriman paket data dari sumber menuju tujuan. Semakin kecil nilai *Packet Loss*, maka semakin baik pula kualitas jaringan karena proses transmisi data dapat berlangsung lebih stabil dan minim gangguan. dapat disimpulkan bahwa *Packet Loss* merupakan kondisi hilangnya paket data pada saat proses transmisi dalam jaringan komputer sehingga paket yang dikirim tidak berhasil diterima oleh tujuan. *Packet Loss* digunakan sebagai salah satu parameter *Quality Of Service (QoS)* untuk mengukur kualitas dan tingkat keberhasilan pengiriman data pada jaringan *internet*.

Disisi lain *Packet Loss* dipengaruhi oleh berbagai faktor, seperti kemacetan trafik jaringan, collision, gangguan media transmisi, kapasitas *bandwidth* yang terbatas, serta kualitas perangkat jaringan yang digunakan. Semakin kecil nilai *Packet Loss*, maka semakin baik kualitas jaringan karena proses komunikasi data dapat berlangsung lebih stabil, cepat, dan efisien tanpa banyak paket data yang hilang selama transmisi.

2.6 *Packet Filtering*

Packet Filtering merupakan salah satu teknik keamanan jaringan yang digunakan untuk menyaring lalu lintas data berdasarkan aturan tertentu sebelum paket data diperbolehkan masuk atau keluar dari jaringan. Teknik ini bekerja dengan memeriksa informasi yang terdapat pada header paket data, seperti alamat sumber (*Source address*), alamat tujuan (*Destination address*), jenis protokol, dan nomor *Port* yang digunakan. Dalam perkembangan teknologi jaringan hingga saat ini, *Packet Filtering* menjadi bagian penting dalam sistem keamanan jaringan karena mampu membantu administrator mengontrol akses jaringan secara lebih efektif.

Packet Filtering digunakan sebagai mekanisme pengendalian akses jaringan untuk membatasi pengguna dalam mengakses situs atau layanan tertentu pada jaringan komputer berbasis *Mikrotik*. Penerapan *Packet Filtering* dilakukan melalui *Konfigurasi firewall* sehingga administrator jaringan dapat memblokir akses terhadap situs yang dianggap tidak sesuai, seperti media sosial, game *online*, maupun situs berbahaya lainnya (Muniraa et al., 2024).

Dalam implementasinya, *Packet Filtering* melakukan penyaringan paket data berdasarkan beberapa parameter utama, yaitu *Source address*, *Destination address*, *Protocol*, dan *Port*. Keempat parameter tersebut menjadi dasar dalam menentukan apakah suatu paket data diizinkan atau ditolak oleh sistem keamanan jaringan.

2.6.1 *Source Address*

Source address merupakan alamat sumber yang digunakan untuk mengidentifikasi perangkat pengirim paket data dalam suatu jaringan komputer. *Source address* biasanya berupa alamat IP atau *MAC* address yang berfungsi untuk menunjukkan asal paket data sehingga proses komunikasi dan pengelolaan lalu lintas jaringan dapat dilakukan dengan lebih terstruktur (Novianto et al., 2024).

Pada *source address* memiliki peran penting dalam proses filtering jaringan, khususnya pada sistem keamanan berbasis *Mikrotik*. Melalui penerapan filtering berdasarkan *MAC* address dan alamat IP sumber, administrator jaringan dapat mengontrol perangkat mana saja yang diizinkan untuk mengakses jaringan serta mencegah perangkat asing atau tidak dikenal masuk ke dalam sistem jaringan.

Selain itu *source address* juga digunakan dalam *Konfigurasi DHCP* dan *ARP* untuk memastikan bahwa hanya perangkat yang telah terdaftar pada *Router* yang dapat memperoleh alamat IP dan melakukan komunikasi data di jaringan. Dengan mekanisme tersebut, keamanan jaringan dapat ditingkatkan karena perangkat yang tidak memiliki *source address* yang sesuai akan ditolak aksesnya oleh sistem jaringan.

Dalam implementasi keamanan jaringan, penggunaan *source address*

memungkinkan administrator melakukan pengawasan dan pengendalian akses jaringan secara lebih efektif. Penerapan metode filtering berbasis *source address* terbukti mampu mencegah serangan jaringan, seperti *DHCP* Starvation dan *DHCP Rogue*, sehingga stabilitas serta keamanan jaringan komputer dapat tetap terjaga.

2.6.2 *Destination Address*

Destination address merupakan alamat tujuan pada paket data yang digunakan untuk menentukan perangkat atau host penerima dalam proses komunikasi jaringan komputer. *Destination address* berfungsi sebagai identitas tujuan pengiriman data sehingga *Router* atau perangkat jaringan dapat meneruskan paket data ke alamat yang sesuai.

Destination address digunakan dalam mekanisme *Network Address Translation* (*NAT*) untuk melakukan translasi alamat IP tujuan pada proses pengiriman paket data melalui jaringan *internet*. Dalam penerapannya, *Router NAT* akan mengubah alamat IP tujuan dari paket data agar dapat diteruskan menuju server atau perangkat yang berada di jaringan lokal maupun publik sesuai kebutuhan komunikasi jaringan (Naufal & Albar, 2021).

Selain itu *destination address* memiliki peranan penting dalam proses *routing* jaringan karena digunakan untuk menentukan jalur atau rute pengiriman paket data menuju host tujuan. Dengan adanya *Destination address*, perangkat jaringan dapat melakukan pemilihan rute terbaik sehingga layanan intranet dan *internet* dapat berjalan secara bersamaan dan komunikasi data dapat berlangsung dengan lebih efektif.

Dalam implementasi *public cloud storage* berbasis *Mikrotik*, *Destination address* digunakan pada proses port forwarding dan *NAT* untuk meneruskan paket data dari alamat IP publik menuju alamat *IP private server* yang berada di jaringan lokal. Mekanisme ini memungkinkan layanan private cloud storage dapat diakses melalui jaringan *internet* secara *online* tanpa mengubah struktur jaringan lokal yang sudah ada.

2.6.3 *Protocol*

Protocol merupakan seperangkat aturan atau standar komunikasi yang

digunakan untuk mengatur proses pertukaran data antar perangkat dalam jaringan komputer. *Protocol* berfungsi untuk memastikan bahwa proses pengiriman dan penerimaan data dapat berjalan dengan baik, terstruktur, dan sesuai tujuan alamat jaringan yang ditentukan (Ikhwandi et al., 2025).

Dalam jaringan komputer, *Protocol* yang umum digunakan adalah *Transmission Control Protocol/Internet Protocol* (*TCP/IP*) yang berfungsi sebagai dasar komunikasi data pada jaringan *internet* maupun jaringan lokal. *TCP/IP* digunakan untuk melakukan pengalamatan jaringan serta mengatur proses pengiriman paket data dari sumber menuju alamat tujuan sehingga komunikasi antar perangkat dapat berlangsung secara efektif dan stabil.

Di dalam *protocol* juga diterapkan pada teknologi *Virtual Private Network (VPN)*, seperti *PPTP*, *L2TP*, *IPSec*, *OpenVPN*, dan *WireGuard* yang digunakan untuk mengamankan komunikasi data pada jaringan publik. *Protocol VPN* bekerja dengan cara membuat jalur komunikasi terenkripsi sehingga data yang dikirimkan melalui jaringan *internet* dapat terlindungi dari penyadapan maupun akses tidak sah.

Selain itu *protocol* memiliki peranan penting dalam proses *routing* jaringan karena digunakan untuk menentukan jalur terbaik dalam meneruskan paket data menuju tujuan. Dengan adanya *protocol routing*, komunikasi antar *Router* pada jaringan berskala besar dapat berjalan lebih efisien sehingga kualitas layanan jaringan, keamanan data, dan stabilitas koneksi dapat tetap terjaga.

2.6.4 *Port*

Port merupakan antarmuka atau jalur komunikasi pada perangkat jaringan yang digunakan untuk menghubungkan perangkat lain dalam proses pertukaran data pada jaringan komputer. *Port* memiliki fungsi penting dalam mengatur lalu lintas komunikasi antar perangkat sehingga koneksi jaringan dapat berjalan dengan baik dan terstruktur (Kurniawan & Setiawan, 2025).

Dalam implementasi jaringan komputer, port digunakan pada perangkat *switch*, *Router*, maupun *access point* untuk menghubungkan perangkat pengguna ke dalam jaringan lokal maupun *internet*. Setiap port dapat

di*Konfigurasi* sesuai kebutuhan jaringan, seperti *mode access* dan *mode trunk* pada *VLAN* untuk mengatur segmentasi lalu lintas data antar jaringan.

Pada port juga berperan penting dalam penerapan sistem keamanan jaringan melalui metode *Port Security* pada *switch Cisco*. *Port Security* digunakan untuk membatasi perangkat yang dapat terhubung ke suatu port berdasarkan *MAC* Address tertentu sehingga perangkat asing atau tidak sah tidak dapat mengakses jaringan komputer.

Selain itu pengelolaan *port* dilakukan dengan cara menonaktifkan *port* yang tidak digunakan untuk meningkatkan keamanan jaringan dari ancaman akses ilegal. Dengan pengaturan *port* yang baik, administrator jaringan dapat mengontrol akses perangkat, menjaga stabilitas komunikasi data, serta meningkatkan keamanan dan efisiensi jaringan komputer secara keseluruhan.

2.6.5 Layer *Packet Filtering*

Layer *Packet Filtering* atau *Layer 7 Protocol* merupakan metode filtering pada *firewall Mikrotik* yang digunakan untuk melakukan penyaringan paket data berdasarkan *Protocol* aplikasi yang digunakan pada lalu lintas jaringan. Metode ini bekerja pada layer aplikasi (*application layer*) sehingga mampu mengenali dan memblokir akses terhadap situs web maupun aplikasi tertentu, seperti *YouTube*, *Facebook*, dan *Twitter* melalui aturan *firewall* yang telah di*Konfigurasi* (Syahputri et al., 2023).

Disisi lain Layer *Packet Filtering* digunakan sebagai mekanisme keamanan jaringan untuk mengontrol akses *internet* dan membatasi penggunaan situs atau aplikasi tertentu yang dianggap dapat mengganggu produktivitas maupun keamanan jaringan. Penerapan filtering dilakukan dengan menambahkan *Filter Rules* pada menu *Layer 7 Protocol* di *Router Mikrotik* menggunakan pola *Regular Expression (RegExp)* untuk mendeteksi alamat situs atau *Protocol* aplikasi yang akan diblokir.

Selain itu, Layer *Packet Filtering* memiliki fungsi untuk meningkatkan keamanan dan efisiensi penggunaan jaringan dengan cara menyaring lalu lintas data berdasarkan isi paket maupun *Protocol* aplikasi yang digunakan. Dengan penerapan metode ini, administrator jaringan dapat melakukan

pengawasan terhadap aktivitas pengguna jaringan serta mencegah akses ke situs negatif, media sosial, maupun aplikasi tertentu yang tidak diizinkan dalam lingkungan jaringan komputer.

Di dalam Layer *Packet Filtering* juga diterapkan untuk melakukan pemblokiran aplikasi dan game *online* menggunakan *firewall Mikrotik*. Proses filtering dilakukan berdasarkan *Protocol TCP* dan *UDP* serta port tertentu yang digunakan oleh aplikasi atau game sehingga akses pengguna terhadap layanan tersebut dapat dibatasi atau diblokir sesuai kebijakan jaringan yang diterapkan (Roberts Tamu Umbu et al., 2024).

Dapat disimpulkan bahwa Layer *Packet Filtering* merupakan metode penyaringan paket data pada *firewall* jaringan yang bekerja pada layer aplikasi (*Layer 7*) untuk mengontrol lalu lintas data berdasarkan *Protocol*, isi paket, aplikasi, alamat situs, maupun port tertentu. Metode ini digunakan untuk meningkatkan keamanan jaringan dengan cara memblokir akses terhadap situs web, media sosial, aplikasi, maupun game *online* yang tidak diizinkan pada jaringan komputer.

2.7 *Queue Tree* Dan *PCQ*

2.7.1 *Queue Tree*

Queue Tree adalah metode manajemen *bandwidth* berbasis *Mikrotik* yang digunakan untuk meningkatkan kualitas layanan jaringan melalui pembatasan *bandwidth* pada setiap perangkat yang terhubung ke jaringan. Dengan penerapan *Queue Tree*, penggunaan *bandwidth* menjadi lebih stabil, merata, dan efisien sehingga aktivitas jaringan dapat berjalan dengan lebih baik tanpa menyebabkan koneksi *internet* melambat pada pengguna lainnya (nasir et al., 2023).

Queue Tree merupakan teknik pengaturan *bandwidth* yang memanfaatkan mekanisme *Hierarchical Token Bucket (HTB)* untuk mengelola antrian paket data sehingga distribusi *bandwidth* dapat dilakukan secara lebih efisien dan sesuai kebutuhan pengguna. Penelitian tersebut menjelaskan bahwa *Queue Tree* mampu mengurangi terjadinya perebutan *bandwidth* antar pengguna karena trafik dapat diprioritaskan berdasarkan

aturan tertentu.

Selain itu *Queue Tree* efektif digunakan untuk optimalisasi *bandwidth* pada jaringan perusahaan maupun institusi pendidikan. Dengan *Queue Tree*, administrator dapat menentukan batas minimum dan maksimum *bandwidth* pada setiap bagian jaringan sehingga penggunaan *internet* menjadi lebih stabil dan terkontrol.

Secara umum, *Queue Tree* memiliki kelebihan berupa kemampuan pengaturan *bandwidth* yang detail, fleksibel, dan mendukung prioritas trafik tertentu seperti video *conference*, *browsing*, maupun *streaming*. Namun, *Konfigurasi Queue Tree* relatif lebih kompleks karena memerlukan proses *mangle* untuk menandai paket data sebelum dilakukan pengaturan *bandwidth*.

2.7.2 *PCQ* (*Per Connection Queue*)

Peer Connection Queue (*PCQ*) merupakan metode manajemen *bandwidth* yang digunakan untuk mengatur dan membagi *bandwidth* secara otomatis kepada setiap pengguna atau koneksi pada jaringan komputer. Metode *PCQ* diterapkan bersama *Queue Tree* untuk mengoptimalkan penggunaan *bandwidth* sehingga setiap klien memperoleh alokasi *bandwidth* yang sesuai tanpa saling berebut koneksi *internet*.

Penerapan metode *PCQ* mampu meningkatkan kualitas jaringan karena *bandwidth* dibagi berdasarkan aturan manajemen *bandwidth* yang telah ditentukan. Dengan menggunakan metode *PCQ*, setiap pengguna mendapatkan pembagian *bandwidth* yang lebih adil sehingga aktivitas *internet*, seperti *browsing*, upload, download, dan penggunaan layanan lainnya dapat berjalan lebih stabil dan optimal.

PCQ adalah metode pembagian *bandwidth* yang digunakan untuk memberikan pengalaman *Quality Of Service (QoS)* yang baik bagi seluruh pengguna jaringan *internet*. Metode ini bekerja dengan cara membagi *bandwidth* secara merata kepada setiap klien menggunakan *Queue Tree* sehingga koneksi *internet* menjadi lebih stabil dan tidak terjadi ketimpangan penggunaan *bandwidth* antar pengguna jaringan (Mufrot & Sobari, 2023).

Metode *PCQ* sangat efektif diterapkan pada jaringan berbasis *Mikrotik*

karena mampu mengatasi masalah distribusi *bandwidth* yang tidak merata. Dengan penerapan *PCQ*, seluruh pengguna yang terhubung ke jaringan memperoleh alokasi *bandwidth* yang seimbang sehingga kualitas layanan *internet* menjadi lebih baik dan pengguna merasa lebih adil dalam penggunaan jaringan *internet*.

Selain itu, *PCQ* digunakan sebagai metode *bandwidth* management untuk meningkatkan performa jaringan melalui pengaturan upload dan download *bandwidth* berdasarkan *Source address* dan *Destination address*. Dengan penerapan metode ini, penggunaan *bandwidth* menjadi lebih efisien, koneksi *internet* lebih stabil, serta mampu mengurangi gangguan jaringan akibat penggunaan *bandwidth* berlebih oleh pengguna tertentu.

2.8 Mekanisme *Bufferbloat* Dan Dampaknya Pada QoS

Secara teknis, *Bufferbloat* terjadi karena tiga faktor interaktif adanya bottleneck link di mana kecepatan ingress melebihi kapasitas egress, ukuran buffer router yang terlalu besar akibat penurunan harga memori sehingga pabrikan memaksimalkan kapasitas buffer, dan ketidakmampuan mekanisme FIFO (First In First Out) bawaan router untuk melakukan drop paket lebih awal sebelum buffer terisi penuh (Gettys & Nichols, 2011).

Dampak *Bufferbloat* pada parameter QoS dapat dijabarkan sebagai berikut. Pertama, *Delay* meningkat secara dramatis karena paket harus menunggu antrian panjang untuk ditransmisikan. Kedua, *Jitter* meningkat karena waktu tunggu paket bervariasi bergantung pada seberapa penuh buffer pada saat paket tiba. Ketiga, meskipun buffer yang besar menunda *Packet Loss*, *Throughput* efektif akhirnya menurun karena mekanisme TCP congestion control bereaksi terlambat dan window size tidak disesuaikan tepat waktu. Keempat, *Packet Loss* akhirnya tetap terjadi ketika buffer benar-benar terisi penuh (tail drop), namun dengan dampak yang lebih parah karena loss bersifat burst.

2.9 Teknik Mitigasi *Bufferbloat*

Komunitas riset jaringan telah mengembangkan beberapa pendekatan mitigasi *Bufferbloat* yang berkembang secara bertahap:

2.9.1 *Active Queue Management (AQM)*

AQM adalah pendekatan di mana router secara proaktif mendrop atau menandai paket sebelum buffer terisi penuh, sehingga sinyal kongesti mencapai pengirim lebih awal. Algoritma *RED (Random Early Detection)* merupakan AQM generasi pertama yang direkomendasikan IETF, namun memiliki kelemahan dalam hal kompleksitas konfigurasi (Floyd & Jacobson, 1993).

2.9.2 CoDel Dan *FQ-CoDel*

CoDel (Controlled Delay) mengatasi keterbatasan RED dengan mengukur sojourn time (waktu paket berada dalam antrian) daripada panjang antrian. Jika sojourn time melebihi target (5ms secara default), CoDel mulai mendrop paket secara adaptif. *FQ-CoDel* kemudian menambahkan Fair Queuing (pemisahan arus per aliran) ke mekanisme CoDel, menjadikannya solusi yang lebih efektif untuk lingkungan multi-pengguna (Nichols & Jacobson 2012).

2.9.3 *CAKE (Common Applications Kept Enhanced)*

CAKE merupakan evolusi dari *FQ-CoDel* yang mengintegrasikan traffic shaping, flow isolation, dan AQM dalam satu mekanisme terpadu. CAKE unggul dibandingkan *FQ-CoDel* dalam skenario jaringan dengan beban asimetris dan multiple bottleneck. Pada RouterOS *Mikrotik* versi 7, CAKE telah tersedia sebagai Queue Type pilihan (Høiland-Jørgensen et al. (2018).

2.9.4 *Packet Filtering* Dan *Queue Tree* Sebagai Mitigasi Pada *Mikrotik*

Pada platform *Mikrotik RouterOS*, mekanisme mitigasi *Bufferbloat* dapat diimplementasikan melalui kombinasi packet marking (Firewall Mangle), *Queue Tree*, dan *Per Connection Queue (PCQ)*. Meskipun tidak mengimplementasikan AQM murni seperti CoDel, kombinasi ini efektif karena *Packet Filtering* menyaring trafik tidak produktif yang berkontribusi pada pengisian buffer, *Queue Tree* mengimplementasikan *Hierarchical Token Bucket (HTB)* yang membatasi burst traffic penyebab buffer overflow, dan PCQ mendistribusikan bandwidth secara adil sehingga tidak ada aliran

tunggal yang mendominasi buffer.

2.10 Kerangka Berpikir

Kerangka berpikir dalam penelitian ini disusun berdasarkan permasalahan yang terjadi pada jaringan *internet* di SMKS Al-Islam Joresan Mlarak Ponorogo. Permasalahan utama yang ditemukan adalah penggunaan *bandwidth* yang tidak merata akibat tingginya aktivitas pengguna jaringan, seperti *streaming* video, media sosial, download file berukuran besar, dan aktivitas *internet* lainnya yang dilakukan secara bersamaan. Kondisi tersebut menyebabkan kualitas layanan jaringan menurun yang ditandai dengan koneksi lambat, tingginya *Delay*, *Jitter*, serta terjadinya *Packet Loss* pada jaringan sekolah.

Tahap pertama dalam penelitian ini dimulai dari identifikasi permasalahan jaringan. Pada tahap ini dilakukan pengamatan terhadap kondisi jaringan yang sedang berjalan untuk mengetahui penyebab terjadinya gangguan kualitas layanan *internet*. Identifikasi dilakukan dengan melihat kestabilan koneksi, penggunaan *bandwidth*, serta pola akses pengguna jaringan di lingkungan sekolah.

Setelah permasalahan jaringan diketahui, tahap berikutnya adalah analisis trafik jaringan. Analisis trafik dilakukan untuk mengetahui jenis lalu lintas data yang paling banyak menggunakan *bandwidth* dan berpotensi menyebabkan gangguan jaringan. Trafik yang dianalisis meliputi aktivitas *streaming*, game *online*, media sosial, upload dan download file, serta layanan *internet* lainnya. Tahap ini bertujuan untuk menentukan jenis trafik yang perlu dikendalikan melalui mekanisme *Packet Filtering*.

Tahap selanjutnya adalah penerapan *Packet Filtering* pada perangkat *Mikrotik*. *Packet Filtering* dilakukan menggunakan fitur *firewall Mikrotik* untuk menyaring dan mengontrol paket data tertentu sesuai aturan yang telah ditetapkan. Melalui *Packet Filtering*, trafik yang dianggap mengganggu kestabilan jaringan dapat dibatasi sehingga penggunaan *bandwidth* menjadi lebih teratur dan terkendali.

Setelah *Packet Filtering* diterapkan, dilakukan pengukuran *Quality Of*

Service (QoS) untuk mengetahui pengaruh penerapan *Packet Filtering* terhadap kualitas jaringan. Parameter *QoS* yang digunakan dalam penelitian ini meliputi *Throughput*, *Delay*, *Jitter*, dan *Packet Loss*. Pengukuran dilakukan sebelum dan sesudah penerapan *Packet Filtering* untuk memperoleh perbandingan kualitas layanan jaringan secara objektif.

Tahap berikutnya adalah pengujian jaringan. Pengujian dilakukan menggunakan tools monitoring jaringan untuk memperoleh data performa jaringan setelah *Konfigurasi Packet Filtering* diterapkan. Hasil pengujian kemudian dianalisis untuk mengetahui tingkat efektivitas *Packet Filtering* dalam meningkatkan kualitas layanan jaringan *internet*.

Berdasarkan hasil analisis tersebut, diperoleh *Konfigurasi* optimal jaringan yang mampu meningkatkan kestabilan koneksi, mengurangi trafik yang tidak diperlukan, serta menjaga kualitas layanan *internet* agar lebih baik bagi seluruh pengguna jaringan di SMKS Al-Islam Joresan Mlarak Ponorogo.

Gambar 2.10 Kerangka Berpikir

BAB III
METODE PENELITIAN

3.1 Jenis, Sifat, Dan Pendekatan Penelitian

Penelitian ini menggunakan metode eksperimen kuantitatif dengan pendekatan jaringan nyata real-network study. Tiga skenario pengujian dilaksanakan secara bertahap baseline tanpa mitigasi, penerapan *Packet Filtering*, dan penerapan kombinasi QoS+Filtering. Setiap skenario diukur menggunakan Wireshark dan Speedtest untuk mendapatkan nilai *Throughput*, *Delay*, *Jitter*, dan *Packet Loss*. Pendekatan ini konsisten dengan metodologi dalam studi AQM di jaringan universitas nyata (Barczyk & Chydzinski 2022).

3.2 Metode Pengumpulan Data

Metode pengumpulan data merupakan tahapan yang dilakukan peneliti untuk memperoleh data dan informasi yang dibutuhkan dalam penelitian. Pada penelitian yang berjudul "Analisis Mitigasi *Bufferbloat* Untuk Peningkatan *Quality Of Service* Pada Jaringan Pendidikan Berbasis *Mikrotik* (Studi Kasus Di SMKS Al-Islam Joresan Mlarak Ponorogo)", metode pengumpulan data dilakukan untuk mengetahui kondisi jaringan sebelum dan sesudah penerapan *Packet Filtering* pada *Router Mikrotik*. Data yang diperoleh nantinya digunakan sebagai dasar dalam melakukan analisis terhadap pengaruh *Packet Filtering* terhadap kualitas layanan jaringan.

3.2.1 Observasi

Metode observasi dilakukan dengan cara mengamati secara langsung kondisi jaringan komputer yang digunakan di SMKS Al-Islam Joresan Mlarak Ponorogo. Observasi bertujuan untuk memperoleh gambaran nyata mengenai sistem jaringan yang sedang berjalan, termasuk perangkat jaringan yang digunakan, topologi jaringan, penggunaan *bandwidth internet*, serta kondisi lalu lintas data pada jaringan sekolah. Selain itu, observasi juga dilakukan terhadap *Konfigurasi firewall* dan *Packet Filtering* pada *Router Mikrotik* untuk mengetahui bagaimana sistem pengelolaan jaringan diterapkan.

Penelitian ini dilaksanakan di SMKS Al-Islam Joresan Mlarak Ponorogo yang beralamat di Kecamatan Mlarak, Kabupaten Ponorogo, Jawa

Timur. Pemilihan lokasi penelitian didasarkan pada kondisi jaringan *internet* sekolah yang digunakan secara bersama oleh guru, tenaga administrasi, dan siswa sehingga sering terjadi kepadatan trafik jaringan pada waktu tertentu.

Jaringan *internet* di SMKS Al-Islam Joresan Mlarak Ponorogo menggunakan *Router Mikrotik* sebagai pusat pengelolaan jaringan. Namun, pada implementasinya masih ditemukan beberapa permasalahan seperti pembagian *bandwidth* yang belum merata, tingginya penggunaan *bandwidth* oleh pengguna tertentu, serta belum adanya prioritas trafik untuk layanan penting seperti video *conference* dan pembelajaran daring.

Melalui metode observasi, peneliti dapat mengetahui kondisi awal jaringan sebelum dilakukan penerapan *Packet Filtering*. Hasil observasi ini menjadi dasar dalam menentukan langkah pengujian dan analisis *Quality Of Service (QoS)* pada jaringan sekolah.

3.2.2 Wawancara

Metode wawancara dilakukan dengan cara melakukan tanya jawab secara langsung kepada pihak yang bertanggung jawab terhadap pengelolaan jaringan *internet* di sekolah, seperti administrator jaringan atau teknisi laboratorium komputer. Wawancara bertujuan untuk memperoleh informasi yang lebih mendalam mengenai kondisi jaringan, permasalahan yang sering terjadi, serta pengelolaan *bandwidth internet* pada jaringan sekolah.

Dalam proses wawancara, peneliti menggali informasi terkait penerapan *Packet Filtering* pada *Router Mikrotik*, kendala yang dihadapi dalam menjaga stabilitas jaringan, serta kebutuhan pengguna jaringan terhadap kualitas layanan *internet*. Data hasil wawancara digunakan sebagai pendukung data observasi sehingga informasi yang diperoleh menjadi lebih lengkap dan akurat.

3.2.3 Dokumentasi

Metode dokumentasi dilakukan dengan cara mengumpulkan berbagai dokumen yang berkaitan dengan penelitian. Dokumentasi digunakan untuk memperkuat data hasil observasi dan wawancara yang telah dilakukan sebelumnya. Dokumen yang dikumpulkan meliputi struktur atau topologi

jaringan sekolah, *Konfigurasi Router Mikrotik*, data penggunaan *bandwidth*, screenshot *Konfigurasi Packet Filtering*, hasil pengujian jaringan, serta dokumentasi kegiatan penelitian.

Selain itu, dokumentasi juga mencakup data log aktivitas jaringan dan foto perangkat jaringan yang digunakan dalam penelitian. Data dokumentasi tersebut digunakan sebagai bukti pendukung agar hasil penelitian dapat dipertanggungjawabkan secara ilmiah.

3.2.4 Eksperimen Pengujian

Pada penelitian ini dilakukan tiga skenario eksperimen untuk menganalisis pengaruh *Packet Filtering* terhadap kualitas layanan jaringan (*Quality Of Service/QoS*) pada jaringan *Mikrotik* di SMKS Al-Islam Joresan Mlarak Ponorogo. Setiap skenario dirancang secara bertahap mulai dari kondisi jaringan normal tanpa pengaturan, penerapan *Packet Filtering*, hingga implementasi *QoS* menggunakan metode *Queue Tree* dan *Per Connection Queue (PCQ)*.

Pelaksanaan skenario eksperimen dilakukan untuk memperoleh data pengukuran *QoS* berupa *Throughput, Delay, Jitter*, dan *Packet Loss* pada setiap kondisi jaringan. Hasil pengukuran tersebut kemudian dibandingkan untuk mengetahui pengaruh *Konfigurasi* jaringan terhadap kualitas layanan *internet*.

3.2.4.1 Skenario 1 *Baseline*

Skenario pertama merupakan tahap pengujian awal (*Baseline*) yang dilakukan pada kondisi jaringan asli tanpa penerapan *Packet Filtering* maupun *Konfigurasi QoS*. Pada tahap ini *Router Mikrotik* hanya berfungsi sebagai penghubung jaringan *internet* tanpa adanya pengaturan manajemen *bandwidth* dan prioritas trafik.

Pada skenario ini seluruh pengguna jaringan memperoleh akses *internet* secara langsung tanpa pembatasan trafik tertentu. *Bandwidth* digunakan secara bebas oleh seluruh pengguna sehingga kemungkinan terjadinya perebutan *bandwidth* antar pengguna masih sangat tinggi. Kondisi ini digunakan untuk mengetahui performa awal jaringan sebelum dilakukan optimasi. Karakteristik pada skenario *Baseline* meliputi tidak

menggunakan *Packet Filtering*, tidak menggunakan *QoS*, tidak menggunakan *Queue Tree*, tidak menggunakan metode *PCQ*, tidak terdapat prioritas trafik, dan jaringan berjalan sesuai kondisi asli.

Tujuan utama dari skenario ini adalah untuk memperoleh data awal kualitas layanan jaringan sebagai pembanding terhadap skenario berikutnya. Pengukuran dilakukan pada kondisi jaringan normal sehingga dapat diketahui tingkat performa jaringan sebelum dilakukan pengaturan *bandwidth* dan filtering trafik. Pada tahap ini dilakukan pengukuran terhadap parameter *QoS* yang meliputi *Throughput*, *Delay*, *Jitter*, dan *Packet Loss*. Hasil pengukuran pada skenario *Baseline* akan digunakan sebagai acuan dalam mengevaluasi peningkatan performa jaringan setelah implementasi *Packet Filtering* dan *QoS*.

Jaringan beroperasi tanpa konfigurasi filtering maupun QoS. Kondisi ini merepresentasikan situasi *Bufferbloat* yang tidak dimitigasi, di mana buffer router dapat terisi bebas oleh trafik dari semua pengguna.

3.2.4.2 Skenario 2 *Packet Filtering*

Skenario kedua merupakan tahap implementasi *Packet Filtering* pada *Router Mikrotik* menggunakan fitur *firewall* filter. Pada tahap ini dilakukan pengaturan untuk membatasi, menyaring, dan mengontrol trafik tertentu yang dianggap dapat mempengaruhi performa jaringan *internet*.

Implementasi *Packet Filtering* dilakukan dengan membuat aturan (rule) pada *firewall* filter *Mikrotik* untuk memblokir atau membatasi jenis trafik tertentu berdasarkan *Port*, protokol, maupun layanan jaringan tertentu. Filtering dilakukan terhadap trafik yang tidak diperlukan atau berpotensi mengganggu stabilitas jaringan. *Konfigurasi* yang diterapkan pada skenario ini meliputi *firewall* filter, filtering *port* tertentu, filtering protokol tertentu, pembatasan trafik tertentu, dan pemblokiran akses yang tidak diperlukan.

Tujuan dari skenario ini adalah untuk mengetahui pengaruh penerapan *Packet Filtering* terhadap kualitas layanan jaringan *internet*.

Dengan adanya filtering diharapkan trafik yang tidak penting dapat dikurangi sehingga penggunaan *bandwidth* menjadi lebih efisien dan stabil.

Pada tahap ini dilakukan pengujian kembali terhadap parameter *QoS* untuk mengetahui perubahan kualitas jaringan setelah penerapan *Packet Filtering*. Hasil pengukuran kemudian dibandingkan dengan skenario *Baseline* untuk mengetahui tingkat perubahan performa jaringan. Parameter *QoS* yang diukur pada tahap ini meliputi *Throughput, Delay, Jitter*, dan *Packet Loss*. Melalui pengujian ini dapat diketahui apakah implementasi *Packet Filtering* mampu meningkatkan kualitas layanan jaringan tanpa penerapan manajemen *bandwidth* tambahan.

Firewall Filter diterapkan untuk memblokir trafik tidak produktif (game online, non-educational streaming). Packet marking melalui Firewall Mangle diaktifkan untuk klasifikasi trafik. Skenario ini menguji hipotesis bahwa pengurangan beban trafik irrelevan dapat menekan tekanan pada buffer router.

3.2.4.3 Skenario 3 *QoS* + Filtering

Skenario ketiga merupakan tahap optimasi jaringan dengan menggabungkan implementasi *QoS* dan *Packet Filtering* pada *Router Mikrotik*. Pada tahap ini dilakukan pengaturan manajemen *bandwidth* menggunakan metode *Queue Tree* dan *Per Connection Queue (PCQ)* untuk meningkatkan kualitas layanan jaringan *internet*.

Implementasi *QoS* dilakukan dengan memanfaatkan fitur *mangle* pada *Mikrotik* untuk melakukan packet *marking* terhadap trafik tertentu. Selanjutnya trafik yang telah ditandai akan diatur menggunakan *Queue Tree* dan *PCQ* berdasarkan tingkat prioritas layanan. *Konfigurasi* yang diterapkan pada tahap ini meliputi packet *marking*, *mangle*, *Queue Tree*, *PCQ*, prioritas trafik, dan pengaturan *bandwidth*.

Kombinasi lengkap: Firewall Filter + Packet Marking + *Queue Tree* + PCQ. *Queue Tree* mengimplementasikan HTB dengan prioritas untuk trafik pendidikan. PCQ mendistribusikan bandwidth secara adil. Skenario ini merepresentasikan mitigasi *Bufferbloat* yang komprehensif

Dalam penelitian ini trafik jaringan dibagi menjadi beberapa tingkat prioritas berdasarkan kebutuhan layanan jaringan. Trafik yang membutuhkan koneksi stabil dan latensi rendah akan diberikan prioritas lebih tinggi dibandingkan trafik biasa. Pengelompokan prioritas trafik dilakukan sebagai berikut:

Tabel 3.2.4.3 Pengelompokan Prioritas Trafik

No	Prioritas	Jenis Trafik
1.	Prioritas Tinggi	Pembelajaran Daring (*Gamelab*)
2.	Prioritas Tinggi	Video *Conference* (Zoom)
3.	Prioritas Sedang	Web *Browsing*
4.	Prioritas Rendah	Download Biasa

Trafik pembelajaran daring (*gamelab*) dan video *conference* diberikan prioritas tinggi karena layanan tersebut membutuhkan koneksi yang stabil dengan *Delay* dan *Jitter* rendah agar komunikasi dapat berjalan dengan baik. Sementara itu, aktivitas web *browsing* diberikan prioritas sedang dan aktivitas download biasa ditempatkan pada prioritas rendah karena tidak terlalu sensitif terhadap keterlambatan jaringan.

Tujuan utama dari skenario ini adalah untuk menentukan *Konfigurasi QoS* yang paling optimal dalam meningkatkan kualitas layanan jaringan *internet* di lingkungan sekolah. Dengan metode *Queue Tree* dan *PCQ*, *bandwidth* dapat dibagi secara merata kepada seluruh pengguna jaringan sehingga tidak terjadi monopoli *bandwidth* oleh pengguna tertentu.

Selain itu, penerapan prioritas trafik memungkinkan layanan penting seperti *gamelab* dan zoom memperoleh kualitas layanan yang lebih baik dibandingkan trafik lainnya. Dengan demikian, jaringan *internet* di sekolah diharapkan menjadi lebih stabil, efisien, dan mampu mendukung kegiatan pembelajaran berbasis teknologi informasi. Pada tahap ini dilakukan pengukuran kembali terhadap parameter *QoS* berupa *Throughput, Delay, Jitter*, dan *Packet Loss*.

Hasil pengukuran kemudian dibandingkan dengan skenario sebelumnya untuk mengetahui tingkat peningkatan kualitas layanan jaringan setelah implementasi *QoS* dan *Packet Filtering*.

3.3 Metode Analisis Data

Metode analisis data merupakan tahapan yang dilakukan untuk mengolah data hasil penelitian sehingga dapat digunakan untuk menjawab rumusan masalah dan tujuan penelitian. Pada penelitian yang berjudul "Analisis Mitigasi *Bufferbloat* Untuk Peningkatan *Quality Of Service* Pada Jaringan Pendidikan Berbasis *Mikrotik* (Studi Kasus Di SMKS Al-Islam Joresan Mlarak Ponorogo)", metode analisis data yang digunakan adalah metode analisis deskriptif kuantitatif. Metode ini digunakan untuk menganalisis dan membandingkan nilai *Quality Of Service (QoS)* sebelum dan sesudah penerapan *Packet Filtering* pada *Router Mikrotik*.

Data yang diperoleh dari hasil observasi, wawancara, dokumentasi, dan eksperimen terlebih dahulu dikumpulkan dan dikelompokkan berdasarkan parameter *Quality Of Service (QoS)*, yaitu *Throughput*, *Delay*, *Jitter*, dan *Packet Loss*. Selanjutnya data tersebut diolah untuk mengetahui perubahan kualitas layanan jaringan setelah dilakukan penerapan *Packet Filtering*.

Pada tahap awal, peneliti melakukan pengukuran kondisi jaringan sebelum penerapan *Packet Filtering*. Pengukuran dilakukan untuk memperoleh nilai awal dari parameter *QoS* yang digunakan dalam penelitian. Setelah itu dilakukan *Konfigurasi Packet Filtering* pada *Router Mikrotik* sesuai kebutuhan pengelolaan jaringan sekolah. Selanjutnya dilakukan kembali pengukuran *QoS* untuk memperoleh data kondisi jaringan sesudah penerapan *Packet Filtering*.

Data hasil pengukuran kemudian dianalisis dengan cara membandingkan nilai parameter *QoS* sebelum dan sesudah penerapan *Packet Filtering*. analisis dilakukan untuk mengetahui apakah penerapan *Packet Filtering* memberikan pengaruh terhadap peningkatan kualitas layanan jaringan. Semakin baik nilai *Throughput* dan semakin kecil nilai *Delay*, *Jitter*, serta *Packet Loss*, maka kualitas jaringan dinilai semakin baik.

Dalam proses analisis data, peneliti menggunakan standar *Quality Of Service (QoS)* untuk menentukan kategori kualitas jaringan. Hasil pengukuran dapat disajikan dalam bentuk tabel maupun grafik agar mempermudah proses analisis dan interpretasi data. Penyajian data tersebut bertujuan untuk melihat perbedaan kualitas jaringan secara lebih jelas sebelum dan sesudah penerapan *Packet Filtering*.

3.3.1 Parameter Pengukuran

Semua parameter diukur berdasarkan standar TIPHON (Telecommunications and *Internet* Protocol Harmonization Over Networks) sesuai standar ETSI TR 101 329:

Tabel 3.3.1 Parameter Pengukuran

No	Parameter	Sangat Baik	Baik	Sedang/Buruk
1.	*Throughput*	> 100% nominal	> 75%	< 75%
2.	*Delay*	< 150 ms	150–300 ms	> 300 ms
3.	*Jitter*	< 20 ms	20–50 ms	> 50 ms
4.	*Packet Loss*	0%	< 1%	> 1%

3.3.1.1 *Throughput*

Throughput merupakan jumlah data yang berhasil dikirim dan diterima melalui jaringan dalam satuan waktu tertentu. Parameter ini menunjukkan tingkat kecepatan efektif transfer data pada jaringan komputer. Semakin besar nilai *Throughput*, maka semakin baik kualitas jaringan karena proses pengiriman data dapat berlangsung lebih cepat dan stabil.

Dalam penelitian ini, pengukuran *Throughput* dilakukan menggunakan aplikasi *Wireshark* dengan cara melakukan *capture traffic* pada jaringan selama proses pengujian berlangsung. Data yang diperoleh kemudian dianalisis untuk mengetahui rata-rata kecepatan transfer data pada setiap skenario eksperimen. Nilai *Throughput* dipengaruhi oleh

beberapa faktor, seperti kapasitas *bandwidth*, kepadatan trafik jaringan, kualitas perangkat jaringan, pengaturan *QoS*, dan jumlah pengguna aktif.

Pengukuran *Throughput* pada penelitian ini bertujuan untuk mengetahui seberapa besar pengaruh *Packet Filtering* dan *QoS* terhadap peningkatan kecepatan transfer data pada jaringan sekolah.

3.3.1.2 *Delay*

Delay merupakan waktu yang dibutuhkan paket data untuk melakukan perjalanan dari sumber menuju tujuan dalam jaringan komputer. Parameter ini sering disebut sebagai waktu tunda (*latency*). Semakin kecil nilai *Delay*, maka semakin baik kualitas jaringan karena proses komunikasi data berlangsung lebih cepat.

Pada penelitian ini, pengukuran *Delay* dilakukan menggunakan perintah ping terhadap perangkat tujuan yang terhubung dalam jaringan. Hasil pengujian akan menunjukkan waktu rata-rata pengiriman paket data dalam satuan milidetik (ms). Beberapa faktor yang mempengaruhi nilai *Delay* antara lain jarak pengiriman data, kepadatan trafik jaringan, kualitas media transmisi, beban *Router* dan *switch*, dan pengaturan antrean (queue).

Nilai *Delay* sangat penting terutama pada layanan *real-time* seperti video *conference*, *VoIP*, pembelajaran daring, *e-learning*, dan *streaming* video. Pada penelitian ini, pengukuran *Delay* digunakan untuk mengetahui tingkat respons jaringan setelah penerapan *Packet Filtering* dan *QoS*.

3.3.1.3 *Jitter*

Jitter merupakan variasi waktu kedatangan paket data pada jaringan komputer. Parameter ini menunjukkan kestabilan pengiriman paket data selama proses komunikasi berlangsung. Semakin kecil nilai *Jitter*, maka jaringan dianggap semakin stabil.

Pengukuran *Jitter* pada penelitian ini dilakukan menggunakan aplikasi *Wireshark* melalui analisis hasil *capture traffic* jaringan. Nilai *Jitter* diperoleh dari perbedaan waktu kedatangan antar paket data selama proses transmisi berlangsung. Faktor-faktor yang mempengaruhi *Jitter* antara lain

kepadatan trafik jaringan, antrean paket data, kemacetan jaringan (*network congestion*), dan kualitas *Konfigurasi QoS*.

Nilai *Jitter* sangat berpengaruh pada layanan komunikasi *real-time* seperti *VoIP*, video *conference*, dan *streaming* audio dan video. Jika nilai *Jitter* terlalu tinggi, maka komunikasi suara dan video dapat mengalami gangguan seperti suara terputus-putus atau tampilan video yang tidak stabil. Oleh karena itu, parameter *Jitter* menjadi salah satu indikator penting dalam penelitian *QoS*.

3.3.1.4 *Packet Loss*

Packet Loss merupakan jumlah paket data yang hilang atau gagal diterima oleh tujuan selama proses transmisi data berlangsung. Hilangnya paket data dapat menyebabkan penurunan kualitas layanan jaringan karena data yang dikirim tidak dapat diterima secara lengkap.

Pada penelitian ini, pengukuran *Packet Loss* dilakukan menggunakan perintah ping dengan menghitung jumlah paket yang berhasil dikirim dan diterima selama proses pengujian jaringan. Beberapa faktor yang menyebabkan terjadinya *Packet Loss* antara lain kepadatan trafik jaringan, kerusakan perangkat jaringan, gangguan media transmisi, antrean jaringan yang penuh, dan *Konfigurasi* jaringan yang tidak optimal.

Semakin kecil nilai *Packet Loss*, maka kualitas jaringan semakin baik karena proses pengiriman data berlangsung lebih stabil dan minim gangguan. Dalam penelitian ini, parameter *Packet Loss* digunakan untuk mengetahui tingkat keberhasilan transmisi data setelah penerapan *Packet Filtering* dan *QoS* pada jaringan *Mikrotik*.

Berdasarkan parameter pengujian tersebut, hasil penelitian diharapkan dapat menunjukkan pengaruh penerapan *Packet Filtering* dan *QoS* terhadap peningkatan kualitas layanan jaringan *internet* di SMKS Al-Islam Joresan Mlarak Ponorogo. Data hasil pengukuran dari setiap parameter akan dianalisis dan dibandingkan pada masing-masing skenario eksperimen untuk menentukan *Konfigurasi* jaringan yang paling optimal.

3.4 Alur Penelitian

Alur penelitian merupakan tahapan atau langkah-langkah sistematis yang dilakukan dalam proses penelitian mulai dari identifikasi masalah hingga penarikan kesimpulan. Pada penelitian yang berjudul "Analisis Mitigasi *Bufferbloat* Untuk Peningkatan *Quality Of Service* Pada Jaringan Pendidikan Berbasis *Mikrotik* (Studi Kasus Di SMKS Al-Islam Joresan Mlarak Ponorogo)", alur penelitian disusun secara terstruktur agar proses penelitian dapat berjalan dengan baik dan sesuai dengan tujuan yang ingin dicapai.

Penelitian ini bertujuan untuk mengetahui pengaruh penerapan *Packet Filtering* terhadap kualitas layanan jaringan atau *Quality Of Service (QoS)* pada jaringan *Mikrotik* di SMKS Al-Islam Joresan Mlarak Ponorogo. Tahapan penelitian dilakukan secara berurutan mulai dari pengamatan kondisi jaringan, perancangan sistem *Packet Filtering*, pengujian jaringan, hingga analisis hasil pengujian *QoS*.

3.4.1 Identifikasi Masalah

Tahap pertama dalam penelitian ini adalah identifikasi masalah. Pada tahap ini peneliti melakukan pengamatan awal terhadap kondisi jaringan komputer yang digunakan di sekolah. Pengamatan dilakukan untuk mengetahui berbagai permasalahan yang terjadi pada jaringan, seperti koneksi *internet* yang tidak stabil, penggunaan *bandwidth* yang tidak merata, tingginya trafik jaringan, serta menurunnya kualitas layanan jaringan ketika digunakan oleh banyak pengguna secara bersamaan. Selain itu, peneliti juga mengamati pengelolaan lalu lintas jaringan pada *Router Mikrotik* yang digunakan di sekolah. Berdasarkan hasil identifikasi tersebut, peneliti menentukan bahwa diperlukan penerapan *Packet Filtering* untuk membantu mengatur lalu lintas jaringan agar kualitas layanan jaringan menjadi lebih baik.

3.4.2 Studi *Literature*

Setelah melakukan identifikasi masalah, tahap selanjutnya adalah studi literatur. Pada tahap ini peneliti mempelajari berbagai teori dan referensi yang berkaitan dengan penelitian. Studi literatur dilakukan dengan mempelajari

buku, jurnal ilmiah, artikel penelitian, serta penelitian terdahulu yang membahas tentang jaringan komputer, *Packet Filtering*, *firewall*, dan *Quality Of Service (QoS)*. Peneliti juga mempelajari *Konfigurasi firewall* filter rule pada *Mikrotik* serta parameter *QoS* yang meliputi *Throughput, Delay*, *Jitter*, dan *Packet Loss*. Studi literatur dilakukan untuk memperoleh landasan teori yang digunakan sebagai dasar dalam pelaksanaan penelitian.

3.4.3 Pengumpulan Data

Tahap berikutnya adalah pengumpulan data. Pengumpulan data dilakukan menggunakan beberapa metode, yaitu observasi, wawancara, dokumentasi, dan eksperimen. Observasi dilakukan dengan mengamati kondisi jaringan sekolah secara langsung, termasuk topologi jaringan, perangkat jaringan, penggunaan *bandwidth*, dan kondisi trafik jaringan. Wawancara dilakukan kepada administrator jaringan atau teknisi laboratorium komputer untuk memperoleh informasi mengenai permasalahan jaringan, pengelolaan *bandwidth*, serta penggunaan *Router Mikrotik* di sekolah. Dokumentasi dilakukan dengan mengumpulkan data berupa topologi jaringan, *Konfigurasi Router Mikrotik*, screenshot *Konfigurasi firewall*, data penggunaan *bandwidth*, serta hasil pengujian jaringan. Selain itu, dilakukan eksperimen awal dengan mengukur kondisi jaringan sebelum penerapan *Packet Filtering* untuk memperoleh data awal *Quality Of Service (QoS)*.

3.4.4 Analisis Kebutuhan Sistem

Setelah data terkumpul, tahap selanjutnya adalah analisis kebutuhan sistem. Pada tahap ini peneliti menganalisis kebutuhan jaringan yang diperlukan dalam penerapan *Packet Filtering*. Analisis dilakukan terhadap topologi jaringan, jumlah pengguna jaringan, penggunaan *bandwidth*, jenis trafik jaringan, dan kebutuhan keamanan jaringan. Selain itu, peneliti juga menentukan parameter *QoS* yang akan diuji dalam penelitian, yaitu *Throughput, Delay*, *Jitter*, dan *Packet Loss*. Hasil analisis kebutuhan sistem digunakan sebagai dasar dalam merancang *Konfigurasi Packet Filtering* pada *Router Mikrotik*.

3.4.5 Perancangan Sistem *Packet Filtering*

Tahap berikutnya adalah perancangan sistem *Packet Filtering*. Pada tahap ini peneliti merancang *Konfigurasi firewall* filter rule pada *Router Mikrotik* sesuai dengan kebutuhan jaringan sekolah. Perancangan dilakukan dengan menentukan rule atau aturan yang digunakan untuk mengatur lalu lintas paket data pada jaringan. Peneliti menentukan jenis trafik yang diperbolehkan, trafik yang dibatasi atau diblokir, pengaturan akses pengguna jaringan, serta manajemen *bandwidth* jaringan. Perancangan sistem ini bertujuan agar lalu lintas jaringan dapat dikontrol dengan baik sehingga kualitas layanan jaringan menjadi lebih optimal.

3.4.6 Implementasi *Packet Filtering*

Setelah proses perancangan selesai, tahap selanjutnya adalah implementasi *Packet Filtering* pada *Router Mikrotik*. Implementasi dilakukan dengan memasukkan *Konfigurasi firewall* filter rule ke dalam *Router Mikrotik* menggunakan aplikasi *Winbox*. Pada tahap ini peneliti melakukan *Konfigurasi* rule *Packet Filtering*, mengatur action allow, drop, maupun reject pada trafik tertentu, serta melakukan pengecekan terhadap *Konfigurasi* yang telah diterapkan. Implementasi dilakukan agar pengelolaan lalu lintas jaringan menjadi lebih teratur dan penggunaan *bandwidth* dapat berjalan lebih optimal.

3.4.7 Pengujian *Quality Of Service (QoS)*

Tahap berikutnya adalah pengujian *Quality Of Service (QoS)*. Pengujian dilakukan untuk mengetahui pengaruh penerapan *Packet Filtering* terhadap kualitas layanan jaringan. Pengujian dilakukan dalam dua tahap, yaitu sebelum dan sesudah penerapan *Packet Filtering*. Parameter *QoS* yang diuji meliputi *Throughput*, *Delay*, *Jitter*, dan *Packet Loss*. Pengujian dilakukan menggunakan beberapa tools seperti *Wireshark*, *ping test*, *torch Mikrotik*, dan *bandwidth* test *Mikrotik*. Hasil pengujian dicatat dan digunakan sebagai data penelitian untuk dianalisis lebih lanjut.

3.4.8 Analisis Data

Tahap selanjutnya adalah analisis data. Pada tahap ini data hasil pengujian *QoS* dianalisis menggunakan metode deskriptif kuantitatif dengan

cara membandingkan hasil pengukuran sebelum dan sesudah penerapan *Packet Filtering*. Peneliti menghitung dan membandingkan nilai *Throughput, Delay*, *Jitter*, dan *Packet Loss* untuk mengetahui perubahan kualitas layanan jaringan setelah penerapan *Packet Filtering*. Data hasil pengujian kemudian disajikan dalam bentuk tabel dan grafik agar lebih mudah dipahami dan dianalisis.

3.4.9 Kesimpulan dan Saran

Tahap terakhir dalam penelitian ini adalah penarikan kesimpulan dan pemberian saran. Kesimpulan dibuat berdasarkan hasil analisis data yang telah dilakukan untuk mengetahui pengaruh *Packet Filtering* terhadap *Quality Of Service (QoS)* pada jaringan *Mikrotik* di SMKS Al-Islam Joresan Mlarak Ponorogo. Selain itu, peneliti juga memberikan saran yang dapat digunakan sebagai bahan pengembangan penelitian selanjutnya maupun sebagai rekomendasi dalam pengelolaan jaringan sekolah agar kualitas layanan jaringan menjadi lebih baik dan stabil di masa mendatang.

3.5 Alur Penelitian

Alur penelitian pada penelitian yang berjudul "Analisis Mitigasi *Bufferbloat* Untuk Peningkatan *Quality Of Service* Pada Jaringan Pendidikan Berbasis *Mikrotik* (Studi Kasus Di SMKS Al-Islam Joresan Mlarak Ponorogo)" dilakukan secara sistematis mulai dari tahap identifikasi masalah hingga penarikan kesimpulan dan saran. Setiap tahapan penelitian disusun untuk memperoleh hasil yang akurat mengenai pengaruh penerapan *Packet Filtering* terhadap kualitas layanan jaringan atau *Quality Of Service (QoS)* pada jaringan *Mikrotik* di lingkungan sekolah.

Tahap pertama dalam penelitian ini adalah identifikasi masalah. Pada tahap ini peneliti melakukan observasi awal terhadap kondisi jaringan komputer di SMKS Al-Islam Joresan Mlarak Ponorogo untuk mengetahui berbagai permasalahan yang terjadi pada jaringan. Permasalahan yang diamati meliputi koneksi *internet* yang tidak stabil, penggunaan *bandwidth* yang tidak merata, tingginya trafik jaringan, serta penurunan kualitas layanan jaringan ketika digunakan secara bersamaan oleh banyak pengguna. Selain itu, peneliti juga

mengidentifikasi pengelolaan lalu lintas data pada *Router Mikrotik* yang digunakan di sekolah. Hasil identifikasi masalah tersebut digunakan sebagai dasar dalam menentukan rumusan masalah dan tujuan penelitian.

Setelah tahap identifikasi masalah selesai, penelitian dilanjutkan dengan studi literatur. Pada tahap ini peneliti mempelajari berbagai teori dan referensi yang berkaitan dengan jaringan komputer, *Packet Filtering*, *firewall*, dan *Quality Of Service (QoS)*. Peneliti juga mempelajari *Konfigurasi firewall* filter rule pada *Mikrotik* serta metode pengukuran kualitas jaringan. Studi literatur dilakukan melalui buku, jurnal ilmiah, artikel penelitian, dan penelitian terdahulu yang relevan dengan topik penelitian. Tujuan studi literatur adalah untuk memperoleh landasan teori yang dapat digunakan sebagai dasar dalam proses penelitian dan analisis data.

Tahap berikutnya adalah pengumpulan data. Pengumpulan data dilakukan menggunakan metode observasi, wawancara, dokumentasi, dan eksperimen awal. Observasi dilakukan dengan mengamati kondisi jaringan sekolah secara langsung, termasuk topologi jaringan, perangkat jaringan, penggunaan *bandwidth*, dan kondisi trafik jaringan. Wawancara dilakukan kepada administrator jaringan atau teknisi laboratorium komputer untuk memperoleh informasi mengenai pengelolaan jaringan dan permasalahan yang sering terjadi. Dokumentasi dilakukan dengan mengumpulkan data berupa *Konfigurasi Router Mikrotik*, data *bandwidth*, topologi jaringan, dan hasil pengujian jaringan. Selain itu, dilakukan eksperimen awal berupa pengukuran *Quality Of Service (QoS)* sebelum penerapan *Packet Filtering* untuk memperoleh data awal kondisi jaringan.

Setelah data terkumpul, tahap selanjutnya adalah analisis kebutuhan sistem. Pada tahap ini peneliti menganalisis kondisi jaringan sekolah, seperti topologi jaringan, jumlah pengguna, jenis trafik jaringan, penggunaan *bandwidth*, dan kebutuhan keamanan jaringan. Hasil analisis digunakan untuk menentukan kebutuhan sistem *Packet Filtering* yang akan diterapkan pada *Router Mikrotik*. Peneliti juga menentukan parameter *QoS* yang akan diuji, yaitu *Throughput*, *Delay*, *Jitter*, dan *Packet Loss*.

Tahap berikutnya adalah pembuatan model atau perancangan sistem *Packet Filtering*. Pada tahap ini peneliti merancang *Konfigurasi Packet Filtering* sesuai kebutuhan jaringan sekolah. Perancangan dilakukan dengan menentukan rule *firewall* filter seperti *allow, drop*, dan *reject* untuk mengatur lalu lintas paket data pada jaringan. Selain itu, peneliti juga merancang pengaturan akses pengguna, pembatasan trafik tertentu, serta manajemen *bandwidth* agar penggunaan jaringan menjadi lebih optimal. Hasil dari tahap ini berupa desain *Konfigurasi Packet Filtering* yang akan diterapkan pada *Router Mikrotik*.

Setelah model selesai dirancang, tahap selanjutnya adalah implementasi model. Pada tahap ini peneliti menerapkan *Konfigurasi Packet Filtering* pada *Router Mikrotik* menggunakan aplikasi *Winbox*. Implementasi dilakukan dengan memasukkan rule *firewall* filter, melakukan pengaturan *NAT* jika diperlukan, serta mengaktifkan rule *Packet Filtering* sesuai desain yang telah dibuat. Setelah *Konfigurasi* diterapkan, dilakukan verifikasi awal untuk memastikan rule berjalan dengan baik dan konektivitas jaringan tetap stabil.

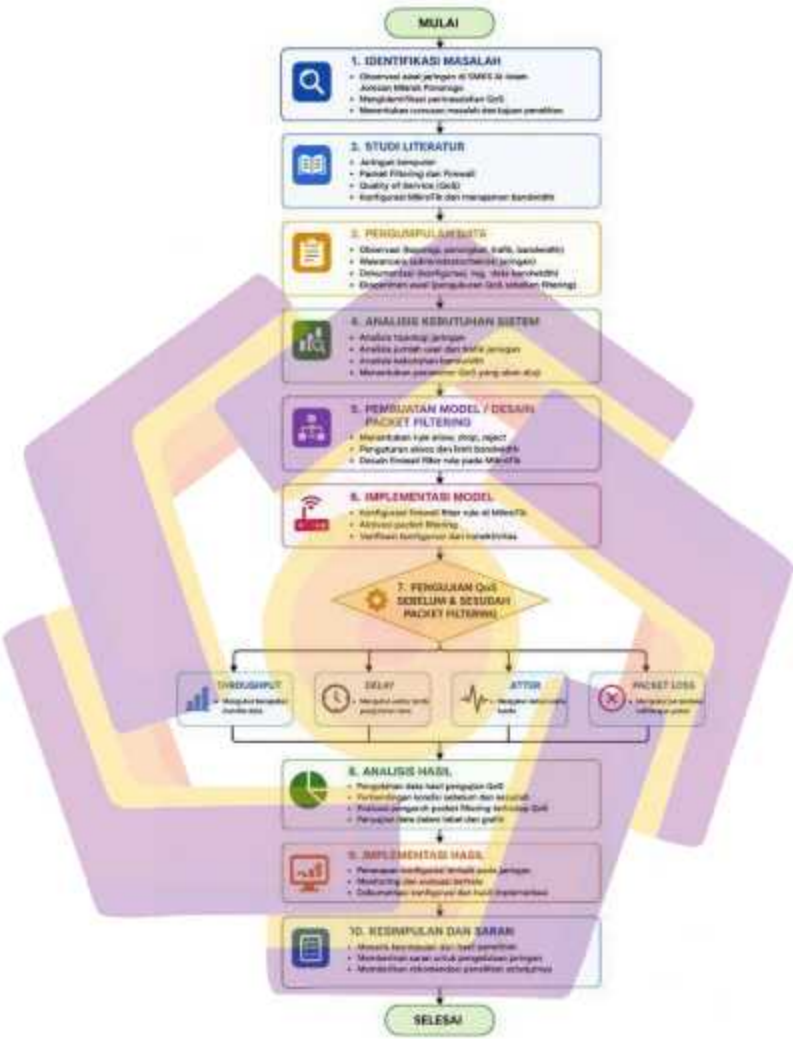
Tahap berikutnya adalah pengujian atau evaluasi model. Pengujian dilakukan untuk mengetahui pengaruh penerapan *Packet Filtering* terhadap *Quality Of Service (QoS)* pada jaringan sekolah. Pengujian dilakukan dalam dua kondisi, yaitu sebelum dan sesudah penerapan *Packet Filtering*. Parameter *QoS* yang diukur meliputi *Throughput, Delay, Jitter*, dan *Packet Loss*. Pengujian dilakukan menggunakan beberapa tools, seperti *Wireshark, ping test, torch Mikrotik, bandwidth* test, dan speedtest. Data hasil pengujian kemudian dicatat untuk dianalisis lebih lanjut.

Tahap selanjutnya adalah analisis hasil. Pada tahap ini data hasil pengujian *QoS* diolah dan dibandingkan antara kondisi sebelum dan sesudah penerapan *Packet Filtering*. Peneliti menghitung rata-rata nilai *Throughput, Delay, Jitter*, dan *Packet Loss* untuk mengetahui perubahan kualitas layanan jaringan. Hasil analisis kemudian disajikan dalam bentuk tabel dan grafik agar lebih mudah dipahami. Dari hasil analisis tersebut dapat diketahui apakah

Packet Filtering memberikan pengaruh terhadap peningkatan kualitas jaringan dan parameter *QoS* mana yang mengalami perubahan paling signifikan.

Setelah analisis selesai dilakukan, tahap berikutnya adalah implementasi hasil. Pada tahap ini hasil penelitian diterapkan dalam pengelolaan jaringan sekolah secara berkelanjutan. Peneliti menerapkan *Konfigurasi Packet Filtering* yang dianggap paling optimal berdasarkan hasil pengujian dan analisis. Selain itu, dilakukan monitoring jaringan secara berkala untuk memastikan kualitas layanan jaringan tetap stabil. Seluruh *Konfigurasi* dan hasil implementasi juga didokumentasikan sebagai bahan evaluasi dan referensi pengelolaan jaringan di masa mendatang.

Tahap terakhir dalam penelitian ini adalah penarikan kesimpulan dan pemberian saran. Kesimpulan dibuat berdasarkan hasil analisis dan pengujian yang telah dilakukan untuk menjawab rumusan masalah penelitian mengenai pengaruh *Packet Filtering* terhadap *Quality Of Service (QoS)* pada jaringan *Mikrotik* di SMKS Al-Islam Joresan Mlarak Ponorogo. Selain itu, peneliti juga memberikan saran terkait pengelolaan jaringan dan pengembangan penelitian selanjutnya agar kualitas layanan jaringan dapat terus ditingkatkan.



Gambar 3.5 Alur Penelitian

BAB IV
HASIL PENELITIAN DAN PEMBAHASAN

4.1 Perancangan Sistem Keamanan Jaringan

Perancangan sistem keamanan jaringan pada penelitian ini dilakukan untuk mendukung Implementasi *Packet Filtering* Dan *Quality Of Service (Qos)* Pada Jaringan *Mikrotik* Di SMKS Al-Islam Joresan Mlarak Ponorogo. Sistem keamanan jaringan dirancang untuk mengontrol lalu lintas data (traffic control), membatasi akses yang tidak diperlukan, serta menjaga stabilitas dan kualitas layanan jaringan *internet* di lingkungan sekolah.

Dalam penelitian ini, keamanan jaringan difokuskan pada penerapan *Packet Filtering* menggunakan fitur *firewall* filter pada *Router Mikrotik*. *Konfigurasi* tersebut bertujuan untuk menyaring paket data yang melewati jaringan berdasarkan aturan tertentu sehingga hanya trafik yang diizinkan saja yang dapat melewati sistem jaringan.

Perancangan keamanan jaringan dilakukan karena jaringan *internet* sekolah digunakan oleh banyak pengguna, seperti guru, tata usaha, dan siswa, sehingga diperlukan pengaturan akses jaringan yang baik agar penggunaan *bandwidth* lebih optimal dan terhindar dari penyalahgunaan jaringan.

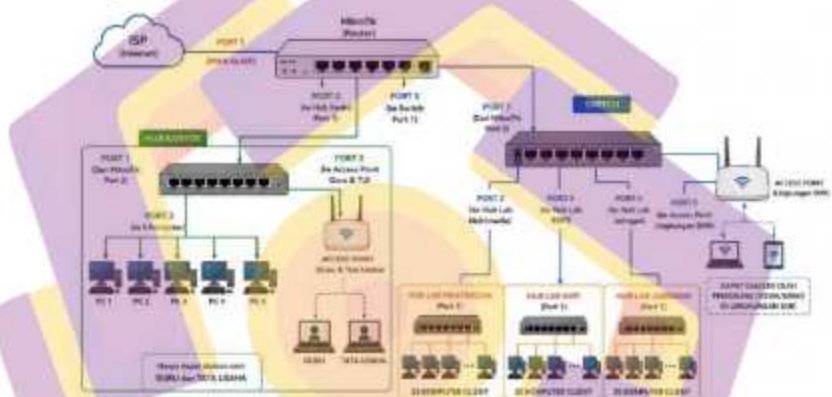
4.2 Implementasi Sistem

Implementasi sistem merupakan tahapan penerapan hasil perancangan sistem ke dalam lingkungan jaringan yang sebenarnya. Pada penelitian yang berjudul "Analisis Mitigasi *Bufferbloat* Untuk Peningkatan *Quality Of Service* Pada Jaringan Pendidikan Berbasis *Mikrotik* (Studi Kasus Di SMKS Al-Islam Joresan Mlarak Ponorogo)", implementasi sistem dilakukan dengan menerapkan *Konfigurasi Packet Filtering* pada *Router Mikrotik* untuk mengatur lalu lintas jaringan dan meningkatkan kualitas layanan jaringan atau *Quality Of Service (QoS)*.

Tahapan implementasi sistem dilakukan secara bertahap mulai dari implementasi topologi jaringan, *Konfigurasi* dasar jaringan, implementasi *Packet Filtering*, manajemen *bandwidth*, hingga pengujian *Quality Of Service (QoS)*.

4.2.1 Implementasi Topologi Jaringan

Topologi jaringan yang digunakan dalam penelitian ini dirancang menggunakan arsitektur jaringan sederhana berbasis *Mikrotik* sebagai pusat pengelolaan trafik jaringan. Topologi penelitian terdiri dari koneksi *internet* dari ISP yang terhubung ke *Router Mikrotik*, kemudian diteruskan ke perangkat *switch* atau hub yang digunakan untuk menghubungkan client dan *access point*. Adapun struktur topologi jaringan penelitian dapat digambarkan sebagai berikut:



Gambar 4.2.1 Topologi Jaringan

Topologi jaringan pada penelitian ini menggunakan *Router Mikrotik* sebagai pusat pengelolaan jaringan yang terhubung langsung dengan ISP sebagai sumber koneksi *internet* utama. Koneksi *internet* dari ISP masuk ke *Mikrotik* melalui *Port* 1 yang berfungsi sebagai jalur WAN (Wide Area Network). Selanjutnya, *Mikrotik* mendistribusikan jaringan ke dua jalur utama, yaitu jaringan kantor dan jaringan laboratorium serta lingkungan sekolah.

Pada jalur pertama, *Port* 2 *Mikrotik* terhubung ke Hub Kantor melalui *Port* 1 hub. Hub kantor digunakan untuk mendistribusikan jaringan ke lima komputer kantor yang digunakan oleh guru dan tata usaha melalui *Port* 2 hub. Selain itu, *Port* 3 hub kantor terhubung ke sebuah *access point* yang

digunakan khusus untuk guru dan tata usaha sehingga akses jaringan pada bagian ini bersifat terbatas dan tidak dapat digunakan oleh siswa.

Pada jalur kedua, *Port* 3 *Mikrotik* terhubung ke *switch* utama melalui *Port* 1 *switch*. *Switch* ini berfungsi sebagai pusat distribusi jaringan untuk area laboratorium dan lingkungan sekolah. *Port* 2 *switch* terhubung ke *Hub Lab Multimedia*, *Port* 3 *switch* terhubung ke *Hub Lab KKPI*, dan *Port* 4 *switch* terhubung ke *Hub Lab Jaringan*. Masing-masing hub laboratorium mendistribusikan koneksi jaringan ke 25 komputer client yang digunakan dalam kegiatan praktikum siswa.

Selain itu, *Port* 5 *switch* terhubung ke *access point* lingkungan sekolah yang digunakan untuk menyediakan akses jaringan nirkabel bagi siswa dan pengguna lain di area SMK. *Access point* ini dapat diakses secara umum oleh siswa/siswi untuk mendukung kegiatan pembelajaran berbasis *internet*.

Dengan struktur topologi tersebut, jaringan dapat dipisahkan berdasarkan kebutuhan pengguna sehingga memudahkan pengelolaan *bandwidth*, penerapan *Packet Filtering*, serta implementasi *QoS* menggunakan *Mikrotik*. Topologi ini juga mendukung proses penelitian dalam menganalisis pengaruh *Packet Filtering* terhadap kualitas layanan jaringan (*Quality Of Service*/*QoS*) pada lingkungan SMKS Al-Islam Joresan Mlarak Ponorogo.

4.2.2 Koneksi ISP Ke *Ether1 Mikrotik*

Pada tahap implementasi topologi jaringan, koneksi *internet* dari *Internet Service Provider (ISP)* dihubungkan langsung ke *Port Ether1* pada *Router Mikrotik*. *Port Ether1* berfungsi sebagai jalur utama atau *gateway* yang menerima akses *internet* dari pihak penyedia layanan. Penggunaan *Ether1* sebagai interface WAN (Wide Area Network) bertujuan untuk memisahkan jalur *internet* eksternal dengan jaringan lokal internal sehingga pengelolaan trafik jaringan dapat dilakukan secara lebih terstruktur dan aman.

Konfigurasi pada *Ether1* dilakukan dengan menyesuaikan jenis koneksi yang diberikan oleh ISP, seperti *DHCP* Client ataupun *Konfigurasi* IP statis. Setelah koneksi berhasil diterapkan, *Router Mikrotik* akan memperoleh akses

internet yang kemudian dapat didistribusikan ke seluruh perangkat dalam jaringan lokal. Selain itu, pada interface ini juga diterapkan pengaturan dasar seperti DNS, *gateway*, dan *Network Address Translation* (*NAT*) agar seluruh perangkat di jaringan lokal dapat mengakses *internet* melalui satu jalur koneksi yang sama.

Implementasi koneksi ISP pada *Ether1* memiliki peranan penting dalam penelitian ini karena seluruh proses pengujian *Quality Of Service (QoS)*, *Packet Filtering*, packet *marking*, serta manajemen *bandwidth* dilakukan melalui jalur *internet* tersebut. Dengan demikian, kestabilan koneksi pada *Ether1* sangat mempengaruhi hasil pengukuran parameter *QoS* seperti *Throughput*, *Delay*, *Jitter*, dan *Packet Loss*.

4.2.3 Implementasi Hub Kantor Pada *Ether2 Mikrotik*

Port Ether2 pada *Router Mikrotik* dihubungkan ke hub kantor yang berfungsi sebagai media distribusi koneksi jaringan ke beberapa komputer administrasi kantor. Hub digunakan untuk membagi koneksi jaringan dari *Mikrotik* menuju beberapa perangkat secara bersamaan sehingga seluruh komputer kantor dapat saling terhubung dalam satu jaringan lokal.

Implementasi hub kantor dilakukan dengan menghubungkan kabel jaringan dari *Ether2 Mikrotik* menuju *Port* utama hub. Selanjutnya, beberapa komputer kantor dihubungkan ke *Port-Port* yang tersedia pada hub menggunakan kabel UTP. Dengan *Konfigurasi* tersebut, seluruh perangkat kantor dapat memperoleh akses *internet* serta komunikasi data antar perangkat dalam jaringan lokal.

Penggunaan hub kantor pada penelitian ini bertujuan untuk mensimulasikan kondisi jaringan nyata di lingkungan sekolah, khususnya pada bagian tata usaha dan administrasi. Aktivitas jaringan yang berasal dari komputer kantor akan menghasilkan trafik data yang digunakan sebagai objek pengamatan dalam analisis *QoS*. Selain itu, implementasi ini juga memungkinkan penerapan *Packet Filtering* untuk membatasi akses terhadap situs tertentu maupun mengatur prioritas trafik berdasarkan jenis layanan yang digunakan.

4.2.4 Implementasi LAB SMK Pada *Ether3 Mikrotik*

Port Ether3 pada *Router Mikrotik* digunakan sebagai jalur utama jaringan *Local Area Network (LAN)* yang menuju ke LAB SMK. Interface ini berfungsi untuk mendistribusikan koneksi *internet* dari *Router* menuju jaringan internal sekolah. Pada implementasinya, *Ether3* di*Konfigurasi* menggunakan alamat IP lokal yang nantinya menjadi *gateway* bagi seluruh perangkat yang terhubung dalam jaringan LAN.

Konfigurasi DHCP Server juga diterapkan pada *Ether3* agar perangkat yang terhubung dapat memperoleh alamat IP secara otomatis. Hal ini mempermudah proses manajemen jaringan karena administrator tidak perlu melakukan pengaturan IP secara manual pada setiap perangkat. Selain itu, implementasi *Ether3* sebagai interface LAN memungkinkan administrator jaringan untuk melakukan pengaturan manajemen *bandwidth*, *Queue Tree*, *Packet Filtering*, dan pengelompokan trafik sesuai kebutuhan penelitian.

Dalam penelitian ini, *Ether3* berfungsi sebagai pusat distribusi trafik menuju perangkat pengguna. Seluruh aktivitas pengguna seperti akses *browsing*, video *conference*, *e-learning*, *streaming*, maupun penggunaan aplikasi pembelajaran daring akan melewati interface ini. Oleh karena itu, *Ether3* menjadi salah satu bagian penting dalam proses analisis pengaruh *Packet Filtering* terhadap performa *Quality Of Service (QoS)* jaringan *Mikrotik*.

4.2.5 Implementasi *Access point* Kantor

Implementasi *Access point* kantor dilakukan untuk menyediakan layanan jaringan nirkabel (wireless) bagi guru, staf tata usaha, dan perangkat pendukung lainnya di lingkungan sekolah. *Access point* berfungsi sebagai media penghubung antara jaringan kabel yang berasal dari *Mikrotik* dengan perangkat pengguna berbasis wireless seperti laptop dan smartphone. Dengan adanya *Access point*, pengguna dapat mengakses jaringan dan *internet* secara lebih fleksibel tanpa harus menggunakan koneksi kabel secara langsung.

Pada tahap implementasi, *Access point* dihubungkan ke hub kantor menggunakan kabel UTP melalui *Port* LAN yang tersedia. Setelah perangkat terhubung, dilakukan *Konfigurasi* dasar berupa pengaturan SSID (Service Set Identifier), alamat IP, keamanan jaringan, serta metode autentikasi pengguna. Penggunaan sistem keamanan seperti password WPA/WPA2 bertujuan untuk menjaga jaringan agar tidak dapat diakses oleh pengguna yang tidak memiliki izin.

Selain sebagai media distribusi jaringan wireless, *Access point* juga menjadi bagian penting dalam proses penelitian *Quality Of Service (QoS)*. Hal ini dikarenakan sebagian besar pengguna jaringan sekolah menggunakan koneksi wireless yang cenderung menghasilkan trafik lebih dinamis dan tidak stabil dibandingkan jaringan kabel. Oleh karena itu, implementasi *Access point* digunakan untuk mengamati performa jaringan ketika terjadi akses *internet* secara bersamaan dari banyak pengguna.

Dalam penelitian ini, jaringan wireless yang disediakan melalui *Access point* difokuskan untuk mendukung kegiatan administrasi dan pembelajaran. Dengan adanya pengaturan *Packet Filtering* dan manajemen *bandwidth* pada *Mikrotik*, akses *internet* pengguna wireless dapat dikontrol sehingga penggunaan jaringan menjadi lebih optimal, aman, dan merata.

4.2.6 Implementasi Jaringan Laboratorium dan Lingkungan Sekolah

Implementasi jaringan laboratorium dan lingkungan sekolah dilakukan untuk memperluas distribusi akses *internet* ke seluruh area yang mendukung kegiatan pembelajaran dan administrasi sekolah. Jaringan laboratorium digunakan sebagai sarana pendukung kegiatan praktik komputer, sedangkan jaringan lingkungan sekolah digunakan untuk mendukung aktivitas guru dan staf dalam mengakses informasi serta layanan berbasis *internet*.

Pada tahap implementasi, koneksi jaringan dari *Mikrotik* didistribusikan melalui *switch* atau hub menuju perangkat-perangkat komputer di laboratorium. Setiap komputer dihubungkan menggunakan kabel jaringan UTP sehingga membentuk jaringan *Local Area Network (LAN)*. Selain itu, beberapa titik jaringan wireless juga disediakan melalui *Access point* agar

pengguna di lingkungan sekolah dapat terhubung menggunakan perangkat mobile.

Konfigurasi jaringan dilakukan dengan memberikan alamat IP secara otomatis menggunakan *DHCP* Server yang telah di*Konfigurasi* pada *Router Mikrotik*. Dengan sistem tersebut, setiap perangkat yang terhubung dapat memperoleh alamat IP secara otomatis tanpa perlu *Konfigurasi* manual. Implementasi ini bertujuan untuk mempermudah pengelolaan jaringan sekaligus meningkatkan efisiensi administrasi jaringan sekolah.

Dalam penelitian ini, jaringan laboratorium dan lingkungan sekolah menjadi objek utama dalam pengujian *Quality Of Service (QoS)*. Aktivitas pengguna seperti *browsing*, *streaming*, video *conference*, *e-learning*, dan akses aplikasi pembelajaran daring akan menghasilkan trafik jaringan yang digunakan untuk mengukur parameter *Throughput, Delay*, *Jitter*, dan *Packet Loss*. Dengan demikian, implementasi jaringan ini sangat mendukung proses analisis pengaruh *Packet Filtering* terhadap kualitas layanan jaringan.

4.2.7 Implementasi Pengelolaan Trafik Jaringan

Implementasi pengelolaan trafik jaringan dilakukan untuk mengatur aliran data pada jaringan agar penggunaan *bandwidth* menjadi lebih optimal dan stabil. Pengelolaan trafik dilakukan menggunakan fitur-fitur yang tersedia pada *Router Mikrotik* seperti *Packet Filtering*, packet *marking*, *Queue Tree*, dan manajemen *bandwidth*. Tujuan utama dari implementasi ini adalah untuk meningkatkan *Quality Of Service (QoS)* serta memberikan prioritas terhadap trafik tertentu yang dianggap lebih penting.

Pada tahap implementasi, dilakukan pengelompokan trafik berdasarkan jenis layanan dan kebutuhan pengguna. Trafik seperti video *conference*, akses pembelajaran daring, dan layanan administrasi diberikan prioritas *bandwidth* yang lebih tinggi dibandingkan trafik umum seperti *streaming* hiburan atau download file berukuran besar. Pengelompokan tersebut dilakukan menggunakan mekanisme packet *marking* yang kemudian diterapkan pada *Queue Tree* untuk pengaturan *bandwidth*.

Selain itu, implementasi *Packet Filtering* juga dilakukan untuk membatasi akses terhadap situs atau layanan tertentu yang dianggap tidak mendukung aktivitas pembelajaran dan pekerjaan. Dengan adanya *Packet Filtering*, administrator jaringan dapat mengontrol penggunaan *internet* sehingga jaringan menjadi lebih aman dan penggunaan *bandwidth* dapat lebih efisien.

Pengelolaan trafik jaringan dalam penelitian ini berperan penting dalam proses analisis *QoS* karena seluruh parameter pengukuran dipengaruhi oleh kondisi lalu lintas data pada jaringan. Implementasi ini memungkinkan peneliti untuk membandingkan performa jaringan sebelum dan sesudah penerapan *Packet Filtering* serta menentukan *Konfigurasi* yang paling optimal berdasarkan nilai *Throughput, Delay, Jitter*, dan *Packet Loss*.

4.3 Skenario 1 *Baseline*

4.3.1 Deskripsi Skenario *Baseline*

Skenario *Baseline* merupakan tahap awal pengujian jaringan yang dilakukan sebelum penerapan mekanisme manajemen *bandwidth* dan pengendalian trafik pada *Router Mikrotik*. Pada tahap ini jaringan dijalankan dalam kondisi standar tanpa *Konfigurasi mangle*, queue, maupun *firewall* filtering. Tujuan utama dari skenario *Baseline* adalah untuk mengetahui kondisi awal performa jaringan sehingga dapat dijadikan sebagai data pembanding terhadap hasil pengujian setelah penerapan *Quality Of Service (QoS)*.

Dalam skenario ini seluruh pengguna jaringan memperoleh akses *internet* tanpa pembagian *bandwidth* dan tanpa prioritas trafik tertentu. Semua paket data diproses secara default oleh *Router* sehingga trafik seperti *streaming*, download, *browsing*, dan video *conference* berjalan secara bersamaan tanpa pengaturan khusus. Kondisi tersebut menyebabkan penggunaan *bandwidth* menjadi tidak terkontrol ketika banyak pengguna mengakses *internet* secara bersamaan.

Pengujian *Baseline* dilakukan pada jaringan kantor, laboratorium, dan jaringan wireless sekolah untuk mengetahui performa jaringan pada kondisi

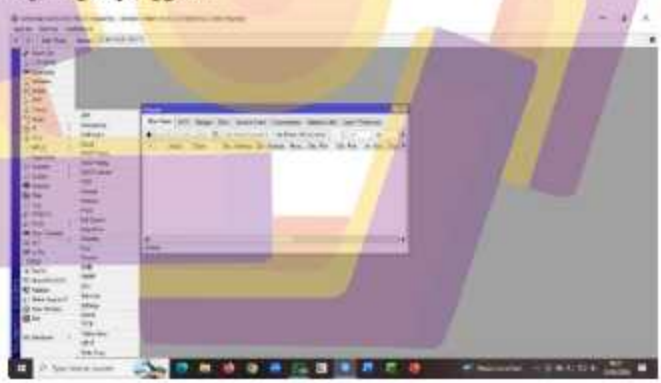
normal. Parameter yang diuji meliputi speedtest, ping, *Throughput, Delay*, dan *Jitter*. Hasil pengujian *Baseline* nantinya digunakan sebagai acuan dalam menganalisis pengaruh penerapan *Packet Filtering*, packet *marking*, dan *Queue Tree* terhadap peningkatan kualitas layanan jaringan.

4.3.2 Langkah-Langkah Pengujian *Baseline*

4.3.2.1 Menonaktifkan *Konfigurasi QoS* dan Filtering

Tahap pertama dilakukan dengan memastikan *Router Mikrotik* tidak menggunakan *Konfigurasi* pengelolaan trafik jaringan. Administrator membuka aplikasi *Winbox* kemudian login ke *Router Mikrotik*. Setelah masuk ke sistem, dilakukan pengecekan pada menu IP → *Firewall* → *Mangle* untuk memastikan tidak terdapat rule packet *marking* yang aktif.

Selanjutnya dilakukan pengecekan pada menu *Queues* untuk memastikan tidak terdapat *Konfigurasi Queue Tree* maupun Simple Queue yang berjalan. Setelah itu administrator memeriksa menu IP → *Firewall* → *Filter Rules* dan memastikan tidak terdapat rule filtering yang membatasi trafik jaringan pengguna.



Gambar 4.3.2.1 *Firewall* (*Filter Rules*)

Tahap ini bertujuan agar jaringan berjalan secara default tanpa adanya pengaturan prioritas trafik maupun pembatasan *bandwidth* sehingga hasil pengujian benar-benar menunjukkan kondisi asli jaringan.

4.3.2.2 Pengujian *Speedtest*

Setelah seluruh *Konfigurasi QoS* dinonaktifkan, dilakukan pengujian speedtest untuk mengetahui kecepatan download dan upload jaringan. Pengujian dilakukan menggunakan perangkat komputer yang terhubung ke jaringan kantor maupun laboratorium.

Pengguna membuka browser kemudian menjalankan layanan speedtest untuk mengukur kapasitas *bandwidth* yang diterima oleh jaringan. Pengujian dilakukan beberapa kali pada jam penggunaan normal dan jam sibuk untuk memperoleh data yang lebih akurat.

Gambar 4.3.2.2 Hasil Pengujian Saat Jam Normal

Gambar 4.3.2.2 Hasil Pengujian Saat Jam Sibuk

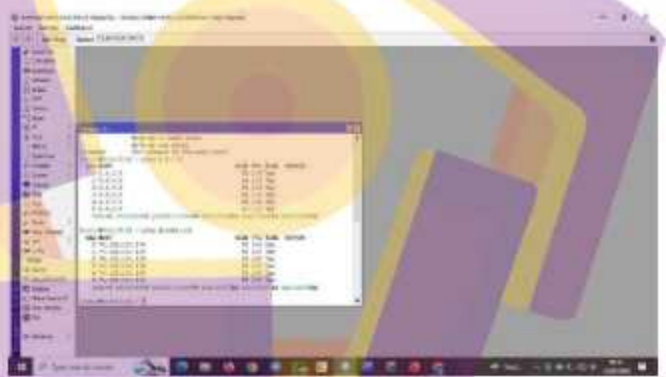
Hasil pengujian menunjukkan bahwa kecepatan *internet* yang diterima setiap pengguna tidak stabil. Ketika terdapat pengguna lain

melakukan download atau *streaming* dalam jumlah besar, *bandwidth* yang diterima pengguna lain menjadi menurun secara signifikan. Kondisi ini menunjukkan bahwa tanpa manajemen *bandwidth*, distribusi *bandwidth* pada jaringan belum merata.

4.3.2.3 Pengujian Ping

Tahap berikutnya adalah pengujian ping untuk mengetahui kestabilan koneksi jaringan dan waktu respon terhadap server *internet*. Pengujian dilakukan menggunakan fitur Ping pada *Mikrotik* maupun Command Prompt pada komputer pengguna.

Administrator melakukan ping ke alamat IP publik seperti 8.8.8.8 dan domain google.com secara terus menerus. Pengujian dilakukan pada kondisi jaringan normal dan ketika banyak pengguna mengakses *internet* secara bersamaan.



Gambar 4.3.2.3 Hasil Pengujian Ping New Terminal *Mikrotik*

Gambar 4.3.2.3 Hasil Pengujian Ping CMD

Hasil pengujian menunjukkan bahwa nilai *Delay* atau waktu respon jaringan cenderung tinggi ketika trafik jaringan meningkat. Selain itu, waktu respon antar paket tidak konsisten sehingga menghasilkan *Jitter* yang tidak stabil. Kondisi tersebut mengakibatkan kualitas koneksi menjadi kurang optimal terutama untuk layanan *real-time* seperti video *conference* dan pembelajaran daring.

4.3.2.4 Pengujian *Throughput*

Pengujian *Throughput* dilakukan untuk mengetahui kemampuan jaringan dalam mengirimkan data secara efektif dalam periode waktu tertentu. Pengukuran *Throughput* dilakukan menggunakan aplikasi monitoring jaringan atau fitur Torch pada *Mikrotik* untuk melihat penggunaan *bandwidth* secara *real-time*.

Pada tahap ini beberapa pengguna melakukan aktivitas jaringan secara bersamaan seperti download file, *streaming* video, *browsing*, dan akses aplikasi pembelajaran daring. Aktivitas tersebut bertujuan untuk menghasilkan kondisi trafik jaringan yang padat sehingga performa jaringan dapat diamati secara langsung.

Gambar 4.3.2.4 Hasil Pengujian *Throughput*

Hasil pengujian menunjukkan bahwa *Throughput* jaringan mengalami fluktuasi yang cukup tinggi. Pengguna yang melakukan aktivitas download berukuran besar cenderung menguasai *bandwidth* sehingga pengguna lain mengalami penurunan kualitas koneksi *internet*. Hal ini menunjukkan bahwa tanpa pengelolaan trafik, penggunaan *bandwidth* pada jaringan belum efisien.

4.3.3 Hasil Pengujian *Baseline*

Berdasarkan hasil pengujian *Baseline*, diperoleh kondisi awal jaringan yang menunjukkan bahwa performa jaringan masih belum optimal. Tidak adanya *Konfigurasi mangle*, queue, dan *firewall* filtering menyebabkan seluruh trafik diproses tanpa prioritas sehingga penggunaan *bandwidth* menjadi tidak terkontrol.

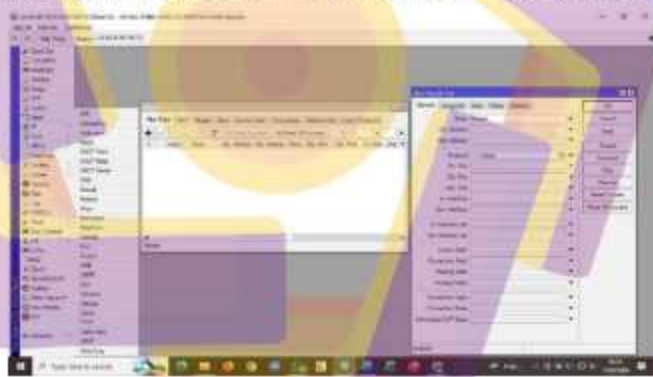
Nilai *Delay* pada jaringan cenderung tinggi ketika terjadi peningkatan trafik pengguna. Tingginya *Delay* menyebabkan waktu respon jaringan menjadi lambat terutama saat mengakses layanan berbasis *real-time* seperti video *conference* dan aplikasi pembelajaran *online*. Selain itu, nilai *Jitter* juga menunjukkan kondisi yang tidak stabil karena perbedaan waktu pengiriman paket data antar pengguna cukup besar.

Distribusi *bandwidth* pada jaringan juga belum merata. Pengguna yang melakukan download atau *streaming* dalam kapasitas besar dapat menghabiskan sebagian besar *bandwidth internet* sehingga pengguna lain

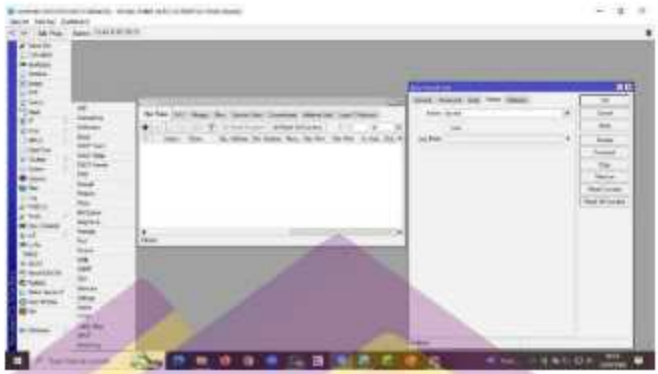
mengalami penurunan kecepatan akses. Kondisi tersebut membuktikan bahwa jaringan memerlukan mekanisme pengelolaan trafik seperti packet *marking*, *Queue Tree*, dan *Packet Filtering* agar kualitas layanan jaringan dapat menjadi lebih stabil, optimal, dan merata bagi seluruh pengguna.

4.4 Skenario 2 *Packet Filtering*

Skenario kedua pada penelitian ini adalah penerapan *Packet Filtering* menggunakan fitur *firewall* filter pada *Router Mikrotik*. *Packet Filtering* merupakan metode pengendalian lalu lintas jaringan dengan cara menyaring paket data berdasarkan aturan tertentu seperti *Protocol*, *Port*, dan alamat IP. Tujuan utama dari implementasi *Packet Filtering* adalah untuk meningkatkan keamanan jaringan, mengontrol penggunaan *bandwidth*, serta menjaga kestabilan trafik jaringan agar kualitas layanan jaringan atau *Quality Of Service (QoS)* menjadi lebih baik. Langkah-langkah *Konfigurasi* filtering berdasarkan *Protocol* ip-*firewall*-filter-add chain=forward *Protocol*=*TCP* action=accept.



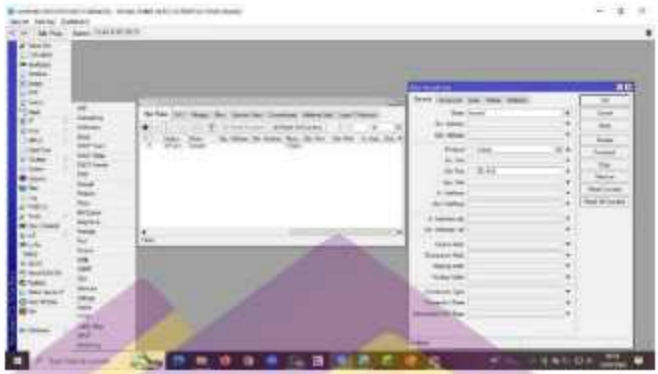
Gambar 4.4 Filtering Berdasarkan Protokol



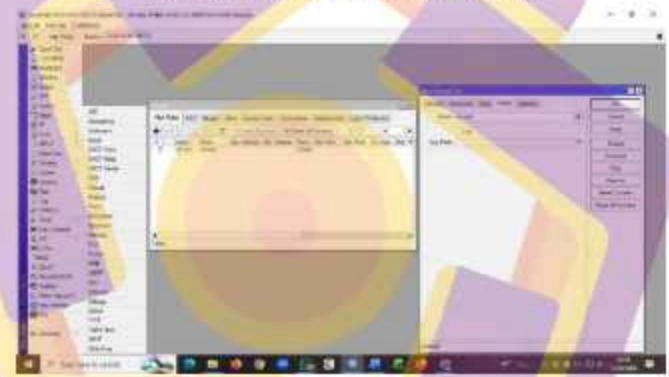
Gambar 4.4 Filtering Berdasarkan Protokol

Konfigurasi filtering berdasarkan *Port* pada *Router Mikrotik* berfungsi untuk mengatur lalu lintas jaringan berdasarkan layanan atau aplikasi tertentu yang menggunakan nomor *Port* tertentu. Setiap layanan *internet* memiliki *Port* komunikasi masing-masing, seperti *Port* 80 untuk *HTTP* dan *Port* 443 untuk *HTTPS*. Dengan filtering berdasarkan *Port*, administrator jaringan dapat menentukan trafik mana yang diizinkan, dibatasi, atau diprioritaskan dalam jaringan.

Fungsi utama filtering berdasarkan *Port* adalah untuk meningkatkan keamanan jaringan, mengontrol penggunaan *bandwidth*, serta memprioritaskan layanan penting. Sebagai contoh, administrator dapat mengizinkan akses website pembelajaran melalui *Port* 80 dan 443, sementara layanan lain yang tidak diperlukan dapat dibatasi. Selain itu, filtering berdasarkan *Port* juga membantu menjaga kestabilan jaringan karena *Router* hanya memproses trafik yang sesuai dengan aturan *firewall* yang telah ditentukan. Langkah Selanjutnya Adalah filtering berdasarkan *Port*, pilih ip-*firewall* filter add chain=forward *Protocol=TCP* dst-*Port*=80,443 action=accept.



Gambar 4.4 Filtering Berdasarkan *Port*



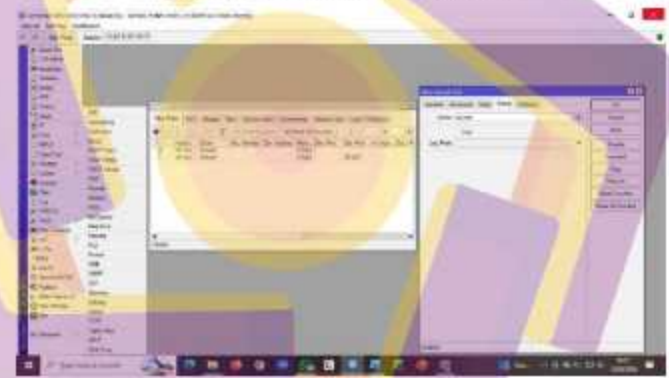
Gambar 4.4 Filtering Berdasarkan *Port*

Langkah selanjutnya adalah *Konfigurasi* filtering berdasarkan *IP Address* berfungsi untuk mengatur hak akses jaringan berdasarkan alamat IP atau segmen jaringan tertentu. Dengan metode ini, administrator dapat menentukan perangkat atau kelompok pengguna mana yang diperbolehkan maupun dibatasi dalam mengakses jaringan dan *internet*.

Pada penelitian ini, filtering berdasarkan IP diterapkan pada subnet jaringan LAB SMK 192.168.20.0/24. Fungsi utamanya adalah untuk memberikan kontrol akses yang lebih terstruktur terhadap pengguna jaringan LAB SMK dibandingkan jaringan lainnya. Selain meningkatkan keamanan jaringan, filtering berdasarkan IP juga membantu pengelolaan *bandwidth* agar penggunaan *internet* menjadi lebih merata dan sesuai kebutuhan masing-

masing pengguna. Langkah-langkahnya adalah sebagai berikut pilih ip-*firewall* filter add chain=forward src-address=192.168.10.0/24 action=accept.

Gambar 4.4 Filtering Berdasarkan IP



Gambar 4.4 Filtering Berdasarkan IP

Selain itu, filtering *IP Address* mempermudah administrator dalam melakukan monitoring trafik jaringan karena setiap segmen jaringan dapat diatur dan diawasi secara terpisah. Dengan demikian, kualitas layanan jaringan atau *Quality Of Service (QoS)* dapat menjadi lebih stabil dan optimal.

Pada skenario ini, *Router Mikrotik* mulai melakukan proses seleksi terhadap paket data yang melewati jaringan. Paket yang sesuai dengan aturan *firewall* akan diteruskan, sedangkan paket yang tidak sesuai dapat dibatasi atau ditolak. Implementasi *Packet Filtering* dilakukan secara bertahap berdasarkan *Protocol*, *Port* layanan, dan alamat IP pengguna jaringan.

Pengujian dilakukan untuk mengetahui pengaruh *Packet Filtering* terhadap performa jaringan, khususnya pada parameter stabilitas trafik, penggunaan *bandwidth*, dan *Delay* jaringan. Hasil pengujian pada skenario ini kemudian dibandingkan dengan hasil pengujian *Baseline* untuk mengetahui peningkatan kualitas layanan jaringan setelah diterapkannya *Packet Filtering*.

Gambar 4.4 Hasil Pengujian Stabilitas Trafik Jaringan

Gambar 4.4 Hasil Pengujian Penggunaan *Bandwidth*

Gambar 4.4 Hasil Pengujian *Delay* Jaringan

4.5 Skenario 3 *QoS* + Filtering

4.5.1 Menambahkan *IP Address* Kedalam *Address List Router*

Penambahan *IP Address* ke dalam *Address List* pada *Router Mikrotik* merupakan salah satu metode yang digunakan untuk mempermudah pengelolaan dan pengaturan trafik jaringan. *Address List* berfungsi sebagai tempat pengelompokan alamat IP berdasarkan kategori atau kebutuhan tertentu sehingga administrator jaringan dapat menerapkan *Konfigurasi firewall*, *Packet Filtering*, manajemen *bandwidth*, maupun *Quality Of Service (QoS)* secara lebih terstruktur dan efisien.

Dengan menggunakan *Address List*, administrator tidak perlu menuliskan alamat IP secara berulang pada setiap rule *Konfigurasi*. Seluruh alamat IP dapat dikelompokkan ke dalam satu nama list tertentu, seperti layanan pembelajaran, media sosial, game *online*, atau server aplikasi lainnya. Metode ini membuat proses administrasi jaringan menjadi lebih sederhana, mudah dikelola, dan fleksibel ketika dilakukan penambahan maupun perubahan *Konfigurasi* jaringan.

4.5.1.1 Menambahkan *IP Address* Server Pembelajaran Daring

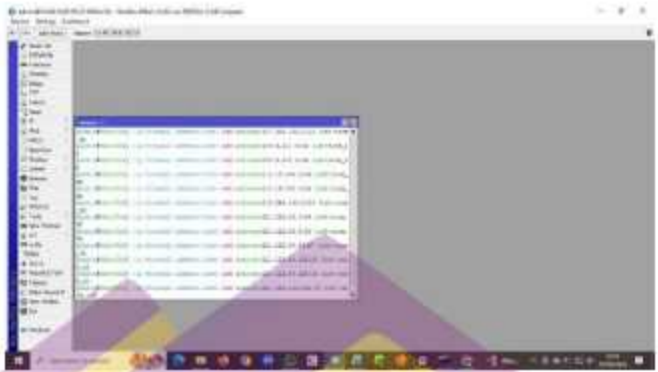
Untuk mendukung kelancaran kegiatan pembelajaran daring, administrator jaringan pada *Router Mikrotik* melakukan penambahan *IP Address* server layanan pembelajaran seperti Zoom dan *Gamelab* ke dalam fitur *Address List*. Penambahan *Address List* ini bertujuan agar trafik

aplikasi dan website pembelajaran dapat lebih mudah dikenali oleh *Router* sehingga nantinya dapat diberikan prioritas *bandwidth* yang lebih tinggi dibandingkan trafik lainnya.

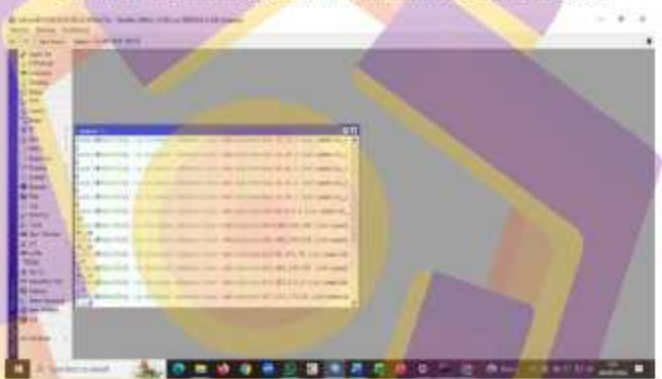
Address List pada *Mikrotik* berfungsi sebagai media pengelompokan alamat IP berdasarkan jenis layanan tertentu. Dengan adanya pengelompokan tersebut, administrator jaringan dapat membuat *Konfigurasi Quality Of Service (QoS)*, packet *marking*, *firewall* filter, dan *Queue Tree* secara lebih terstruktur tanpa harus memasukkan alamat IP server satu per satu pada setiap rule *Konfigurasi*.

Implementasi ini sangat penting dalam lingkungan sekolah karena layanan pembelajaran *online* membutuhkan koneksi yang stabil, *Delay* rendah, dan *bandwidth* yang cukup agar proses video *conference* maupun akses materi pembelajaran dapat berjalan dengan optimal. Langkah-langkahnya adalah buka new terminal-paste *IP Address* server (zoom dan *gamelab*).

Gambar 4.5.1.1 Halaman Awal New Terminal *Mikrotik*



Gambar 4.5.1.1 Menambahkan *IP Address* Server Zoom



Gambar 4.5.1.1 Menambahkan *IP Address* Server *Gamelab*

Penambahan *IP Address* server Zoom dan *Gamelab* ke dalam *Address List* bertujuan untuk memberikan prioritas khusus terhadap trafik pembelajaran *online* pada jaringan sekolah. Dengan adanya *Address List* tersebut, *Router Mikrotik* dapat mengenali trafik aplikasi pembelajaran secara lebih spesifik sehingga administrator dapat menerapkan manajemen *bandwidth* dan *Quality Of Service (QoS)* dengan lebih optimal.

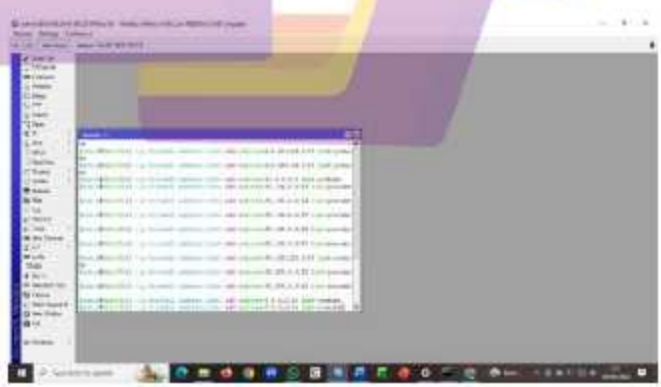
Selain itu, *Konfigurasi* ini membantu menjaga kestabilan koneksi video *conference* dan akses platform pembelajaran daring ketika jaringan digunakan secara bersamaan oleh banyak pengguna. Trafik pembelajaran dapat diprioritaskan dibandingkan trafik hiburan atau media sosial sehingga

proses belajar mengajar tetap berjalan lancar, *Delay* jaringan menjadi lebih rendah, dan penggunaan *bandwidth* menjadi lebih efisien.

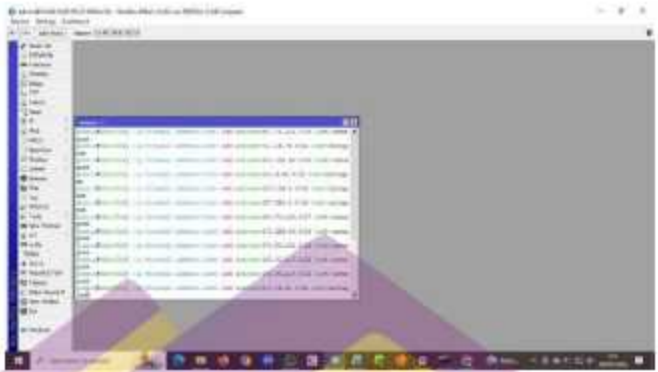
4.5.1.2 Menambahkan *IP Address* Server Media Sosial

Penambahan *IP Address* server media sosial seperti YouTube, Instagram, Facebook, dan TikTok ke dalam *Address List* pada *Router Mikrotik* dilakukan untuk mempermudah proses pengelolaan jaringan dan penerapan pembatasan akses media sosial. Dengan memasukkan *IP Address* server aplikasi dan website media sosial ke dalam *Address List*, administrator jaringan dapat membuat *Konfigurasi firewall* filter, *Packet Filtering*, serta manajemen *bandwidth* secara lebih terstruktur dan efisien.

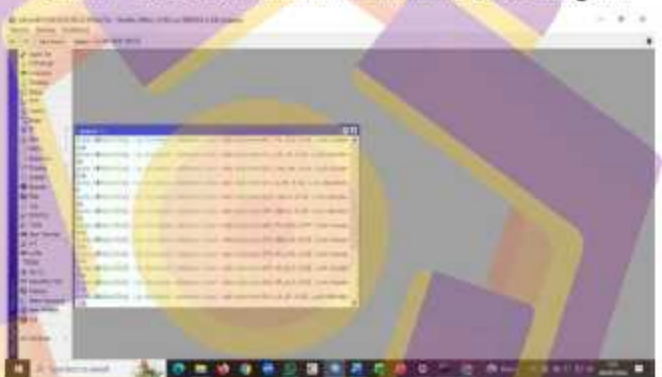
Address List pada *Mikrotik* berfungsi sebagai daftar kumpulan alamat IP yang dikelompokkan dalam satu nama tertentu sehingga dapat digunakan kembali pada berbagai *Konfigurasi* jaringan. Pada penelitian ini, penambahan *Address List* media sosial digunakan sebagai dasar untuk mempermudah penerapan pembatasan akses layanan media sosial agar penggunaan *bandwidth* jaringan sekolah dapat lebih terkontrol dan tidak mengganggu layanan utama seperti pembelajaran *online*, video *conference*, dan administrasi sekolah. Langkah-langkahnya adalah buka new terminal-paste *IP Address* server media sosial (youtube, Instagram, facebook, dan tiktok).



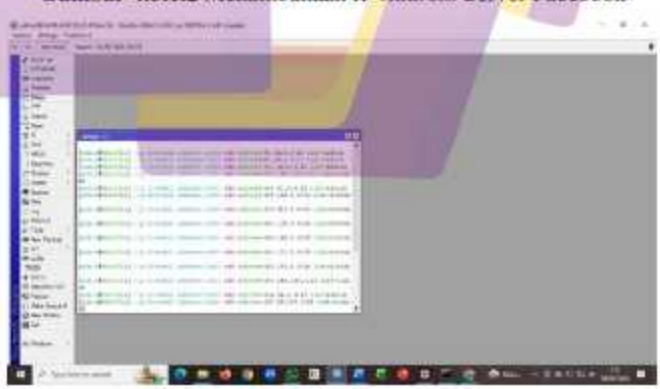
Gambar 4.5.1.2 Menambahkan *IP Address* Server Youtube



Gambar 4.5.1.2 Menambahkan *IP Address* Server Instagram



Gambar 4.5.1.2 Menambahkan *IP Address* Server Facebook



Gambar 4.5.1.2 Menambahkan *IP Address* Server Tiktok

Penambahan *IP Address* server media sosial ke dalam *Address List* bertujuan untuk mempermudah administrator jaringan dalam melakukan pembatasan akses media sosial pada jaringan sekolah. Dengan adanya *Address List*, administrator dapat membuat rule *firewall* filtering dan pengaturan *bandwidth* secara lebih cepat dan efisien tanpa perlu menuliskan alamat IP server satu per satu pada setiap *Konfigurasi*.

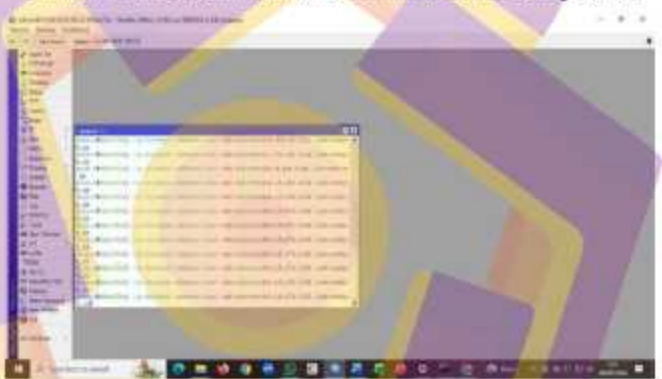
Selain itu, *Konfigurasi* ini membantu mengontrol penggunaan *bandwidth* jaringan agar tidak didominasi oleh akses media sosial dan layanan *streaming* yang berlebihan. Dengan demikian, layanan utama seperti pembelajaran daring, video *conference*, dan sistem administrasi sekolah dapat memperoleh koneksi *internet* yang lebih stabil, optimal, dan merata bagi seluruh pengguna jaringan.

4.5.1.3 Menambahkan *IP Address* Server Games *Online*

Dalam proses pengelolaan jaringan pada *Router Mikrotik*, administrator jaringan dapat menambahkan *IP Address* server game *online* seperti CrazyGames dan Roblox ke dalam fitur *Address List*. Penambahan *Address List* ini bertujuan untuk mempermudah proses identifikasi trafik game *online* sehingga nantinya administrator dapat lebih mudah menerapkan *Konfigurasi* pembatasan akses, *firewall* filtering, maupun manajemen *bandwidth* pada jaringan sekolah.

Address List merupakan fitur pada *Mikrotik* yang digunakan untuk mengelompokkan sejumlah alamat IP ke dalam satu nama tertentu. Dengan metode ini, administrator tidak perlu memasukkan alamat IP server game secara berulang pada setiap rule *Konfigurasi*. Selain membuat pengelolaan jaringan menjadi lebih rapi, penggunaan *Address List* juga meningkatkan efisiensi *Konfigurasi* ketika akan melakukan pembatasan akses terhadap layanan game *online*. Langkah-langkahnya adalah buka new terminal-paste *IP Address* server games *online* (crazygames dan roblox).

Gambar 4.5.1.3 Menambahkan *IP Address* Server CrazyGames



Gambar 4.5.1.3 Menambahkan *IP Address* Server Roblox

Penambahan *IP Address* server game *online* ke dalam *Address List* memiliki fungsi utama untuk mempermudah proses pengendalian akses jaringan pada layanan game *online*. Dengan adanya pengelompokan *IP Address* tersebut, administrator dapat membuat *Konfigurasi firewall* filtering dan pembatasan *bandwidth* secara lebih sederhana tanpa perlu memasukkan alamat IP server satu per satu.

Selain itu, *Konfigurasi* ini membantu menjaga kestabilan jaringan sekolah dengan mengurangi penggunaan *bandwidth* yang berlebihan akibat akses game *online*. Trafik game dapat dikontrol agar tidak mengganggu layanan utama seperti pembelajaran daring, video *conference*, dan sistem administrasi sekolah. Dengan demikian, kualitas layanan jaringan atau

Quality Of Service (QoS) dapat tetap terjaga dan penggunaan *internet* menjadi lebih optimal bagi seluruh pengguna jaringan.

4.5.2 *Konfigurasi Firewall Mangle*

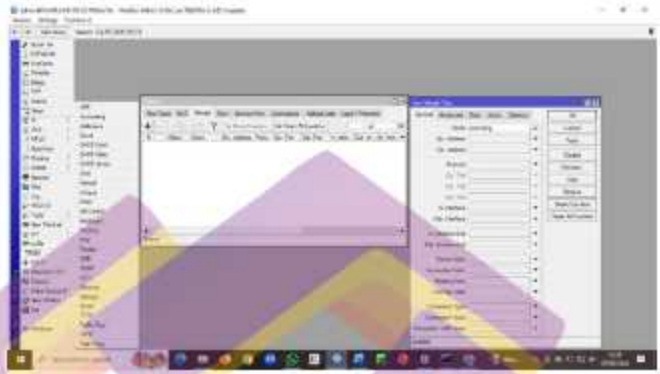
4.5.2.1 *Konfigurasi Firewall Mangle* Pembelajaran Daring

Konfigurasi firewall mangle pada *Mikrotik* digunakan untuk mengidentifikasi dan mengelompokkan trafik aplikasi pembelajaran daring, yaitu Zoom dan *Gamelab*, berdasarkan *Protocol TCP* dan *UDP*. *Konfigurasi* ini dilakukan melalui menu IP → *Firewall* → *Mangle* dengan menggunakan chain pre*routing*, karena proses pemeriksaan paket dilakukan sebelum paket diteruskan ke jaringan tujuan. Tujuan utama *Konfigurasi* ini adalah agar *Router* dapat mengenali trafik yang berasal dari aplikasi pembelajaran daring sehingga nantinya dapat diterapkan manajemen *bandwidth*, prioritas trafik, serta pengaturan *Quality Of Service (QoS)* secara lebih optimal.

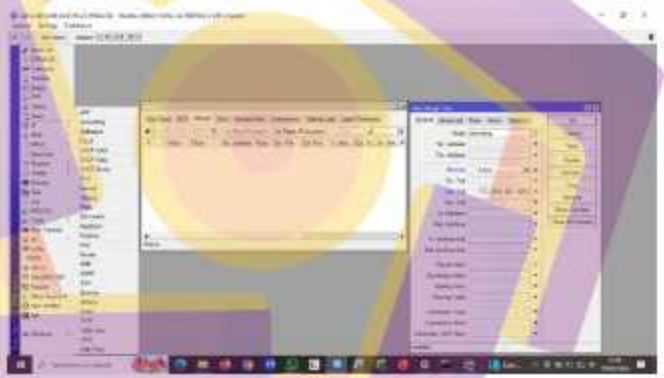
Pada proses *Konfigurasi*, administrator menentukan *Protocol* yang digunakan, yaitu *TCP* dan *UDP*, kemudian memasukkan *Destination Port* (dst-*Port*) milik aplikasi Zoom dan *Gamelab*. Untuk aplikasi Zoom digunakan *Port TCP* dan *UDP* 3478, 3479, 5090, dan 8801-8810, sedangkan aplikasi *Gamelab* menggunakan *Port TCP* 80, 443, dan 8080, serta *Port UDP* 3478-3481. Setelah *Router* mendeteksi paket yang menuju *Port-Port* tersebut, action pada *firewall mangle* diatur menjadi add-dst-to-address-list agar alamat IP tujuan secara otomatis dimasukkan ke dalam daftar alamat tertentu. Trafik Zoom disimpan pada *Address List* bernama zoom_ip, sedangkan trafik *Gamelab* disimpan pada *Address List* *gamelab*_ip.

Melalui *Konfigurasi* tersebut, *Router Mikrotik* dapat membedakan trafik pembelajaran daring dengan trafik *internet* lainnya. Dengan adanya proses penandaan dan pengelompokan IP tujuan tersebut, administrator jaringan menjadi lebih mudah dalam menerapkan pengaturan *bandwidth*, *Queue Tree*, maupun prioritas layanan untuk aplikasi pembelajaran daring. Hal ini bertujuan agar proses belajar mengajar secara *online* dapat berjalan

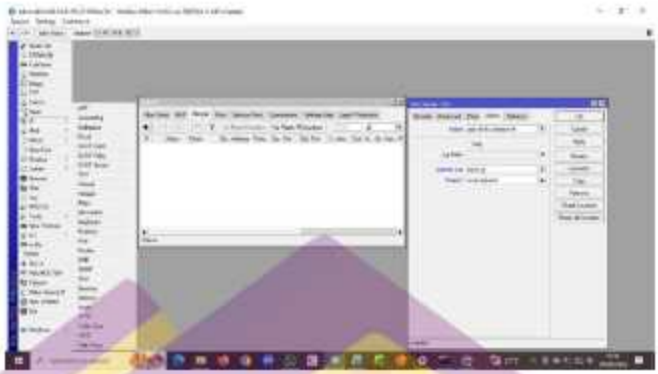
lebih stabil, lancar, dan minim gangguan meskipun jaringan digunakan secara bersamaan oleh banyak pengguna.



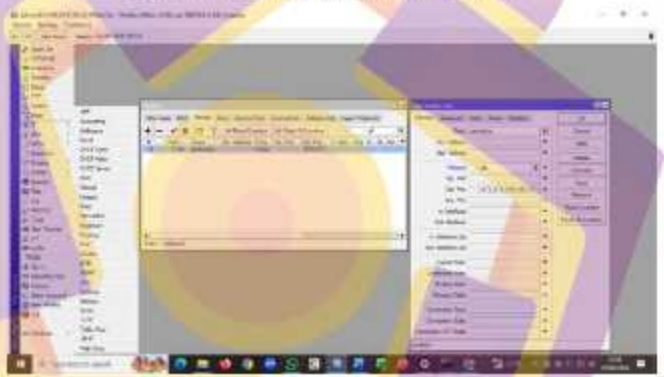
Gambar 4.5.2.1 Tampilan Utama *Firewall Mangle*



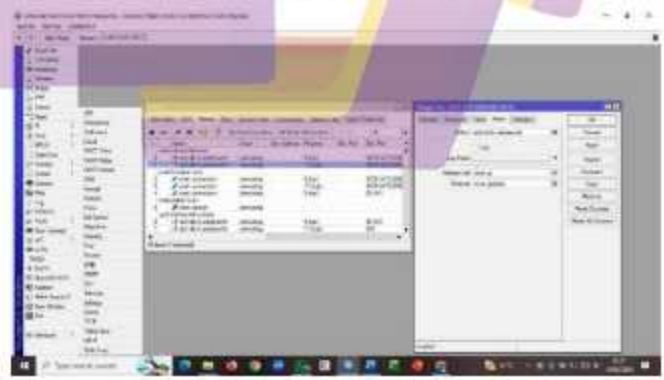
Gambar 4.5.2.1 Rule *Mangle* Zoom *TCP*



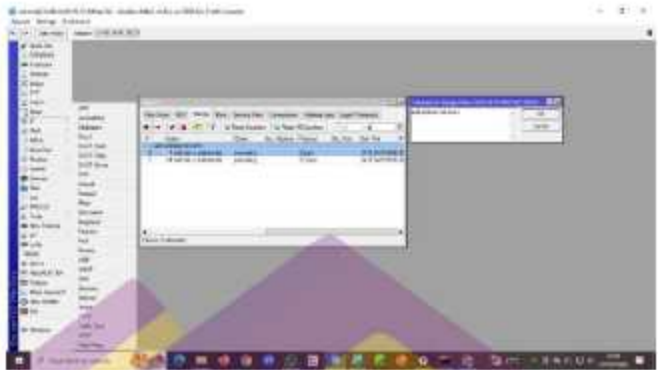
Gambar 4.5.2.1 Rule *Mangle* Zoom *TCP*



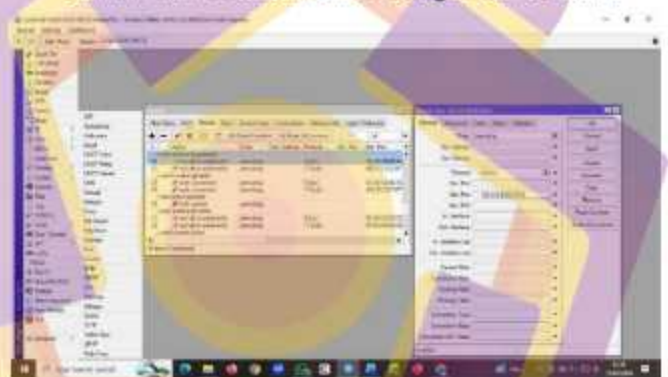
Gambar 4.5.2.1 Rule *Mangle* Zoom *UDP*



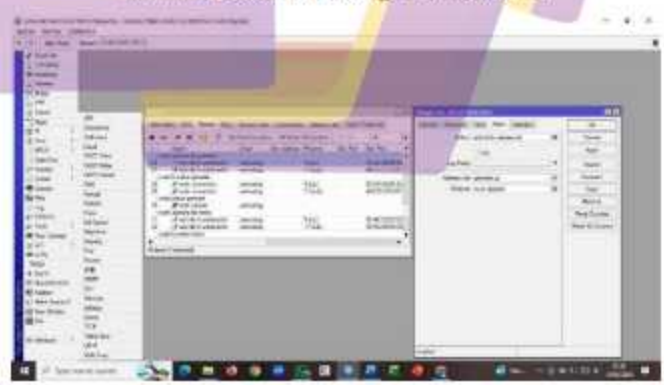
Gambar 4.5.2.1 Rule *Mangle* Zoom *UDP*



Gambar 4.5.2.1 Koment *Mangle* Sebagai Penanda Zoom



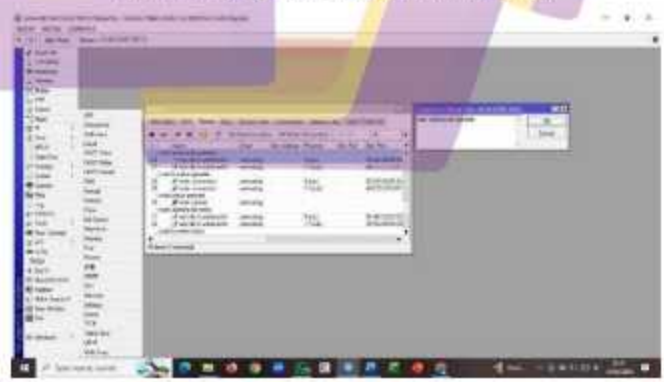
Gambar 4.5.2.1 Rule *Mangle Gamelab TCP*



Gambar 4.5.2.1 Rule *Mangle Gamelab TCP*

Gambar 4.5.2.1 Rule *Mangle Gamelab UDP*

Gambar 4.5.2.1 Rule *Mangle Gamelab UDP*



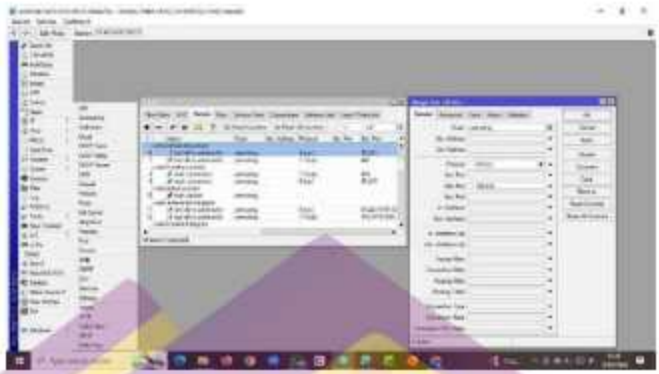
Gambar 4.5.2.1 Koment *Mangle* Sebagai Penanda *Gamelab*

4.5.2.2 *Konfigurasi Firewall Mangle* Media Sosial

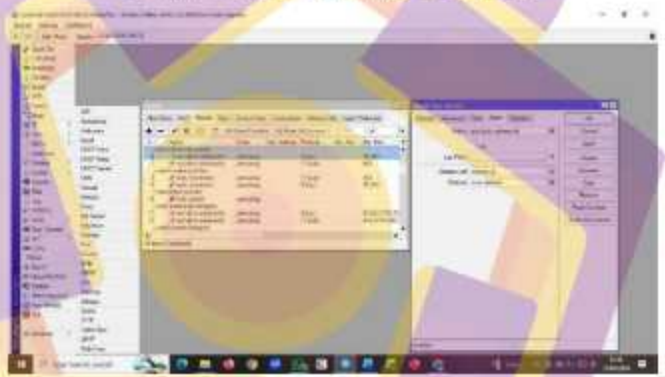
Konfigurasi firewall mangle pada *Router Mikrotik* digunakan untuk mendeteksi, menandai, dan mengelompokkan trafik aplikasi media sosial seperti YouTube, Instagram, Facebook, dan TikTok berdasarkan *Protocol TCP* dan *UDP*. Penerapan *Konfigurasi* ini bertujuan agar administrator jaringan dapat mengenali jenis trafik yang melintas pada jaringan sehingga lebih mudah dalam melakukan pengaturan *bandwidth*, monitoring penggunaan *internet*, pembatasan akses, serta penerapan *Quality Of Service (QoS)*. *Konfigurasi* dilakukan melalui menu IP → *Firewall* → *Mangle* dengan menggunakan chain pre*routing*, karena proses identifikasi paket dilakukan sebelum paket diteruskan menuju jaringan tujuan.

Pada tahap *Konfigurasi*, administrator menentukan *Protocol TCP* dan *UDP* kemudian memasukkan *Destination Port* (dst-*Port*) dari masing-masing aplikasi media sosial. Aplikasi YouTube menggunakan *Port TCP* 80 dan 443, serta *UDP* 443. Instagram menggunakan *Port TCP* 80 dan 443, serta *UDP* 443. Facebook menggunakan *Port TCP* 80 dan 443, serta *UDP* 3478-3481 dan 443. Sementara itu, TikTok menggunakan *Port TCP* 80, 443, dan 8080, serta *UDP* 443 dan 3478-3497. Setelah paket dengan *Port* tersebut terdeteksi, *firewall mangle* menjalankan action add-dst-to-address-list untuk menyimpan alamat IP tujuan ke dalam daftar alamat tertentu sesuai aplikasi yang digunakan. Trafik YouTube akan masuk ke *Address List* youtube_ip, Instagram ke instagram_ip, Facebook ke facebook_ip, dan TikTok ke tiktok_ip.

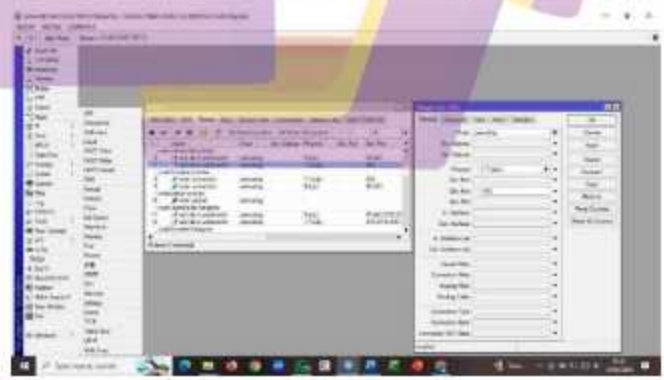
Secara singkat, *Konfigurasi* dilakukan dengan membuat rule *firewall mangle* pada chain pre*routing* menggunakan *Protocol TCP* dan *UDP* sesuai *Port* aplikasi media sosial yang telah ditentukan. Selanjutnya action diatur menjadi add-dst-to-address-list agar *Router* dapat mengelompokkan alamat IP tujuan berdasarkan jenis aplikasi. Dengan adanya proses penandaan tersebut, administrator jaringan dapat lebih mudah mengatur prioritas trafik, melakukan pembatasan *bandwidth* media sosial, serta meningkatkan stabilitas dan efisiensi penggunaan jaringan *internet* pada *Mikrotik*.



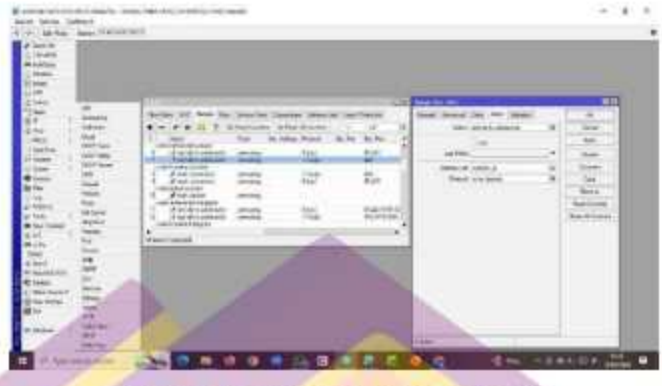
Gambar 4.5.2.2 Rule *Mangle* Youtube *TCP*



Gambar 4.5.2.2 Rule *Mangle* Youtube *TCP*

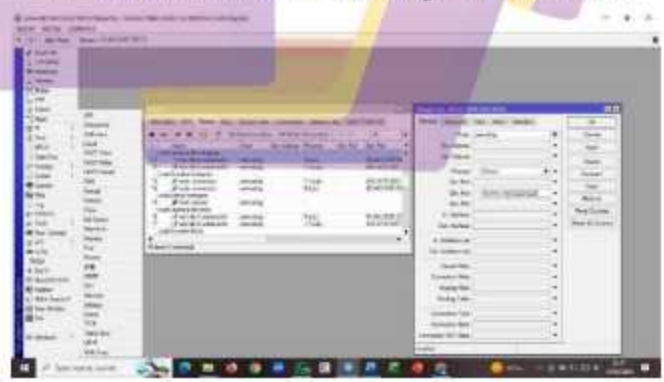


Gambar 4.5.2.2 Rule *Mangle* Youtube *UDP*

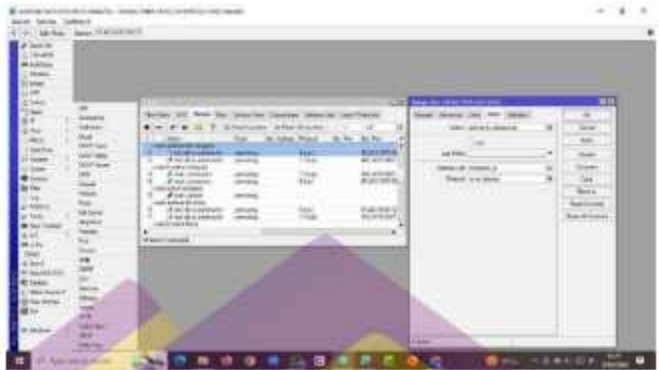


Gambar 4.5.2.2 Rule *Mangle* Youtube *UDP*

Gambar 4.5.2.2 Koment *Mangle* Sebagai Penanda Youtube

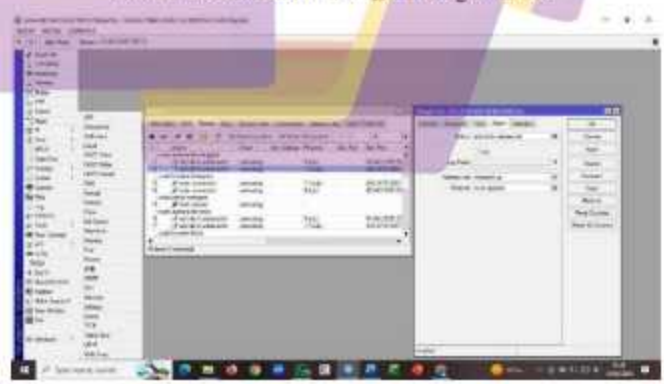


Gambar 4.5.2.2 Rule *Mangle* Instagram *TCP*

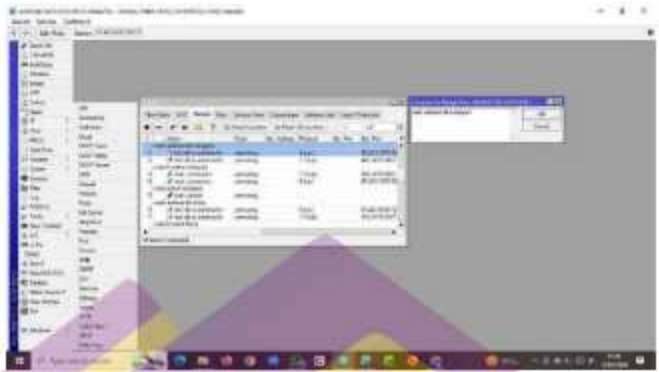


Gambar 4.5.2.2 Rule *Mangle* Instagram *TCP*

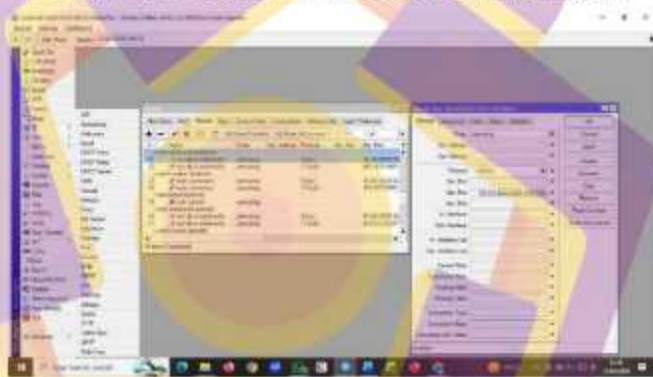
Gambar 4.5.2.2 Rule *Mangle* Instagram *UDP*



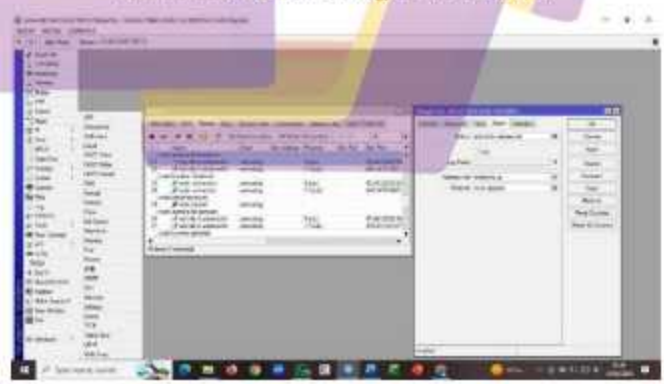
Gambar 4.5.2.2 Rule *Mangle* Instagram *UDP*



Gambar 4.5.2.2 Koment *Mangle* Sebagai Penanda Instagram



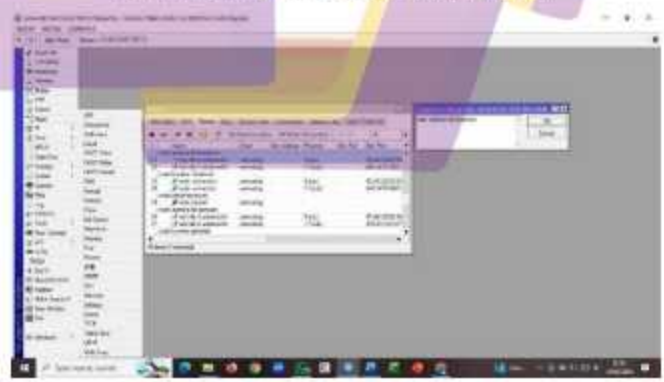
Gambar 4.5.2.2 Rule *Mangle* Facebook *TCP*



Gambar 4.5.2.2 Rule *Mangle* Facebook *TCP*

Gambar 4.5.2.2 Rule *Mangle* Facebook *UDP*

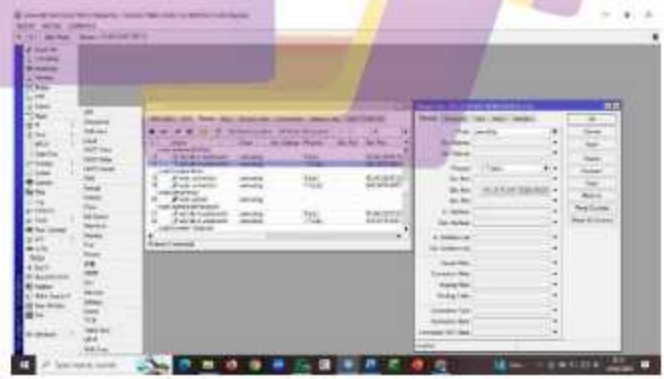
Gambar 4.5.2.2 Rule *Mangle* Facebook *UDP*



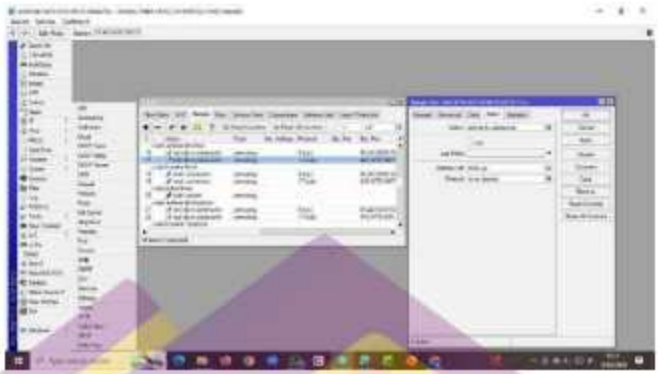
Gambar 4.5.2.2 Koment *Mangle* Sebagai Penanda Facebook

Gambar 4.5.2.2 Rule *Mangle* Tiktok *TCP*

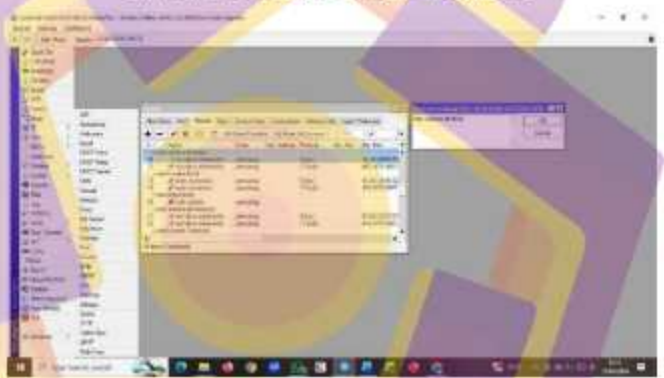
Gambar 4.5.2.2 Rule *Mangle* Tiktok *TCP*



Gambar 4.5.2.2 Rule *Mangle* Tiktok *UDP*



Gambar 4.5.2.2 Rule *Mangle* Tiktok *UDP*



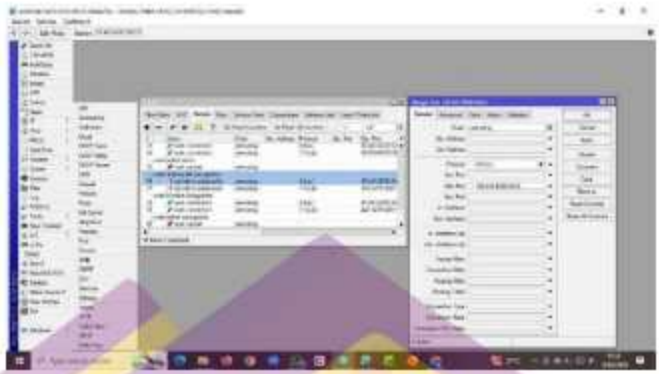
Gambar 4.5.2.2 Koment *Mangle* Sebagai Penanda Tiktok

4.5.2.3 *Konfigurasi Firewall Mangle* Games *Online*

Konfigurasi firewall mangle pada *Mikrotik* digunakan untuk mengidentifikasi dan mengelompokkan trafik game *online* seperti CrazyGames dan Roblox berdasarkan *Protocol TCP* dan *UDP*. Penerapan *Konfigurasi* ini bertujuan agar *Router* dapat mengenali trafik permainan *online* yang melewati jaringan sehingga administrator dapat melakukan pengaturan *bandwidth*, pembatasan akses, monitoring trafik, serta penerapan *Quality Of Service (QoS)* secara lebih efektif. *Konfigurasi* dilakukan melalui menu IP → *Firewall* → *Mangle* dengan menggunakan chain pre*routing*, karena proses penandaan paket dilakukan sebelum paket diteruskan ke jaringan tujuan.

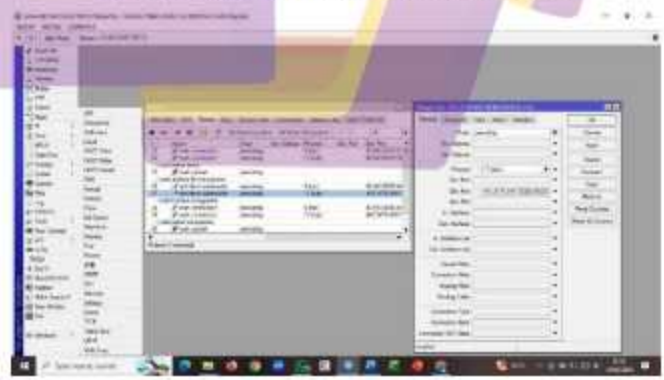
Pada tahap *Konfigurasi*, administrator menentukan *Protocol TCP* dan *UDP* kemudian memasukkan *Destination Port* (dst-*Port*) yang digunakan oleh CrazyGames dan Roblox. CrazyGames umumnya menggunakan *Port TCP* 80 dan 443, serta *UDP* 3478-3480 untuk mendukung koneksi game berbasis browser dan WebRTC. Sementara itu, Roblox menggunakan *Port TCP* 80 dan 443, serta *UDP* 49152-65535 yang digunakan untuk komunikasi *real-time* dan koneksi permainan *online*. Setelah paket dengan *Port* tersebut terdeteksi, *firewall mangle* menjalankan action add-dst-to-address-list untuk menyimpan alamat IP tujuan ke dalam daftar alamat tertentu sesuai jenis aplikasi game yang digunakan. Trafik CrazyGames akan dimasukkan ke *Address List* crazygames_ip, sedangkan trafik Roblox dimasukkan ke *Address List* roblox_ip.

Secara singkat, *Konfigurasi* dilakukan dengan membuat rule *firewall mangle* pada chain pre*routing* menggunakan *Protocol TCP* dan *UDP* sesuai *Port* aplikasi game *online* yang telah ditentukan. Selanjutnya action diatur menjadi add-dst-to-address-list agar *Router* dapat mencatat dan mengelompokkan alamat IP tujuan berdasarkan aplikasi game yang digunakan. Dengan adanya proses pengelompokan tersebut, administrator jaringan dapat lebih mudah melakukan pengaturan *bandwidth*, pembatasan akses game *online*, serta pengendalian trafik jaringan sehingga penggunaan *internet* menjadi lebih stabil, efisien, dan sesuai dengan kebutuhan jaringan sekolah maupun kantor.

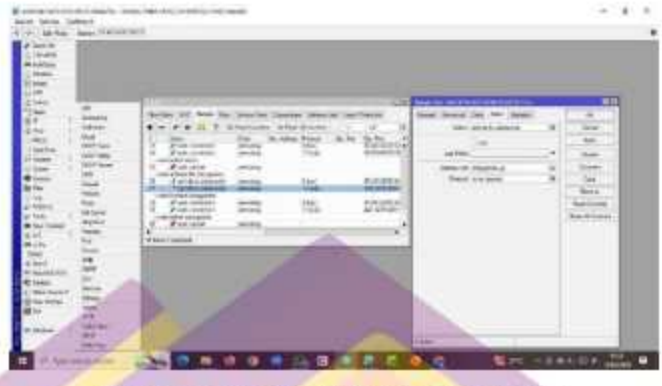


Gambar 4.5.2.3 Rule *Mangle* Crazygames *TCP*

Gambar 4.5.2.3 Rule *Mangle* Crazygames *TCP*

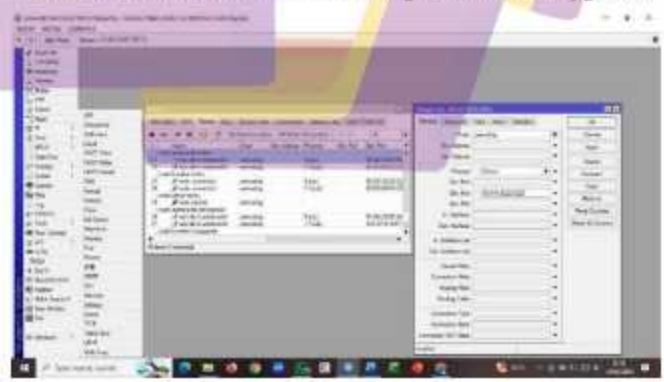


Gambar 4.5.2.3 Rule *Mangle* Crazygames *UDP*



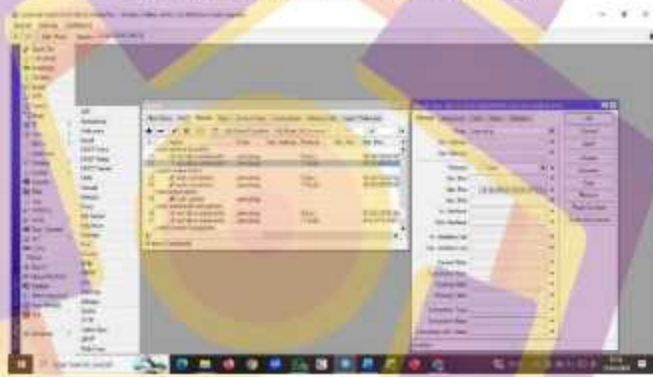
Gambar 4.5.2.3 Rule *Mangle* Crazygames *UDP*

Gambar 4.5.2.3 Koment *Mangle* Sebagai Penanda Crazygames

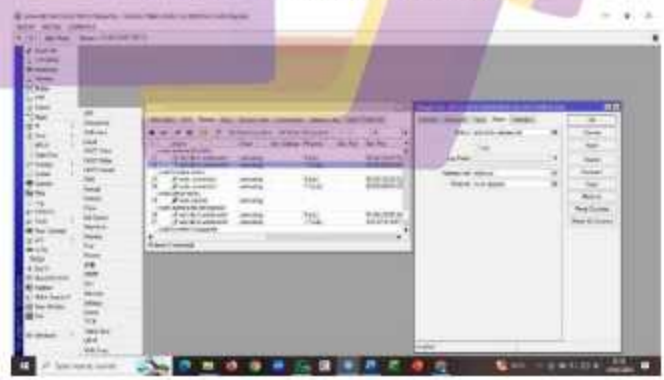


Gambar 4.5.2.3 Rule *Mangle* Roblox *TCP*

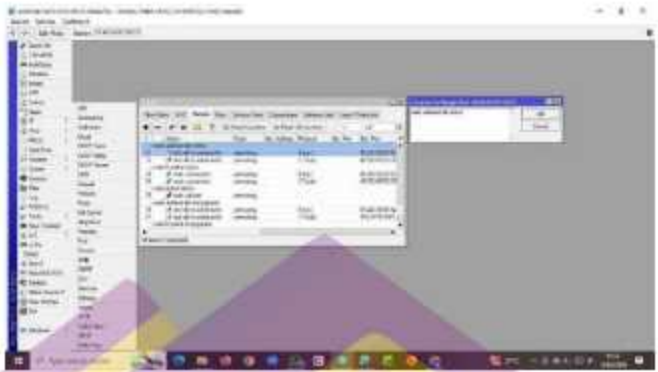
Gambar 4.5.2.3 Rule *Mangle* Roblox *TCP*



Gambar 4.5.2.3 Rule *Mangle* Roblox *UDP*



Gambar 4.5.2.3 Rule *Mangle* Roblox *UDP*



Gambar 4.5.2.3 Koment *Mangle* Sebagai Penanda Roblox

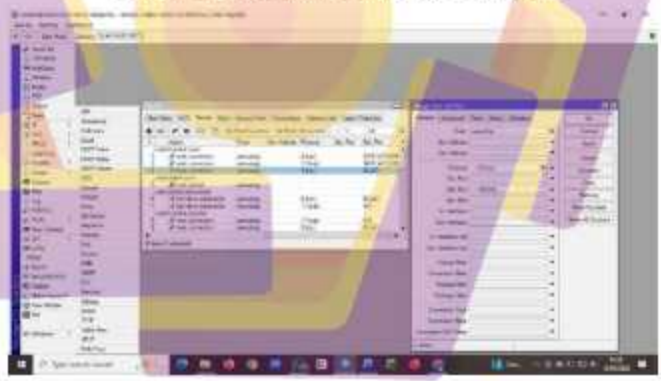
4.5.2.4 *Konfigurasi* Mark Connection *Firewall Mangle* Pembelajaran Daring

Konfigurasi mark connection pada *firewall mangle Mikrotik* digunakan untuk memberikan tanda terhadap koneksi trafik aplikasi pembelajaran daring agar *Router* dapat mengenali jenis koneksi yang melewati jaringan. Pada penelitian ini, proses mark connection diterapkan pada aplikasi Zoom dan *Gamelab* dengan memanfaatkan *Address List* yang sebelumnya telah dibuat melalui proses *firewall mangle*. *Konfigurasi* dilakukan pada menu IP → *Firewall* → *Mangle* menggunakan chain pre*routing*, karena proses identifikasi paket dilakukan sebelum paket diteruskan ke proses *routing* maupun manajemen *bandwidth*. Dengan metode tersebut, *Router* dapat melakukan pengaturan *Quality Of Service (QoS)* secara lebih optimal.

Setelah *Address List* zoom_ip dan *gamelab*_ip berhasil dibuat, tahap berikutnya adalah melakukan *Konfigurasi* mark connection untuk menandai koneksi masing-masing aplikasi. Administrator terlebih dahulu menambahkan rule baru pada *firewall mangle* dengan memilih chain pre*routing*. Pada bagian Advanced, parameter Dst. *Address List* diarahkan ke *Address List* zoom_ip. Pengaturan ini bertujuan agar *Router* hanya memproses koneksi yang menuju alamat IP server Zoom yang sebelumnya telah tersimpan pada daftar *Address List* tersebut. Selanjutnya pada tab Action, action dipilih mark-connection, kemudian pada parameter New

Connection Mark diberikan nama koneksi-zoom dan opsi passthrough diatur menjadi yes agar paket masih dapat diproses oleh rule berikutnya. Dengan *Konfigurasi* tersebut, seluruh koneksi yang menuju server Zoom akan dikenali dan ditandai oleh *Router* sebagai trafik pembelajaran daring Zoom.

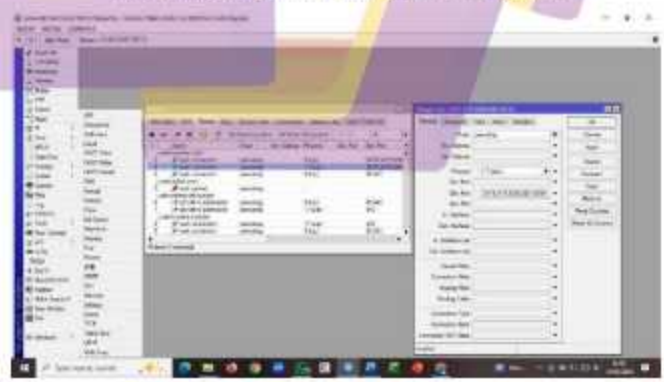
Gambar 4.5.2.4 Mark Connection *TCP* Zoom



Gambar 4.5.2.4 Mark Connection *TCP* Zoom

Gambar 4.5.2.4 Mark Connection *TCP* Zoom

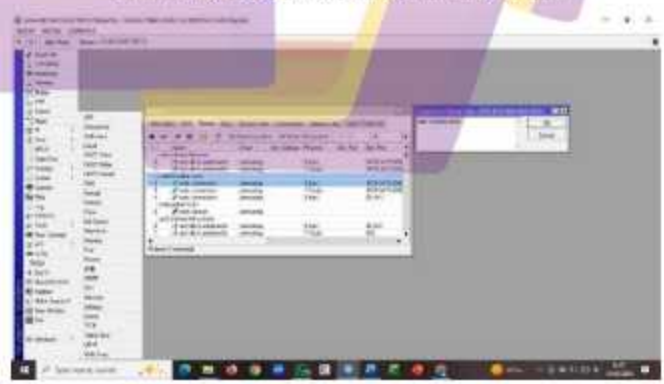
Gambar 4.5.2.4 Mark Connection *TCP* Zoom



Gambar 4.5.2.4 Mark Connection *UDP* Zoom

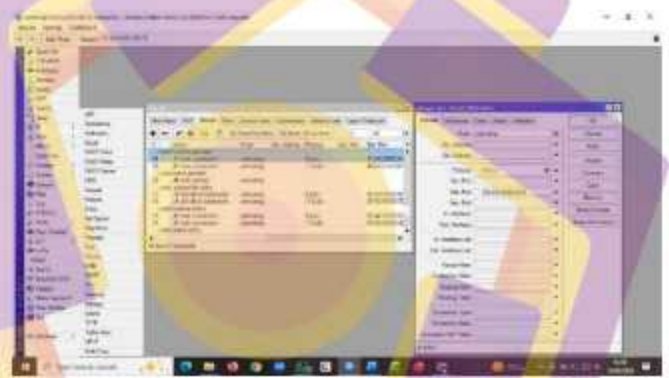
Gambar 4.5.2.4 Mark Connection *UDP* Zoom

Gambar 4.5.2.4 Mark Connection *UDP* Zoom

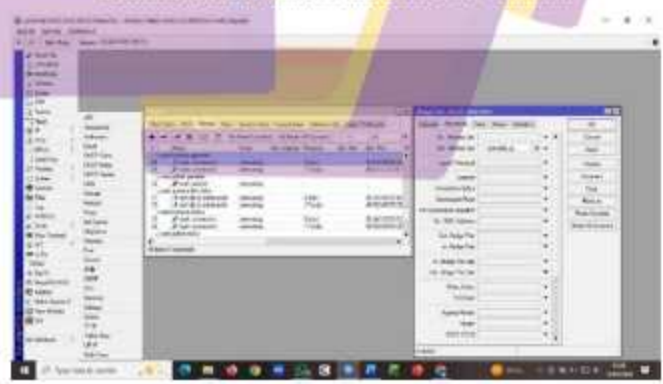


Gambar 4.5.2.4 Koment Mark Connection *UDP* Zoom

Konfigurasi yang sama juga diterapkan pada aplikasi *Gamelab*. Administrator kembali menambahkan rule baru pada menu *firewall mangle* menggunakan chain pre*routing*. Pada tab Advanced, parameter Dst. *Address List* diarahkan ke *gamelab*_ip sehingga *Router* hanya akan memproses koneksi yang menuju alamat IP server *Gamelab*. Selanjutnya pada bagian Action, action diatur menjadi mark-connection, kemudian pada parameter New Connection Mark diberikan nama koneksi-*gamelab* dengan opsi passthrough tetap diaktifkan. Melalui *Konfigurasi* tersebut, *Router Mikrotik* dapat memberikan tanda khusus terhadap seluruh koneksi *Gamelab* secara otomatis.

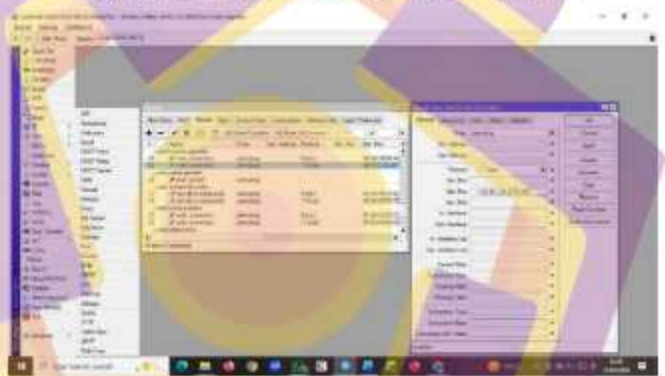


Gambar 4.5.2.4 Mark Connection *TCP Gamelab*

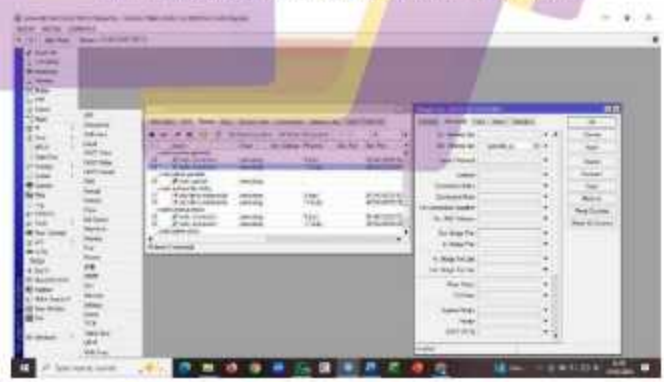


Gambar 4.5.2.4 Mark Connection *TCP Gamelab*

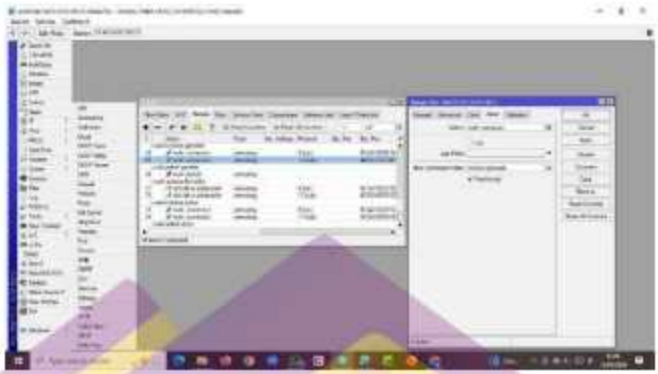
Gambar 4.5.2.4 Mark Connection *TCP Gamelab*



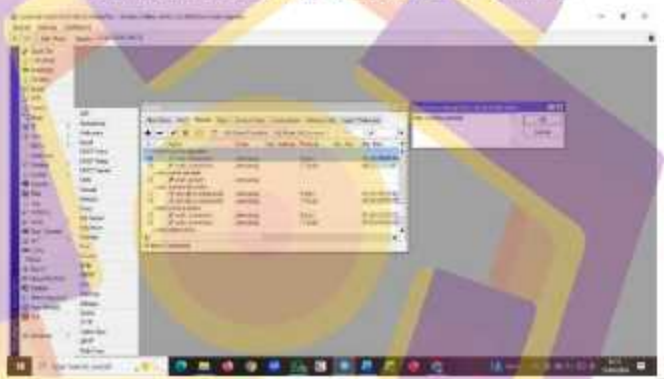
Gambar 4.5.2.4 Mark Connection *UDP Gamelab*



Gambar 4.5.2.4 Mark Connection *UDP Gamelab*



Gambar 4.5.2.4 Mark Connection *UDP Gamelab*



Gambar 4.5.2.4 Koment Mark Connection *Gamelab*

Dengan adanya proses mark connection menggunakan parameter Dst. *Address List* tersebut, *Router Mikrotik* mampu membedakan koneksi aplikasi Zoom dan *Gamelab* dari trafik *internet* lainnya. Penandaan koneksi ini menjadi dasar penting dalam penerapan packet mark, *Queue Tree*, manajemen *bandwidth*, serta pengaturan prioritas layanan jaringan. Melalui metode tersebut, administrator jaringan dapat memberikan prioritas *bandwidth* terhadap aplikasi pembelajaran daring sehingga proses belajar mengajar *online* dapat berlangsung lebih stabil, lancar, dan minim gangguan meskipun jaringan digunakan secara bersamaan oleh banyak pengguna.

4.5.2.5 *Konfigurasi* Mark Connection *Firewall Mangle* Media Sosial

Konfigurasi mark connection pada *firewall mangle Mikrotik* digunakan untuk memberikan tanda terhadap koneksi trafik aplikasi media sosial agar *Router* dapat mengenali dan membedakan jenis trafik yang melewati jaringan. Pada penelitian ini, proses mark connection diterapkan pada aplikasi YouTube, Instagram, Facebook, dan TikTok dengan memanfaatkan *Address List* yang sebelumnya telah dibuat melalui proses *firewall mangle*. *Konfigurasi* dilakukan melalui menu IP → *Firewall* → *Mangle* menggunakan chain pre*routing*, karena proses identifikasi paket dilakukan sebelum paket diteruskan menuju proses *routing* maupun manajemen *bandwidth*. Dengan metode tersebut, *Router Mikrotik* dapat melakukan pengaturan *bandwidth*, monitoring trafik, pembatasan akses, dan penerapan *Quality Of Service (QoS)* secara lebih optimal.

Tahap awal *Konfigurasi* dilakukan dengan membuat *Address List* berdasarkan *Destination Port* masing-masing aplikasi media sosial. Administrator terlebih dahulu menentukan *Protocol TCP* dan *UDP*, kemudian memasukkan *Destination Port* aplikasi yang akan dideteksi. Aplikasi YouTube menggunakan *Port TCP* 80 dan 443 serta *UDP* 443. Instagram menggunakan *Port TCP* 80 dan 443 serta *UDP* 443. Facebook menggunakan *Port TCP* 80 dan 443 serta *UDP* 3478–3481 dan 443. Sementara itu, TikTok menggunakan *Port TCP* 80, 443, dan 8080 serta *UDP* 443 dan 3478–3497. Setelah paket dengan *Port* tersebut terdeteksi, action pada *firewall mangle* diatur menjadi add-dst-to-address-list sehingga *Router* secara otomatis menyimpan alamat IP tujuan ke dalam daftar alamat tertentu. Trafik YouTube disimpan pada *Address List* youtube_ip, Instagram pada instagram_ip, Facebook pada facebook_ip, dan TikTok pada tiktok_ip.

Setelah proses pembuatan *Address List* selesai dilakukan, tahap berikutnya adalah melakukan *Konfigurasi* mark connection untuk menandai koneksi masing-masing aplikasi media sosial. Administrator masuk ke menu IP → *Firewall* → *Mangle* kemudian menambahkan rule baru

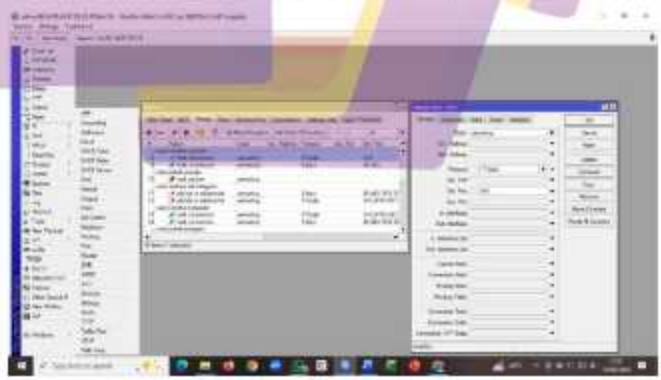
menggunakan chain pre*routing*. Pada tab Advanced, parameter Dst. *Address List* diarahkan ke *Address List* aplikasi yang sebelumnya telah dibuat. Selanjutnya pada tab Action, action diatur menjadi mark-connection dan pada parameter New Connection Mark diberikan nama koneksi sesuai aplikasi yang digunakan.

Pada *Konfigurasi* aplikasi YouTube, administrator membuat rule baru dengan memilih Dst. *Address List* menuju youtube_ip pada tab Advanced. Selanjutnya pada bagian Action dipilih mark-connection, kemudian parameter New Connection Mark diisi dengan nama koneksi-youtube dan opsi passthrough diatur menjadi yes agar paket masih dapat diproses oleh rule berikutnya. Dengan *Konfigurasi* tersebut, seluruh koneksi yang menuju server YouTube akan dikenali dan ditandai secara otomatis oleh *Router Mikrotik*.

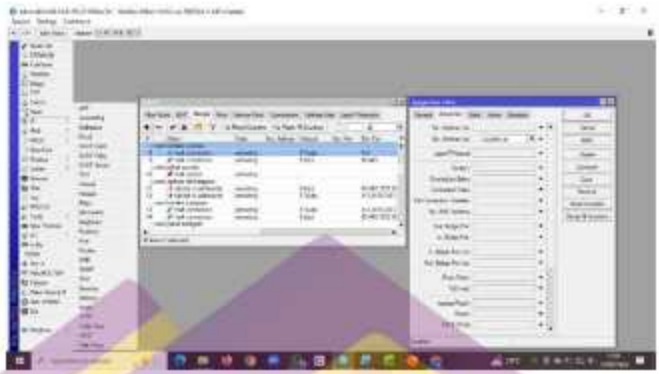
Gambar 4.5.2.5 Mark Connection *TCP* Youtube

Gambar 4.5.2.5 Mark Connection *TCP* Youtube

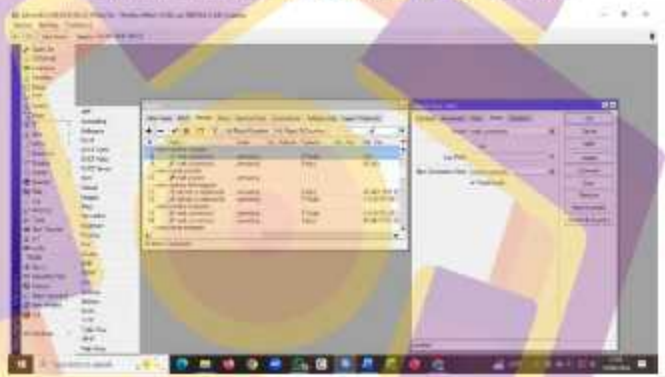
Gambar 4.5.2.5 Mark Connection *TCP* Youtube



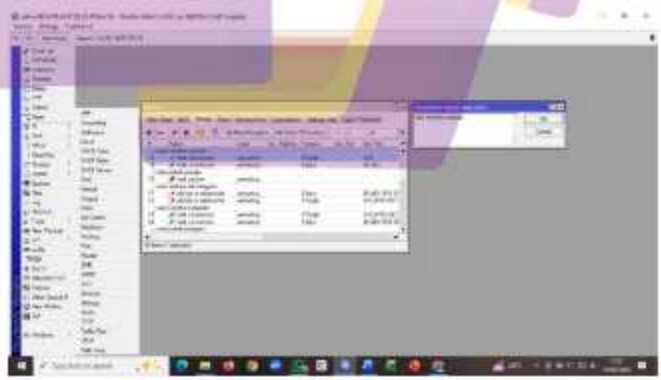
Gambar 4.5.2.5 Mark Connection *UDP* Youtube



Gambar 4.5.2.5 Mark Connection *UDP* Youtube

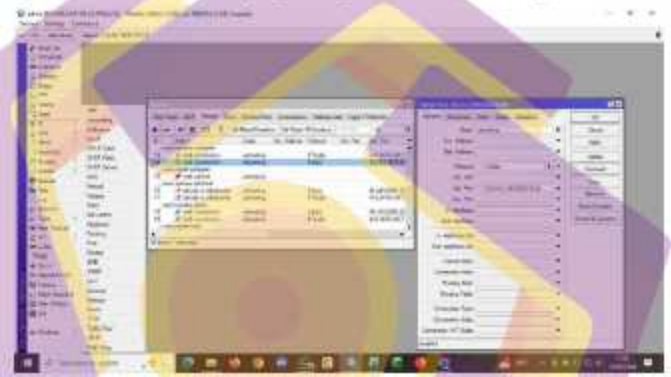


Gambar 4.5.2.5 Mark Connection *UDP* Youtube

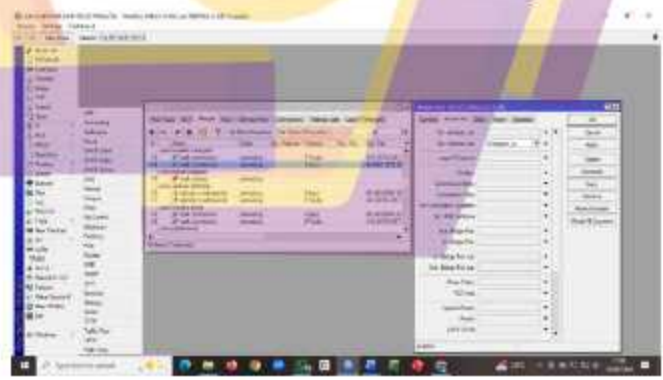


Gambar 4.5.2.5 Koment Mark Connection Youtube

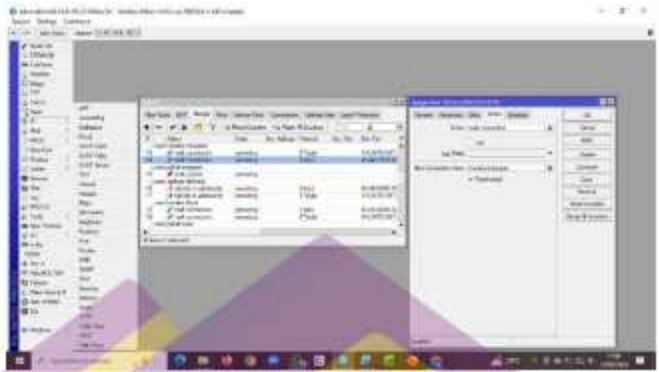
Konfigurasi yang sama diterapkan pada aplikasi Instagram. Administrator membuat rule baru menggunakan chain pre*routing*, kemudian pada tab Advanced parameter Dst. *Address List* diarahkan ke instagram_ip. Selanjutnya pada tab Action dipilih mark-connection dan parameter New Connection Mark diisi dengan nama koneksi-instagram. Opsi passthrough tetap diaktifkan agar proses identifikasi paket dapat dilanjutkan ke rule berikutnya. Melalui *Konfigurasi* tersebut, *Router* dapat mengenali seluruh koneksi yang mengarah ke server Instagram.



Gambar 4.5.2.5 Mark Connection *TCP* Instagram

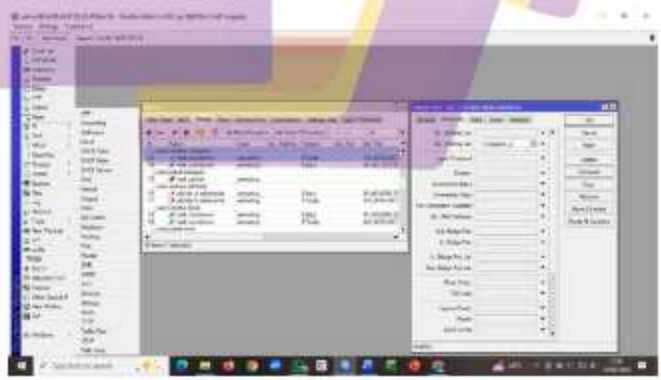


Gambar 4.5.2.5 Mark Connection *TCP* Instagram

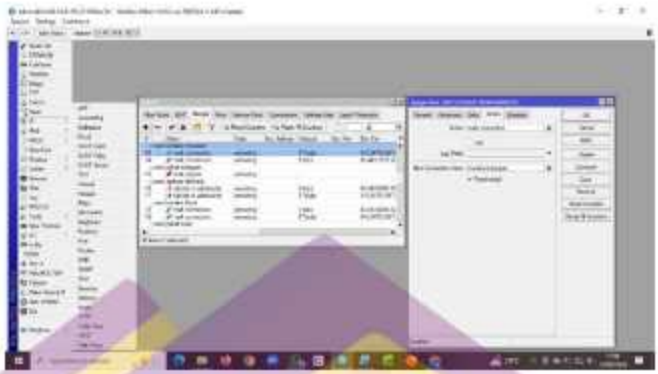


Gambar 4.5.2.5 Mark Connection *TCP* Instagram

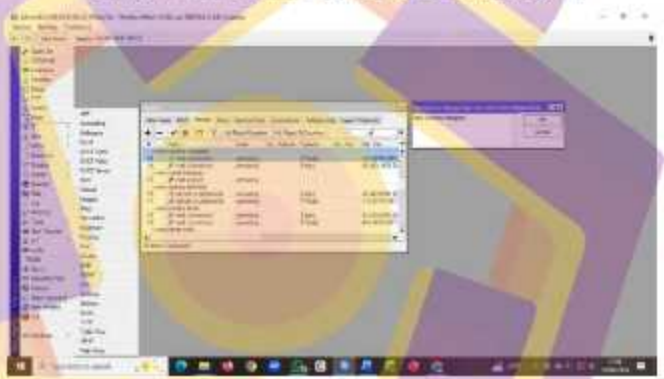
Gambar 4.5.2.5 Mark Connection *UDP* Instagram



Gambar 4.5.2.5 Mark Connection *UDP* Instagram

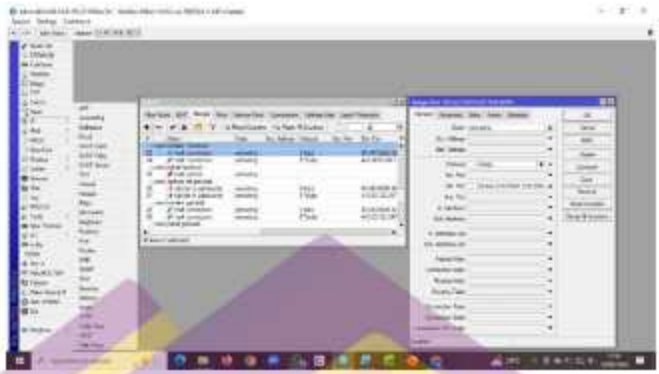


Gambar 4.5.2.5 Mark Connection *UDP* Instagram

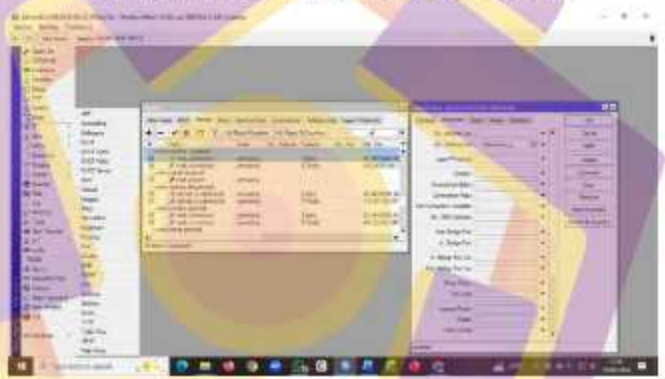


Gambar 4.5.2.5 Koment Mark Connection Instagram

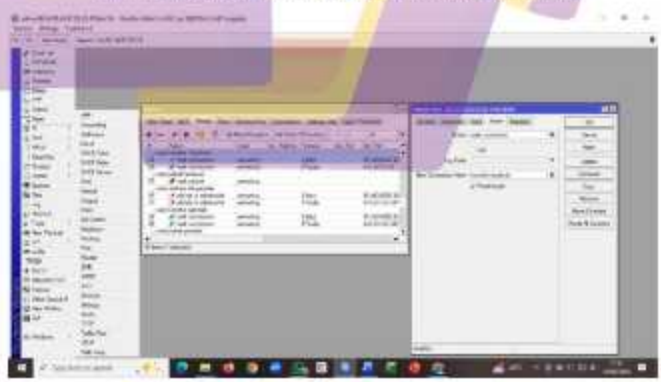
Pada aplikasi Facebook, administrator kembali menambahkan rule *firewall mangle* dengan menggunakan Dst. *Address List* menuju facebook_ip pada tab Advanced. Setelah itu, pada bagian Action dipilih mark-connection dan parameter New Connection Mark diisi dengan nama koneksi-facebook. *Konfigurasi* ini memungkinkan *Router Mikrotik* untuk menandai seluruh koneksi yang menuju layanan Facebook sehingga trafik media sosial dapat dipisahkan dari trafik *internet* lainnya.



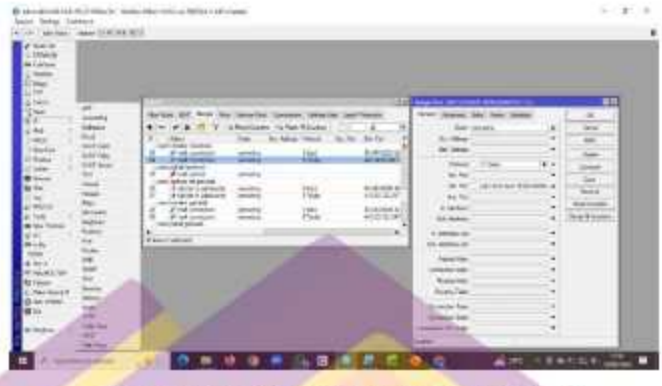
Gambar 4.5.2.5 Mark Connection *TCP* Facebook



Gambar 4.5.2.5 Mark Connection *TCP* Facebook

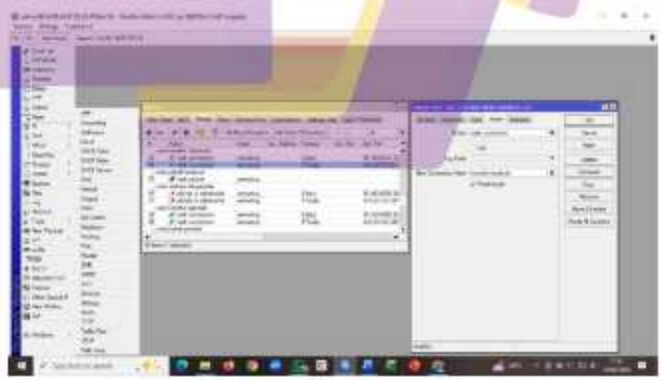


Gambar 4.5.2.5 Mark Connection *TCP* Facebook

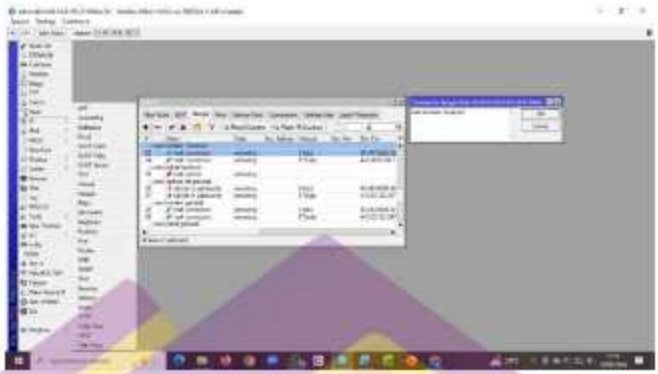


Gambar 4.5.2.5 Mark Connection *UDP* Facebook

Gambar 4.5.2.5 Mark Connection *UDP* Facebook

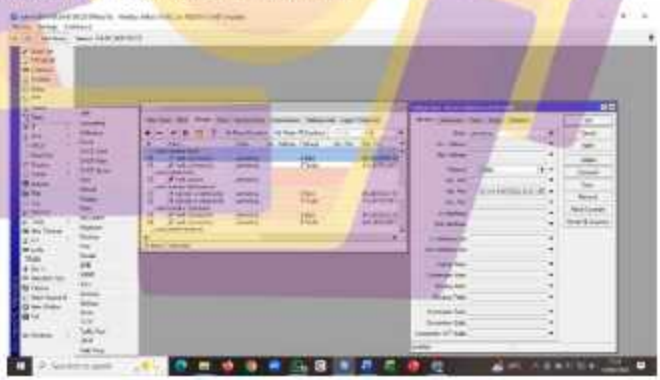


Gambar 4.5.2.5 Mark Connection *UDP* Facebook

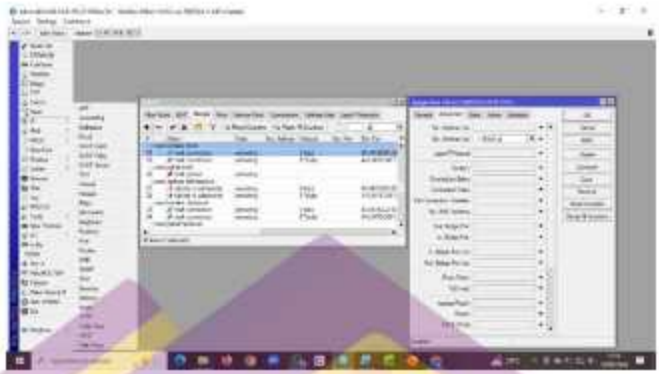


Gambar 4.5.2.5 Koment Mark Connection Facebook

Selanjutnya pada aplikasi TikTok, administrator membuat rule baru menggunakan chain pre*routing* dengan parameter Dst. *Address List* diarahkan ke tiktok_ip. Pada bagian Action dipilih mark-connection, kemudian parameter New Connection Mark diisi dengan nama koneksi-tiktok dan opsi passthrough diatur menjadi yes. Dengan *Konfigurasi* tersebut, *Router* dapat mengenali serta menandai seluruh koneksi yang menuju server TikTok secara otomatis.

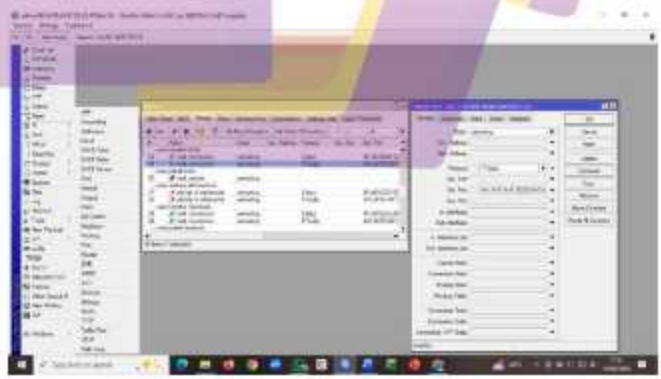


Gambar 4.5.2.5 Mark Connection *TCP* Tiktok

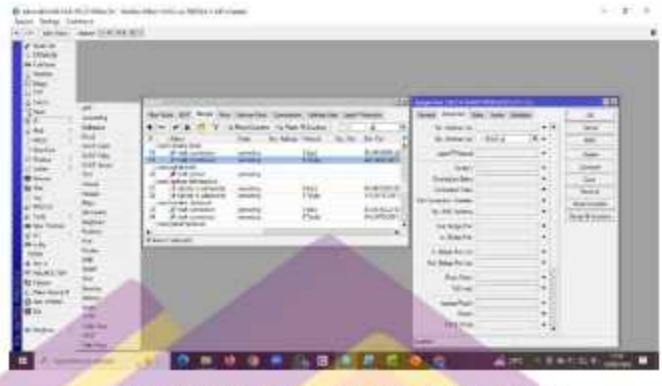


Gambar 4.5.2.5 Mark Connection *TCP* Tiktok

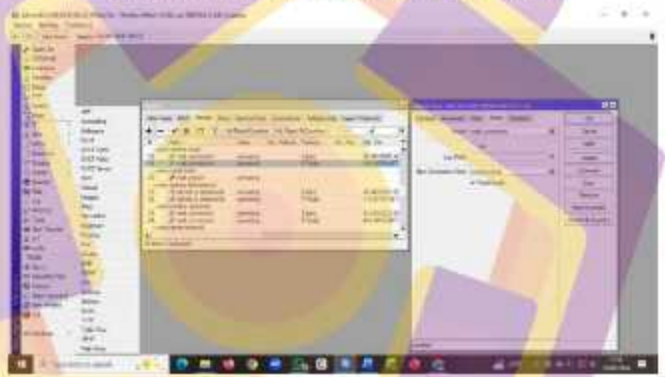
Gambar 4.5.2.5 Mark Connection *TCP* Tiktok



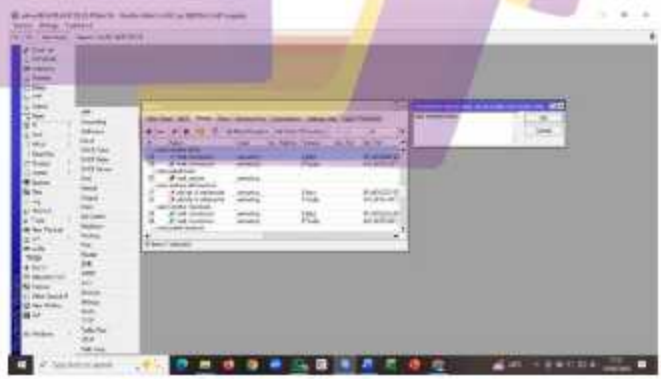
Gambar 4.5.2.5 Mark Connection *UDP* Tiktok



Gambar 4.5.2.5 Mark Connection *UDP* Tiktok



Gambar 4.5.2.5 Mark Connection *UDP* Tiktok



Gambar 4.5.2.5 Koment Mark Connection Tiktok

Melalui proses mark connection tersebut, *Router Mikrotik* dapat mengidentifikasi dan mengelompokkan koneksi aplikasi media sosial berdasarkan jenis aplikasinya. Penandaan koneksi ini menjadi dasar penting dalam penerapan packet *marking*, *Queue Tree*, manajemen *bandwidth*, monitoring penggunaan *internet*, serta pengaturan prioritas layanan jaringan. Dengan adanya pengelompokan trafik media sosial tersebut, administrator jaringan dapat lebih mudah melakukan pembatasan *bandwidth*, pengawasan penggunaan *internet*, dan optimalisasi *Quality Of Service (QoS)* sehingga stabilitas dan efisiensi jaringan *internet* dapat terjaga dengan lebih baik.

4.5.2.6 *Konfigurasi* Mark Connection *Firewall Mangle* Games *Online*

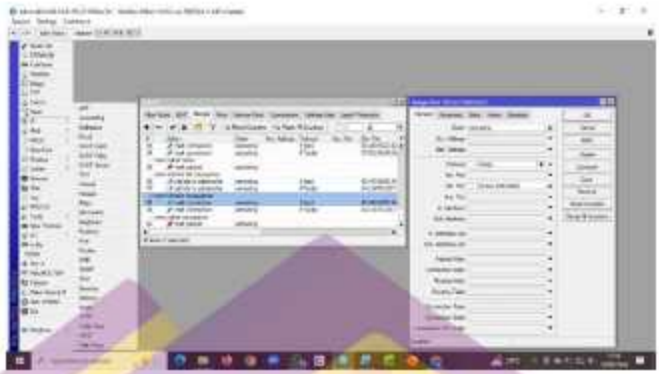
Konfigurasi mark connection pada *firewall mangle Mikrotik* digunakan untuk memberikan tanda terhadap koneksi trafik game *online* agar *Router* dapat mengenali dan membedakan jenis trafik permainan yang melewati jaringan. Pada penelitian ini, proses mark connection diterapkan pada aplikasi game *online* CrazyGames dan Roblox dengan memanfaatkan *Address List* yang sebelumnya telah dibuat melalui *firewall mangle*. *Konfigurasi* dilakukan melalui menu IP → *Firewall* → *Mangle* menggunakan chain pre*routing*, karena proses identifikasi dan penandaan paket dilakukan sebelum paket diteruskan menuju proses *routing* maupun manajemen *bandwidth*. Dengan metode tersebut, *Router Mikrotik* dapat melakukan pengaturan *bandwidth*, monitoring trafik, pembatasan akses permainan *online*, serta penerapan *Quality Of Service (QoS)* secara lebih optimal.

Tahap awal *Konfigurasi* dilakukan dengan membuat *Address List* berdasarkan *Destination Port* dari masing-masing aplikasi game *online*. Administrator terlebih dahulu menentukan *Protocol TCP* dan *UDP*, kemudian memasukkan *Destination Port* yang digunakan oleh CrazyGames dan Roblox. Aplikasi CrazyGames menggunakan *Port TCP* 80 dan 443 serta *UDP* 3478–3480 untuk mendukung koneksi game berbasis browser dan layanan WebRTC. Sementara itu, Roblox menggunakan *Port TCP* 80

dan 443 serta *UDP* 49152–65535 yang digunakan untuk komunikasi *real-time* dalam permainan *online*. Setelah paket dengan *Port* tersebut terdeteksi, action pada *firewall mangle* diatur menjadi add-dst-to-address-list sehingga *Router* secara otomatis menyimpan alamat IP tujuan ke dalam daftar alamat tertentu. Trafik CrazyGames disimpan pada *Address List* crazygames_ip, sedangkan trafik Roblox disimpan pada *Address List* roblox_ip.

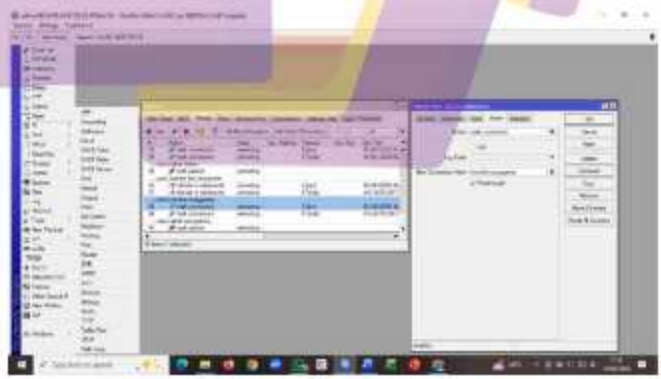
Setelah proses pembuatan *Address List* selesai dilakukan, tahap berikutnya adalah melakukan *Konfigurasi* mark connection untuk menandai koneksi masing-masing aplikasi game *online*. Administrator masuk ke menu IP → *Firewall* → *Mangle* kemudian menambahkan rule baru menggunakan chain pre*routing*. Pada tab Advanced, parameter Dst. *Address List* diarahkan ke *Address List* aplikasi game yang sebelumnya telah dibuat. Selanjutnya pada tab Action, action diatur menjadi mark-connection dan parameter New Connection Mark diberikan nama koneksi sesuai aplikasi game yang digunakan.

Pada *Konfigurasi* aplikasi CrazyGames, administrator membuat rule baru dengan memilih Dst. *Address List* menuju crazygames_ip pada tab Advanced. Selanjutnya pada bagian Action dipilih mark-connection, kemudian parameter New Connection Mark diisi dengan nama koneksi-crazygames dan opsi passthrough diatur menjadi yes agar paket masih dapat diproses pada rule berikutnya. Dengan *Konfigurasi* tersebut, seluruh koneksi yang menuju server CrazyGames akan dikenali dan ditandai secara otomatis oleh *Router Mikrotik* sebagai trafik game *online*.

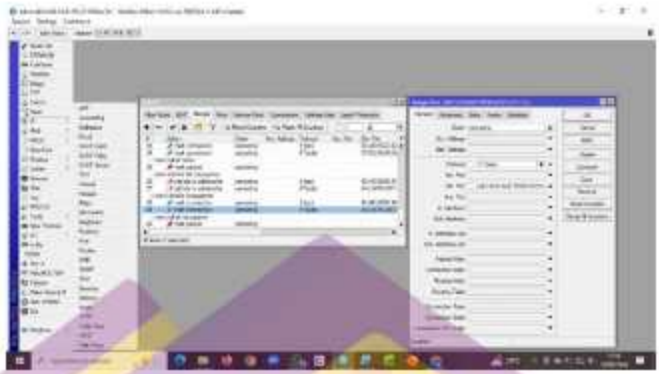


Gambar 4.5.2.6 Mark Connection *TCP* Crazygames

Gambar 4.5.2.6 Mark Connection *TCP* Crazygames

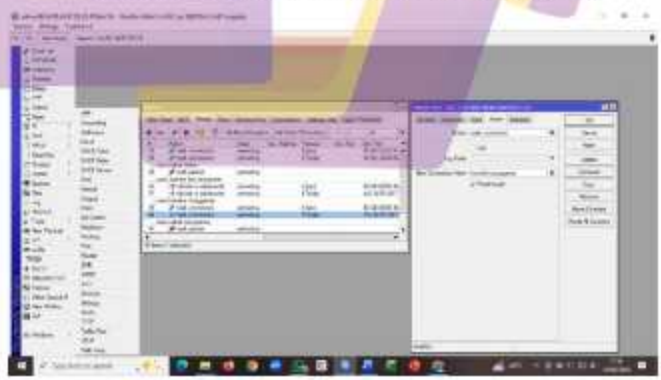


Gambar 4.5.2.6 Mark Connection *TCP* Crazygames

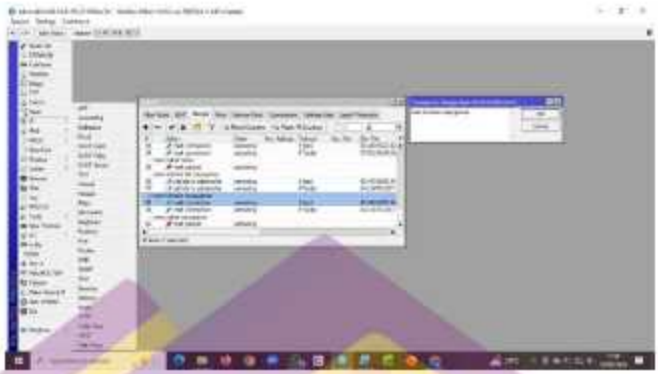


Gambar 4.5.2.6 Mark Connection *UDP* Crazygames

Gambar 4.5.2.6 Mark Connection *UDP* Crazygames

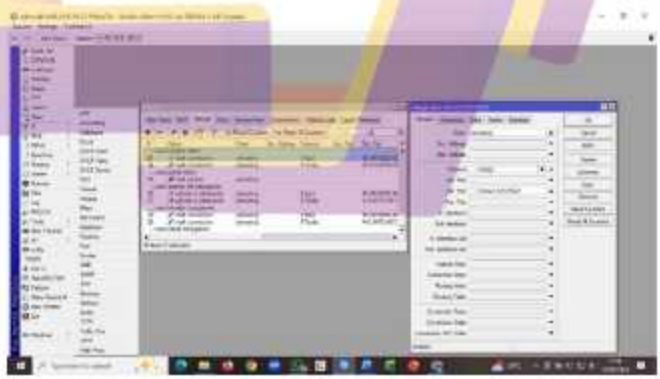


Gambar 4.5.2.6 Mark Connection *UDP* Crazygames

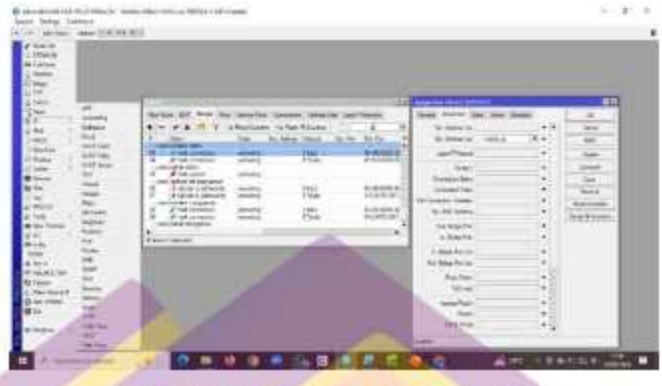


Gambar 4.5.2.6 Koment Mark Connection Crazygames

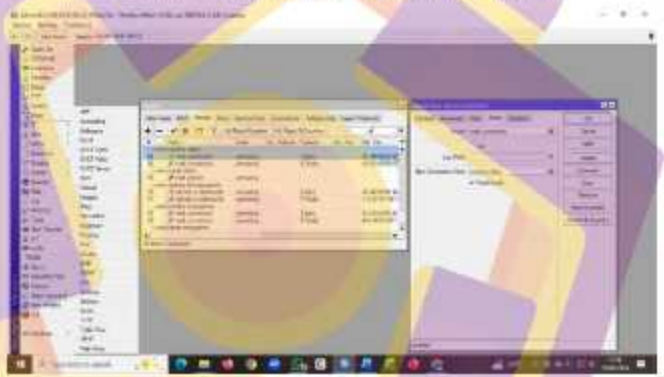
Konfigurasi yang sama diterapkan pada aplikasi Roblox. Administrator kembali menambahkan rule *firewall mangle* menggunakan chain pre*routing*, kemudian pada tab Advanced parameter Dst. *Address List* diarahkan ke roblox_ip. Selanjutnya pada bagian Action dipilih mark-connection dan parameter New Connection Mark diisi dengan nama koneksi-roblox. Opsi passthrough tetap diaktifkan agar paket masih dapat diproses oleh rule *mangle* berikutnya. Melalui *Konfigurasi* tersebut, seluruh koneksi yang menuju server Roblox akan dikenali dan ditandai secara otomatis oleh *Router Mikrotik*.



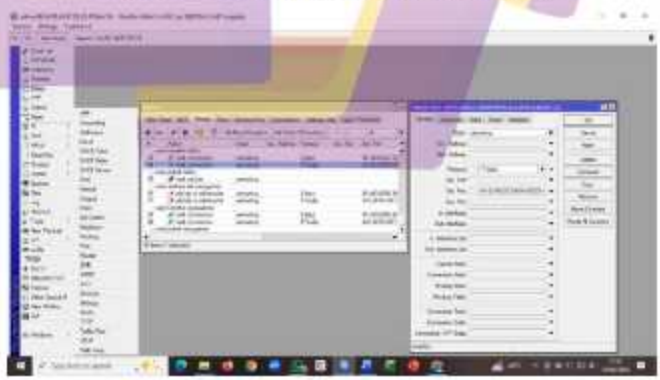
Gambar 4.5.2.6 Mark Connection *TCP* Roblox



Gambar 4.5.2.6 Mark Connection *TCP* Roblox



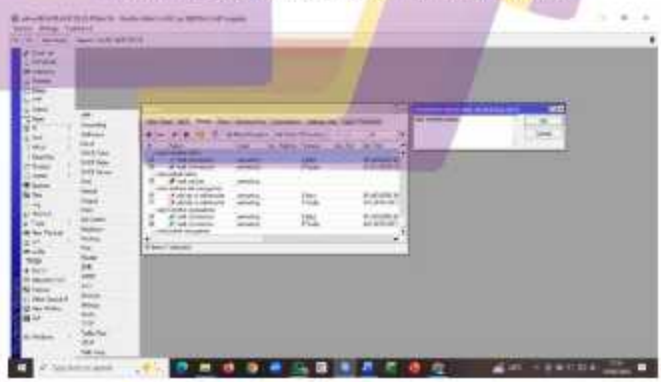
Gambar 4.5.2.6 Mark Connection *TCP* Roblox



Gambar 4.5.2.6 Mark Connection *UDP* Roblox

Gambar 4.5.2.6 Mark Connection *UDP* Roblox

Gambar 4.5.2.6 Mark Connection *UDP* Roblox



Gambar 4.5.2.6 Koment Mark Connection Roblox

Melalui proses mark connection tersebut, *Router Mikrotik* dapat mengidentifikasi dan mengelompokkan koneksi game *online* berdasarkan jenis aplikasinya. Penandaan koneksi ini menjadi dasar penting dalam penerapan packet *marking*, *Queue Tree*, manajemen *bandwidth*, monitoring penggunaan *internet*, serta pengaturan prioritas layanan jaringan. Dengan adanya pengelompokan trafik game *online* tersebut, administrator jaringan dapat lebih mudah melakukan pembatasan *bandwidth* permainan *online*, pengendalian akses game, serta optimalisasi *Quality Of Service (QoS)* sehingga stabilitas, efisiensi, dan performa jaringan *internet* dapat tetap terjaga meskipun digunakan secara bersamaan oleh banyak pengguna.

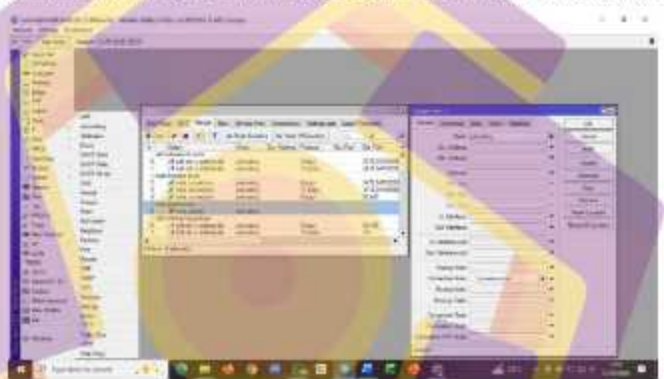
4.5.2.7 *Konfigurasi* Mark Packet *Firewall Mangle* Pembelajaran Daring

Konfigurasi mark packet pada *firewall mangle Mikrotik* digunakan untuk memberikan tanda terhadap paket data yang sebelumnya telah dikenali melalui proses mark connection. Pada penelitian ini, mark packet diterapkan pada trafik aplikasi pembelajaran daring, yaitu Zoom dan *Gamelab*, dengan tujuan agar *Router* dapat mengelompokkan paket data berdasarkan jenis aplikasinya. Penandaan paket ini sangat penting dalam penerapan manajemen *bandwidth*, *Queue Tree*, prioritas layanan, serta *Quality Of Service (QoS)*, karena *Router* akan lebih mudah mengatur trafik sesuai kategori paket yang telah ditentukan.

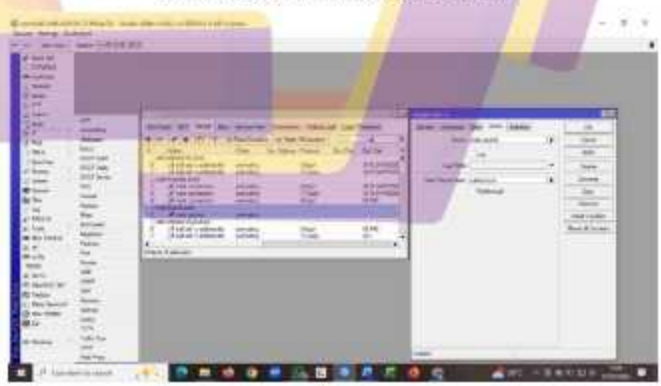
Proses *Konfigurasi* dilakukan melalui menu IP → *Firewall* → *Mangle* menggunakan chain pre*routing*, karena proses identifikasi paket dilakukan sebelum paket diteruskan menuju proses *routing* maupun pengelolaan *bandwidth*. Sebelum melakukan mark packet, administrator terlebih dahulu harus membuat mark connection untuk masing-masing aplikasi pembelajaran daring. Pada tahap sebelumnya, koneksi Zoom telah diberi tanda dengan nama koneksi-zoom, sedangkan koneksi *Gamelab* diberi tanda dengan nama koneksi-*gamelab*. Mark connection tersebut kemudian digunakan sebagai acuan dalam proses penandaan paket data.

Tahap pertama *Konfigurasi* dilakukan dengan membuat rule mark packet untuk aplikasi Zoom. Administrator masuk ke menu IP → *Firewall*

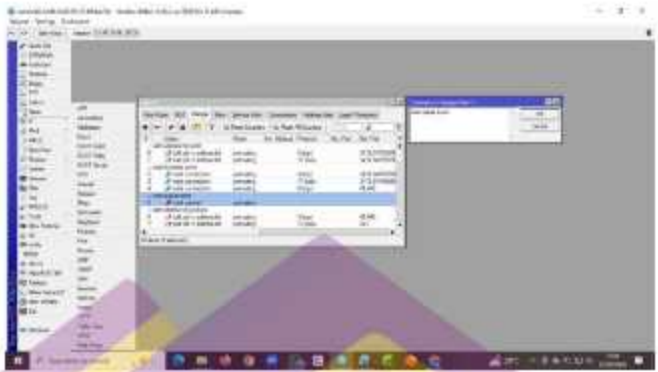
→ *Mangle*, kemudian menambahkan rule baru menggunakan chain pre*routing*. Pada bagian General, parameter Connection Mark diarahkan ke koneksi-zoom sehingga *Router* hanya akan memproses paket yang berasal dari koneksi Zoom. Selanjutnya pada tab Action, action diatur menjadi mark-packet, kemudian pada parameter New Packet Mark diberikan nama paket-zoom. Opsi passthrough diatur menjadi no agar paket tidak perlu diproses kembali oleh rule mark packet berikutnya setelah berhasil ditandai. Dengan *Konfigurasi* tersebut, seluruh paket data yang berasal dari koneksi Zoom akan dikenali dan ditandai secara otomatis oleh *Router Mikrotik*.



Gambar 4.5.2.7 Mark Packet Zoom

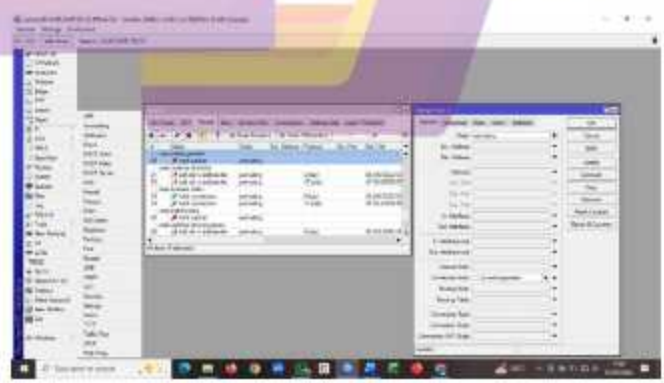


Gambar 4.5.2.7 Mark Packet Zoom

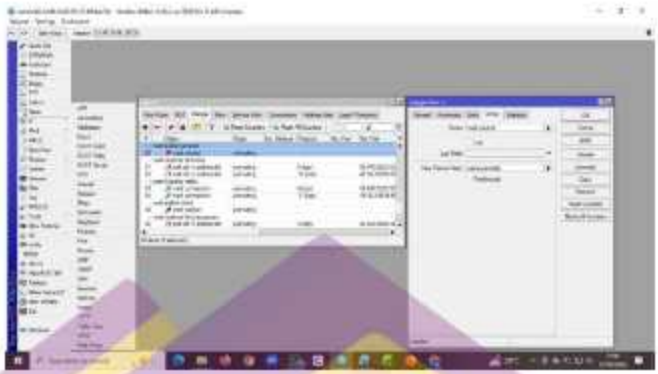


Gambar 4.5.2.7 Koment Mark Packet Zoom

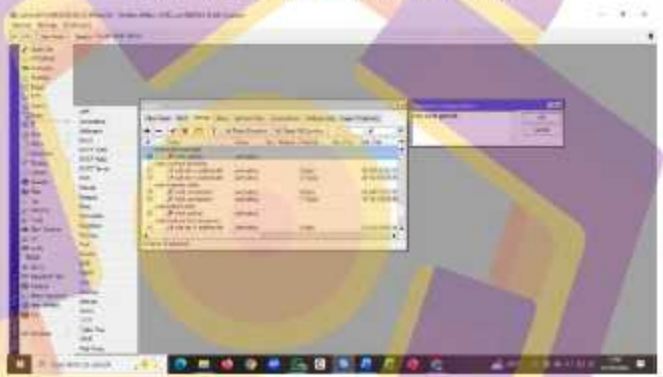
Konfigurasi yang sama diterapkan pada aplikasi *Gamelab*. Administrator kembali menambahkan rule baru menggunakan chain pre*routing*, kemudian pada parameter Connection Mark diarahkan ke koneksi-*gamelab*. Pengaturan ini bertujuan agar *Router* hanya memproses paket yang berasal dari koneksi *Gamelab*. Selanjutnya pada bagian Action, action dipilih mark-packet, kemudian parameter New Packet Mark diisi dengan nama paket-*gamelab*. Opsi passthrough diatur menjadi no sehingga paket yang telah ditandai tidak diproses kembali oleh rule berikutnya. Dengan *Konfigurasi* tersebut, seluruh paket data yang berasal dari aplikasi *Gamelab* akan dikenali dan diberi tanda secara otomatis oleh *Router Mikrotik*.



Gambar 4.5.2.7 Mark Packet *Gamelab*



Gambar 4.5.2.7 Mark Packet *Gamelab*



Gambar 4.5.2.7 Koment Mark Packet *Gamelab*

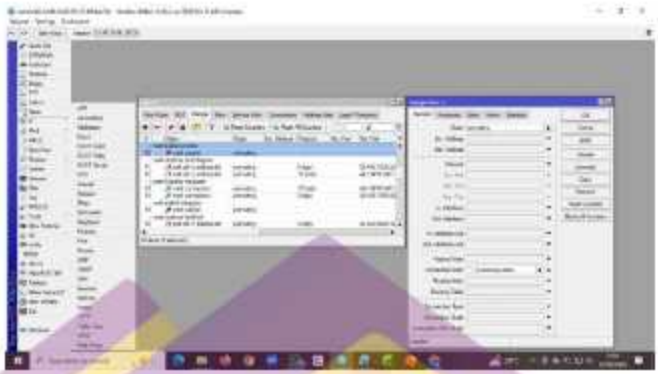
Melalui proses mark packet tersebut, *Router Mikrotik* dapat membedakan paket trafik pembelajaran daring berdasarkan jenis aplikasinya. Penandaan paket ini menjadi dasar utama dalam penerapan *Queue Tree* dan pengaturan *bandwidth* sehingga administrator jaringan dapat memberikan prioritas layanan terhadap aplikasi pembelajaran daring. Dengan adanya pengelompokan paket data tersebut, kualitas koneksi saat video *conference*, pengiriman materi pembelajaran, maupun aktivitas belajar mengajar *online* dapat berjalan lebih stabil, lancar, dan minim gangguan meskipun jaringan digunakan secara bersamaan oleh banyak pengguna.

4.5.2.8 *Konfigurasi* Mark Packet *Firewall Mangle* Media Sosial

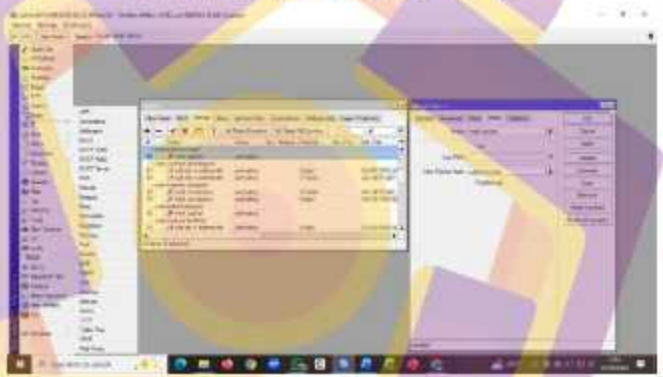
Konfigurasi mark packet pada *firewall mangle Mikrotik* digunakan untuk memberikan tanda terhadap paket data yang sebelumnya telah dikenali melalui proses mark connection. Pada penelitian ini, mark packet diterapkan pada trafik aplikasi media sosial seperti YouTube, Instagram, Facebook, dan TikTok. Tujuan utama *Konfigurasi* ini adalah agar *Router Mikrotik* dapat mengelompokkan paket data berdasarkan jenis aplikasi media sosial sehingga administrator jaringan lebih mudah dalam melakukan pengaturan *bandwidth*, monitoring trafik, pembatasan akses, serta penerapan *Quality Of Service (QoS)*.

Konfigurasi dilakukan melalui menu IP → *Firewall* → *Mangle* menggunakan chain pre*routing*, karena proses identifikasi paket dilakukan sebelum paket diteruskan menuju proses *routing* maupun manajemen *bandwidth*. Sebelum melakukan mark packet, administrator terlebih dahulu harus membuat mark connection untuk masing-masing aplikasi media sosial. Pada tahap sebelumnya, koneksi YouTube telah diberi tanda dengan nama koneksi-youtube, Instagram dengan nama koneksi-instagram, Facebook dengan nama koneksi-facebook, dan TikTok dengan nama koneksi-tiktok. Seluruh connection mark tersebut kemudian digunakan sebagai dasar dalam proses penandaan paket data.

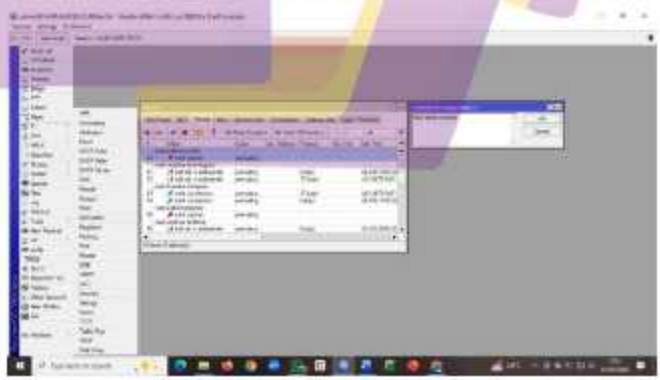
Tahap pertama *Konfigurasi* dilakukan dengan membuat rule mark packet untuk aplikasi YouTube. Administrator masuk ke menu IP → *Firewall* → *Mangle*, kemudian menambahkan rule baru menggunakan chain pre*routing*. Pada bagian General, parameter Connection Mark diarahkan ke koneksi-youtube sehingga *Router* hanya akan memproses paket yang berasal dari koneksi YouTube. Selanjutnya pada tab Action, action diatur menjadi mark-packet, kemudian parameter New Packet Mark diberikan nama paket-youtube. Opsi passthrough diatur menjadi no agar paket yang telah ditandai tidak diproses kembali oleh rule berikutnya. Dengan *Konfigurasi* tersebut, seluruh paket data dari aplikasi YouTube akan dikenali dan ditandai secara otomatis oleh *Router Mikrotik*.



Gambar 4.5.2.8 Mark Packet Youtube



Gambar 4.5.2.8 Mark Packet Youtube

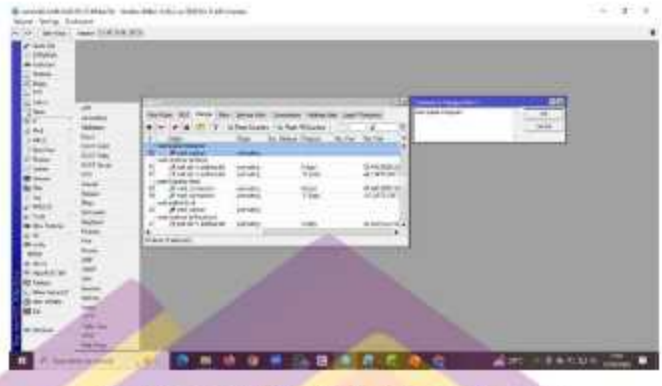


Gambar 4.5.2.8 Koment Mark Packet Youtube

Konfigurasi yang sama diterapkan pada aplikasi Instagram. Administrator kembali menambahkan rule baru menggunakan chain pre*routing*, kemudian pada parameter Connection Mark diarahkan ke koneksi-instagram. Selanjutnya pada bagian Action, action dipilih mark-packet, kemudian parameter New Packet Mark diisi dengan nama paket-instagram dan opsi passthrough diatur menjadi no. Melalui *Konfigurasi* tersebut, seluruh paket data yang berasal dari aplikasi Instagram akan dikenali dan ditandai secara otomatis oleh *Router Mikrotik*.

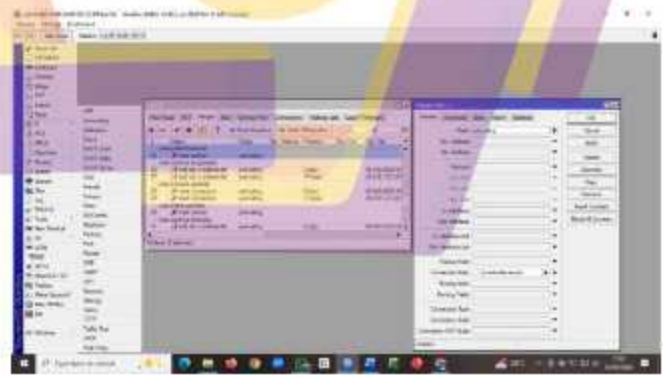
Gambar 4.5.2.8 Mark Packet Instagram

Gambar 4.5.2.8 Mark Packet Instagram

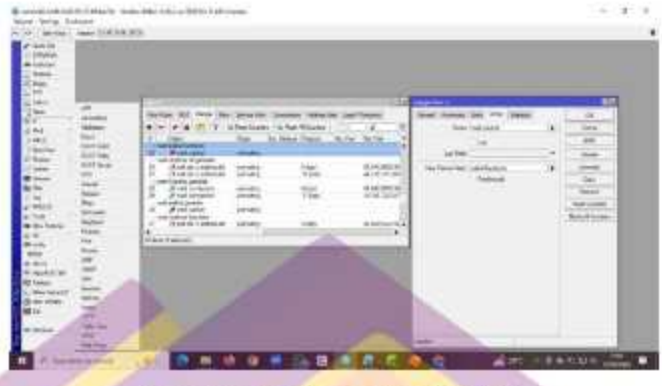


Gambar 4.5.2.8 Koment Mark Packet Instagram

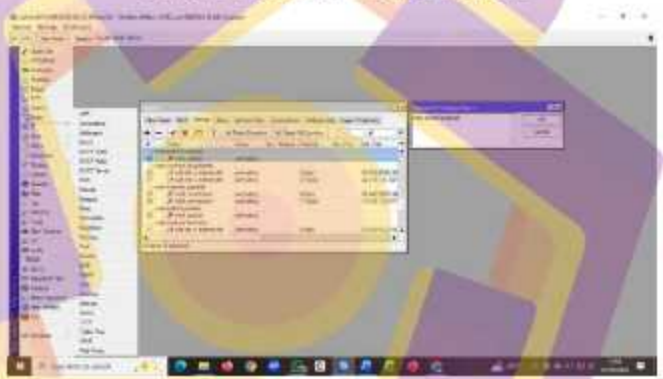
Pada aplikasi Facebook, administrator menambahkan rule *firewall mangle* dengan memilih Connection Mark menuju koneksi-facebook. Selanjutnya pada bagian Action dipilih mark-packet, kemudian parameter New Packet Mark diisi dengan nama paket-facebook. Opsi passthrough tetap diatur menjadi no agar paket yang telah ditandai tidak diproses kembali oleh rule berikutnya. Dengan *Konfigurasi* tersebut, *Router Mikrotik* dapat mengidentifikasi seluruh paket data yang berasal dari aplikasi Facebook secara otomatis.



Gambar 4.5.2.8 Mark Packet Facebook

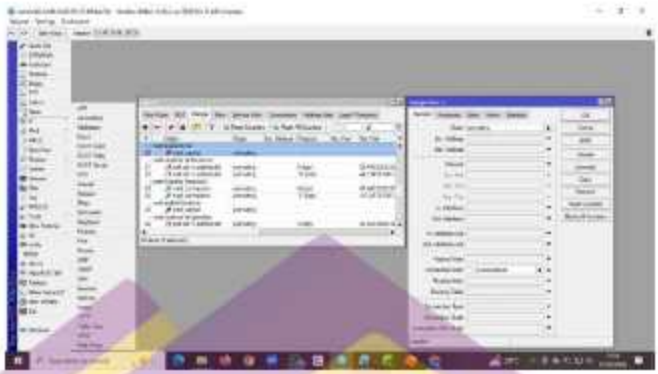


Gambar 4.5.2.8 Mark Packet Facebook

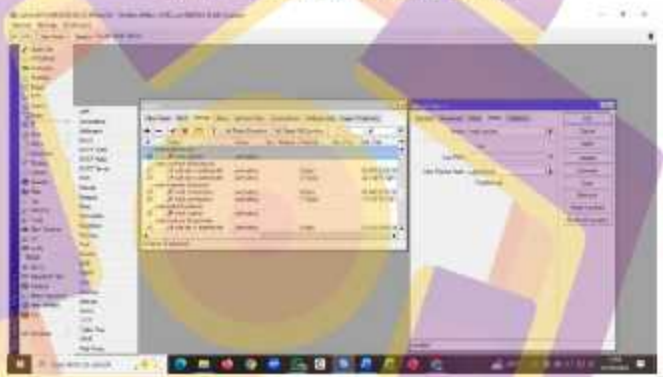


Gambar 4.5.2.8 Koment Mark Packet Facebook

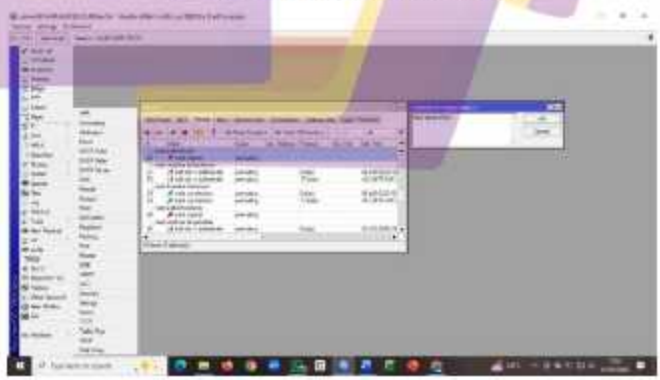
Selanjutnya pada aplikasi TikTok, administrator membuat rule baru menggunakan chain pre*routing* dengan parameter Connection Mark diarahkan ke koneksi-tiktok. Pada bagian Action dipilih mark-packet, kemudian parameter New Packet Mark diisi dengan nama paket-tiktok dan opsi passthrough diatur menjadi no. Dengan *Konfigurasi* tersebut, seluruh paket data yang berasal dari aplikasi TikTok akan dikenali dan ditandai secara otomatis oleh *Router Mikrotik*.



Gambar 4.5.2.8 Mark Packet Tiktok



Gambar 4.5.2.8 Mark Packet Tiktok



Gambar 4.5.2.8 Koment Mark Packet Tiktok

Melalui proses mark packet tersebut, *Router Mikrotik* dapat mengelompokkan paket data media sosial berdasarkan jenis aplikasinya. Penandaan paket ini menjadi dasar penting dalam penerapan *Queue Tree*, pengaturan *bandwidth*, monitoring trafik, pembatasan akses media sosial, serta pengaturan prioritas layanan jaringan. Dengan adanya pengelompokan paket data tersebut, administrator jaringan dapat lebih mudah mengendalikan penggunaan *internet* sehingga stabilitas, efisiensi, dan performa jaringan tetap terjaga meskipun digunakan secara bersamaan oleh banyak pengguna.

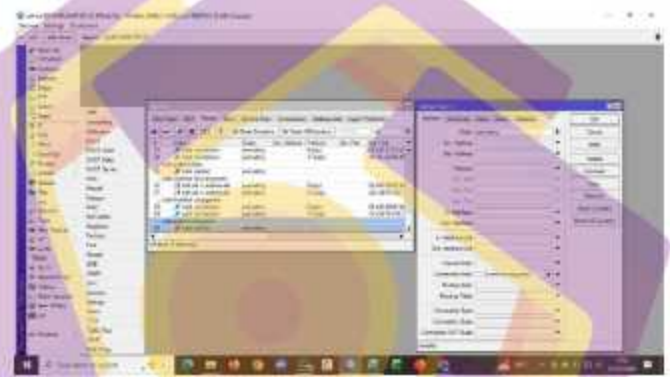
4.5.2.9 *Konfigurasi* Mark Packet *Firewall Mangle* Games *Online*

Konfigurasi mark packet pada *firewall mangle Mikrotik* berfungsi untuk memberikan identitas khusus pada paket data yang telah terdeteksi melalui proses mark connection. Pada implementasi ini, penandaan paket diterapkan pada trafik game *online* CrazyGames dan Roblox agar *Router* dapat mengenali setiap paket data yang berasal dari aktivitas permainan *online*. Dengan adanya proses tersebut, administrator jaringan dapat lebih mudah melakukan pengaturan *bandwidth*, pengendalian trafik game, monitoring penggunaan jaringan, serta penerapan *Quality Of Service (QoS)* secara lebih terarah dan efisien.

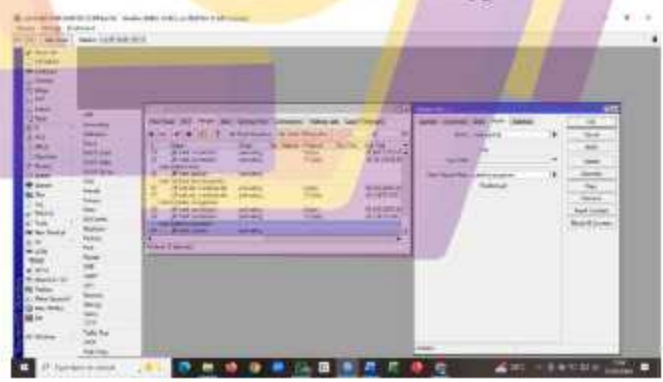
Proses *Konfigurasi* dilakukan melalui menu IP → *Firewall* → *Mangle* menggunakan chain pre*routing*. Penggunaan chain pre*routing* bertujuan agar paket data dapat dikenali sebelum masuk ke tahap *routing* maupun manajemen *bandwidth*. Sebelum melakukan mark packet, administrator terlebih dahulu membuat mark connection untuk masing-masing aplikasi game *online*. Pada tahap sebelumnya, koneksi CrazyGames telah ditandai dengan nama koneksi-crazygames, sedangkan koneksi Roblox ditandai dengan nama koneksi-roblox. Connection mark tersebut kemudian dijadikan acuan dalam proses penandaan paket data.

Tahap pertama dilakukan dengan membuat rule mark packet untuk aplikasi CrazyGames. Administrator menambahkan rule baru pada *firewall mangle* dengan memilih chain pre*routing*. Selanjutnya pada parameter

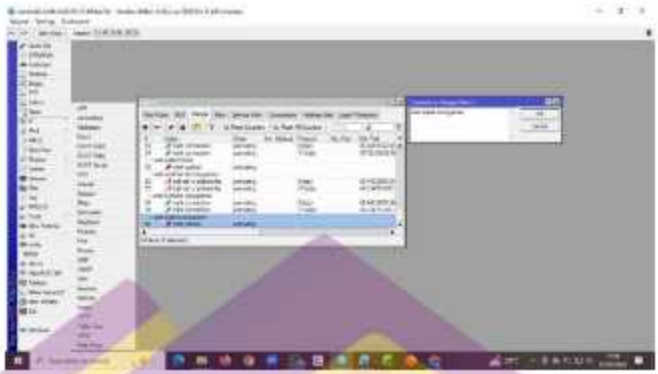
Connection Mark, dipilih koneksi-crazygames agar *Router* hanya memproses paket data yang berasal dari koneksi CrazyGames. Setelah itu, pada bagian Action, action diatur menjadi mark-packet, kemudian parameter New Packet Mark diisi dengan nama paket-crazygames. Opsi passthrough diatur menjadi no sehingga paket yang telah ditandai tidak akan diproses kembali oleh rule berikutnya. Dengan *Konfigurasi* tersebut, seluruh paket data dari CrazyGames akan dikenali dan diberi tanda secara otomatis oleh *Router Mikrotik*.



Gambar 4.5.2.9 Mark Packet Crazygames

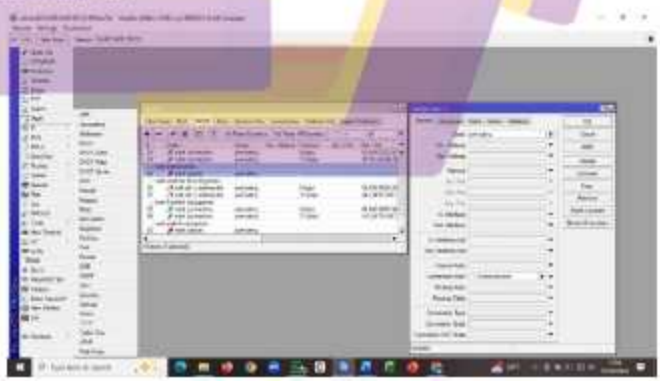


Gambar 4.5.2.9 Mark Packet Crazygames

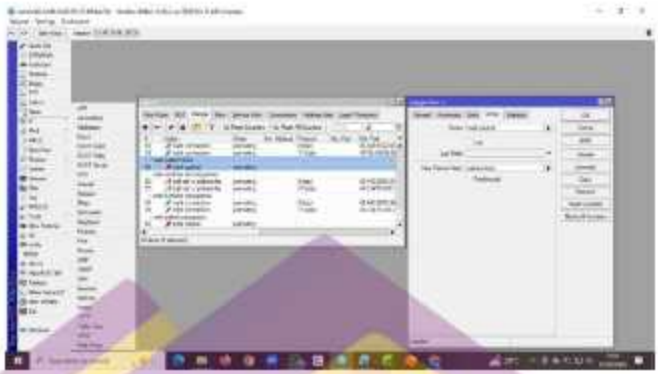


Gambar 4.5.2.9 Koment Mark Packet Crazygames

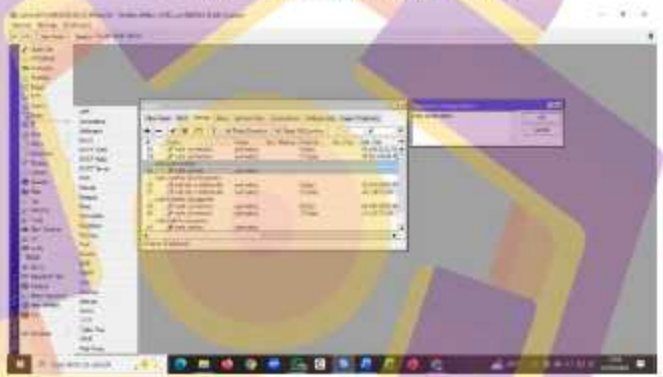
Langkah berikutnya diterapkan pada aplikasi Roblox. Administrator kembali membuat rule baru menggunakan chain pre*routing*, kemudian pada parameter Connection Mark diarahkan ke koneksi-roblox. Pengaturan ini bertujuan agar *Router* hanya menandai paket yang berasal dari koneksi Roblox. Selanjutnya pada tab Action, dipilih action mark-packet, kemudian parameter New Packet Mark diisi dengan nama paket-roblox. Opsi passthrough tetap diatur menjadi no agar paket yang sudah diberi tanda tidak diproses ulang oleh rule lainnya. Dengan *Konfigurasi* tersebut, seluruh paket data Roblox dapat dikenali dan dikelompokkan secara otomatis oleh *Router Mikrotik*.



Gambar 4.5.2.9 Mark Packet Roblox



Gambar 4.5.2.9 Mark Packet Roblox



Gambar 4.5.2.9 Koment Mark Packet Roblox

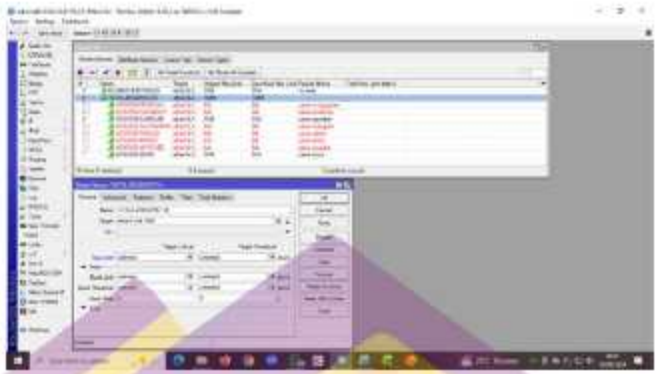
Melalui *Konfigurasi* mark packet tersebut, *Router Mikrotik* mampu membedakan paket data game *online* berdasarkan jenis aplikasinya. Penandaan paket ini menjadi bagian penting dalam penerapan *Queue Tree* dan manajemen *bandwidth* karena administrator dapat menentukan prioritas maupun pembatasan trafik secara lebih spesifik. Dengan adanya pengelompokan paket data CrazyGames dan Roblox, penggunaan jaringan *internet* dapat dikendalikan dengan lebih baik sehingga performa jaringan tetap stabil, penggunaan *bandwidth* lebih efisien, dan gangguan akibat trafik game *online* yang berlebihan dapat diminimalkan.

4.5.3 *Konfigurasi Queues Mikrotik*

Konfigurasi Queues pada *Mikrotik* merupakan salah satu tahapan penting dalam penerapan *Quality Of Service (QoS)* untuk mengatur dan mengendalikan penggunaan *bandwidth* pada jaringan komputer. Fitur queue digunakan untuk membatasi, membagi, serta memprioritaskan *bandwidth* agar penggunaan jaringan menjadi lebih stabil dan merata. Pada penelitian ini, *Konfigurasi* queue diterapkan untuk mengoptimalkan performa jaringan di laboratorium SMK sehingga seluruh pengguna dapat memperoleh akses *internet* yang lebih baik tanpa terjadi perebutan *bandwidth* secara berlebihan. Dengan adanya pengaturan *bandwidth* tersebut, aktivitas jaringan seperti pembelajaran daring, *browsing*, maupun penggunaan aplikasi lainnya dapat berjalan lebih optimal dan terkontrol.

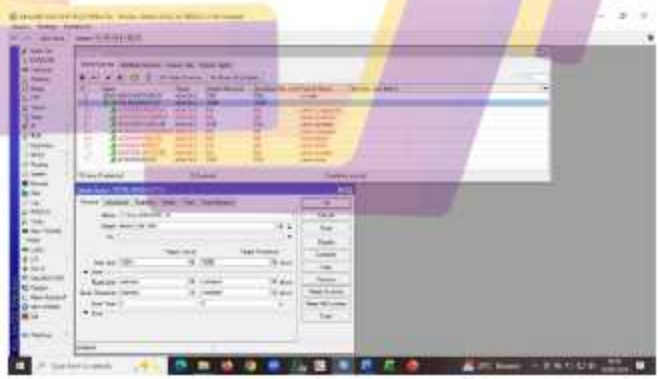
Konfigurasi bandwidth dilakukan menggunakan metode Simple Queue karena lebih mudah diterapkan dan sesuai untuk pengelolaan *bandwidth* pada jaringan laboratorium sekolah. Langkah awal *Konfigurasi* dilakukan dengan membuka aplikasi *Winbox* kemudian login ke *Router Mikrotik* menggunakan akun administrator. Setelah berhasil masuk ke sistem *Router*, administrator memilih menu *Queues* kemudian masuk ke submenu Simple Queue. Pada tahap ini dibuat sebuah queue utama yang digunakan untuk mengatur total *bandwidth* jaringan laboratorium SMK.

Proses *Konfigurasi* dimulai dengan menekan tombol Add (+) untuk menambahkan queue baru. Selanjutnya pada kolom Name diisi dengan nama TOTAL-*BANDWIDTH* sebagai identitas queue utama. Pada bagian Target, dipilih interface *Ether3*-LAB SMK yang merupakan jalur jaringan menuju laboratorium komputer SMK. Penentuan target interface bertujuan agar pengaturan *bandwidth* hanya diterapkan pada jaringan laboratorium sehingga seluruh perangkat yang terhubung melalui interface tersebut akan mengikuti aturan *bandwidth* yang telah ditentukan.



Gambar 4.5.3 Queue Total *Bandwidth*

Tahap berikutnya adalah menentukan batas maksimum *bandwidth* pada bagian Max Limit. Pada *Konfigurasi* ini *bandwidth* upload dan download diatur sebesar 100 Mbps atau dituliskan 100M/100M. Pengaturan tersebut berarti total *bandwidth* maksimal yang dapat digunakan oleh seluruh pengguna pada jaringan laboratorium adalah 100 Mbps untuk upload dan 100 Mbps untuk download. Dengan adanya pembatasan *bandwidth* tersebut, penggunaan *internet* menjadi lebih stabil dan terkontrol sehingga tidak terjadi penggunaan *bandwidth* secara berlebihan oleh pengguna tertentu yang dapat menyebabkan koneksi jaringan menjadi lambat.



Gambar 4.5.3 Queue Total *Bandwidth*

Selain menentukan batas *bandwidth*, *Konfigurasi* Simple Queue juga berfungsi untuk membantu administrator jaringan dalam memonitor

penggunaan *bandwidth* secara *real-time*. *Mikrotik* akan menampilkan informasi trafik upload dan download dari interface yang telah di*Konfigurasi* sehingga administrator dapat mengetahui kondisi penggunaan jaringan secara langsung. Hal ini sangat membantu dalam proses pengawasan jaringan dan analisis performa *QoS* pada penelitian yang dilakukan.

4.5.3.1 *Konfigurasi* Simple *Queues* Pembelajaran Daring

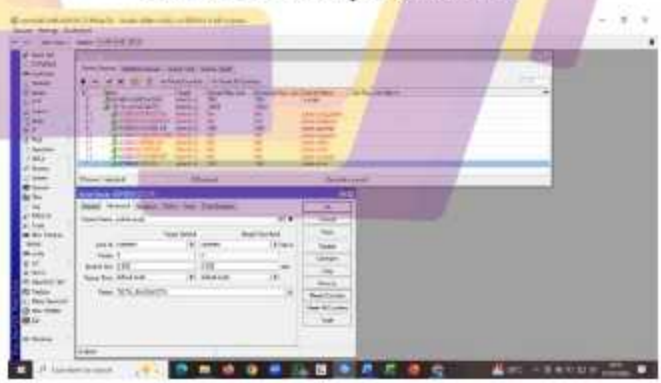
Konfigurasi Simple *Queues* pada *Mikrotik* digunakan untuk mengatur dan membatasi penggunaan *bandwidth* pada trafik pembelajaran daring agar koneksi jaringan menjadi lebih stabil dan terkontrol. Pada implementasi ini, aplikasi yang diprioritaskan adalah Zoom dan *Gamelab* karena keduanya digunakan sebagai media pembelajaran *online* di laboratorium sekolah. Pengaturan *bandwidth* dilakukan pada interface *Ether3*-LAB SMK dengan tujuan agar aktivitas pembelajaran daring memperoleh kualitas layanan jaringan (*Quality Of Service/QoS*) yang lebih baik.

Dalam *Konfigurasi* ini, masing-masing layanan diberikan batas *bandwidth* maksimum sebesar 25 Mbps upload dan 25 Mbps download. Selain itu, digunakan fitur packet mark yang sebelumnya telah dibuat pada menu *Firewall Mangle*. Penandaan paket dilakukan agar *Mikrotik* dapat mengenali trafik berdasarkan jenis aplikasi, sehingga proses manajemen *bandwidth* menjadi lebih spesifik dan efektif. Paket Zoom menggunakan packet mark paket-zoom, sedangkan trafik *Gamelab* menggunakan packet mark paket-*gamelab*.

Langkah pertama dilakukan dengan membuka menu *Queues* → Simple *Queues* pada aplikasi *Winbox Mikrotik*. Selanjutnya administrator memilih tombol Add (+) untuk membuat *Konfigurasi* queue baru khusus aplikasi Zoom. Pada tab General, kolom Name diisi dengan nama KONEKSI-ZOOM sebagai identitas queue. Kemudian pada bagian Target dipilih interface *Ether3*-LAB SMK yang menjadi jalur jaringan laboratorium sekolah. Setelah itu, pada kolom Max Limit diisikan nilai 25M/25M yang menunjukkan batas maksimum *bandwidth* upload dan download sebesar 25 Mbps.

Setelah pengaturan umum selesai dilakukan, *Konfigurasi* dilanjutkan pada tab Advanced. Pada bagian Packet Marks dipilih paket-zoom. Pengaturan ini bertujuan agar queue hanya bekerja pada trafik Zoom yang telah ditandai sebelumnya melalui *Konfigurasi Firewall Mangle*. Dengan adanya packet mark tersebut, trafik video *conference* Zoom dapat diprioritaskan sehingga proses pembelajaran daring menjadi lebih lancar, stabil, dan minim gangguan koneksi. Setelah seluruh pengaturan selesai, administrator menekan tombol Apply dan OK untuk menyimpan *Konfigurasi*.

Gambar 4.5.3.1 Simple *Queues* Zoom

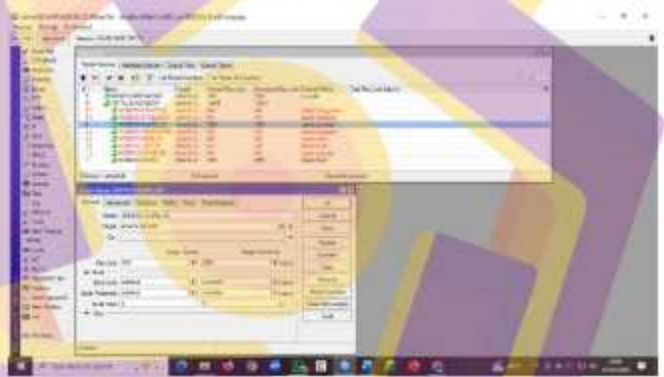


Gambar 4.5.3.1 Simple *Queues* Zoom

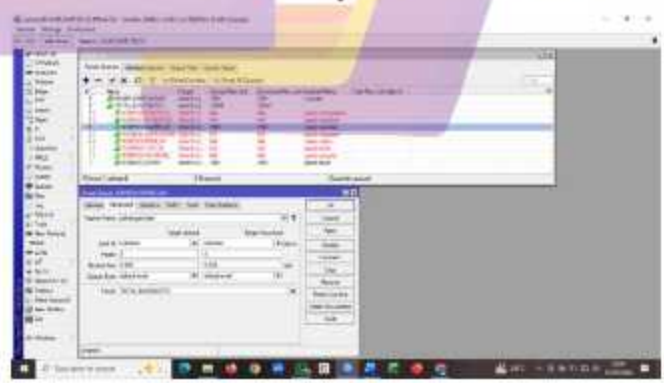
Langkah berikutnya dilakukan untuk aplikasi *Gamelab* dengan prosedur yang hampir sama. Administrator kembali memilih tombol Add

(+) pada menu Simple *Queues*. Pada tab General, kolom Name diisi dengan nama KONEKSI-*GAMELAB*. Selanjutnya pada bagian Target pilih interface *Ether3*-LAB SMK, kemudian pada kolom Max Limit diatur sebesar 25M/25M untuk upload dan download.

Setelah itu *Konfigurasi* dilanjutkan ke tab Advanced. Bagian Packet Marks pilih tanda paket paket-*gamelab* yang telah dibuat sebelumnya di menu *Firewall Mangle*. Penggunaan packet mark ini memungkinkan *Mikrotik* untuk mengenali trafik *Gamelab* secara khusus sehingga *bandwidth* dapat dikelola sesuai kebutuhan aplikasi tersebut. Setelah *Konfigurasi* selesai dilakukan, administrator menekan tombol Apply dan OK agar pengaturan tersimpan dan dapat dijalankan oleh sistem *Mikrotik*.



Gambar 4.5.3.1 Simple *Queues Gamelab*



Gambar 4.5.3.1 Simple *Queues Gamelab*

Penerapan *Konfigurasi* Simple *Queues* pada Zoom dan *Gamelab* memberikan manfaat dalam menjaga kestabilan jaringan pembelajaran daring. *Bandwidth* menjadi lebih terkontrol, trafik pembelajaran memperoleh prioritas layanan, serta kualitas koneksi menjadi lebih optimal. Dengan demikian, kegiatan belajar mengajar berbasis *online* di laboratorium sekolah dapat berlangsung dengan lebih efektif dan efisien.

4.5.3.2 *Konfigurasi* Simple *Queues* Media Sosial

Konfigurasi Simple *Queues* pada *Mikrotik* digunakan untuk melakukan pembatasan *bandwidth* terhadap akses media sosial pada jaringan laboratorium sekolah. Pembatasan ini bertujuan agar penggunaan *internet* lebih terfokus pada kegiatan pembelajaran dan aktivitas akademik, sehingga kualitas layanan jaringan (*Quality Of Service/QoS*) tetap stabil selama proses belajar mengajar berlangsung. Dalam implementasi ini, aplikasi media sosial yang dibatasi meliputi YouTube, Instagram, Facebook, dan TikTok. Seluruh pengaturan diterapkan pada interface *Ether3*-LAB SMK yang digunakan sebagai jalur distribusi jaringan laboratorium sekolah.

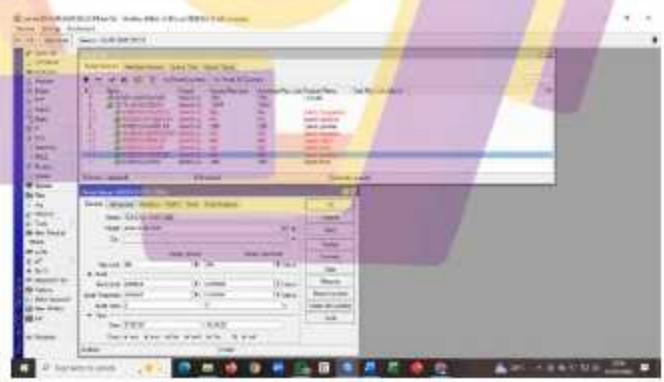
Setiap aplikasi media sosial diberikan batas *bandwidth* maksimum sebesar 64 kbps upload dan 64 kbps download. Pembatasan *bandwidth* tersebut dilakukan agar akses media sosial tidak menghabiskan kapasitas *internet* sekolah yang seharusnya diprioritaskan untuk kebutuhan pembelajaran daring dan akses layanan pendidikan lainnya. Selain itu, *Konfigurasi* pembatasan hanya diaktifkan pada jam aktif belajar sekolah, yaitu mulai pukul 07:00:00 sampai 14:00:00, serta berlaku pada hari Sabtu hingga Kamis. Pengaturan waktu dan hari dilakukan melalui fitur Time dan Days pada menu Simple *Queues Mikrotik*.

Konfigurasi juga memanfaatkan fitur packet mark yang sebelumnya telah dibuat melalui menu *Firewall Mangle*. Penandaan paket dilakukan agar *Mikrotik* dapat mengenali trafik berdasarkan jenis aplikasi media sosial sehingga pembatasan *bandwidth* dapat diterapkan secara lebih spesifik dan efektif. Paket YouTube menggunakan packet mark paket-youtube,

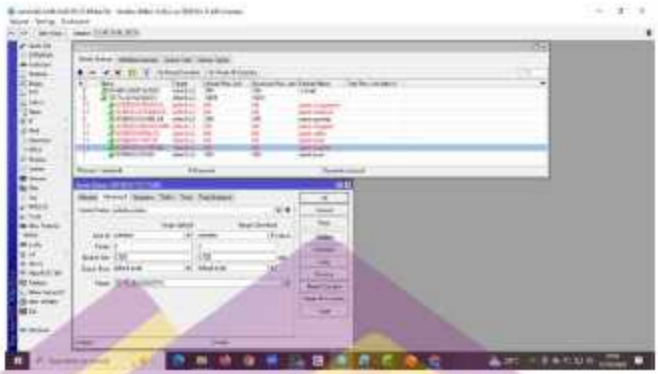
Instagram menggunakan paket-instagram, Facebook menggunakan paket-facebook, dan TikTok menggunakan paket-tiktok.

Konfigurasi pertama dilakukan untuk aplikasi YouTube. Administrator membuka menu *Queues* → Simple *Queues* pada aplikasi *Winbox Mikrotik*, kemudian memilih tombol Add (+) untuk membuat queue baru. Pada tab General, kolom Name diisi dengan nama KONEKSI-YOUTUBE sebagai identitas queue. Selanjutnya pada bagian Target dipilih interface *Ether3*-LAB SMK. Pada kolom Max Limit diisikan nilai 64k/64k yang menunjukkan batas maksimum upload dan download sebesar 64 kbps.

Setelah pengaturan *bandwidth* selesai dilakukan, administrator mengaktifkan bagian Time dengan rentang waktu 07:00:00–14:00:00. Selanjutnya pada bagian Days, dipilih hari Sabtu sampai Kamis agar pembatasan hanya berlaku pada hari aktif sekolah. Setelah itu *Konfigurasi* dilanjutkan pada tab Advanced, kemudian pada bagian Packet Marks dipilih paket-youtube agar queue hanya bekerja pada trafik YouTube yang telah ditandai sebelumnya melalui *Konfigurasi Firewall Mangle*. Setelah seluruh *Konfigurasi* selesai, pengaturan disimpan dengan menekan tombol Apply dan OK..

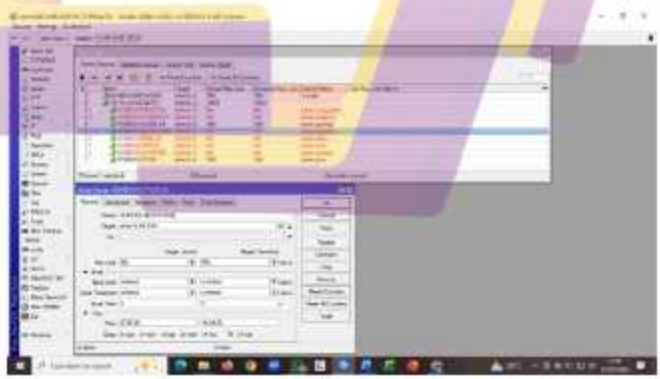


Gambar 4.5.3.2 Simple *Queues* Youtube

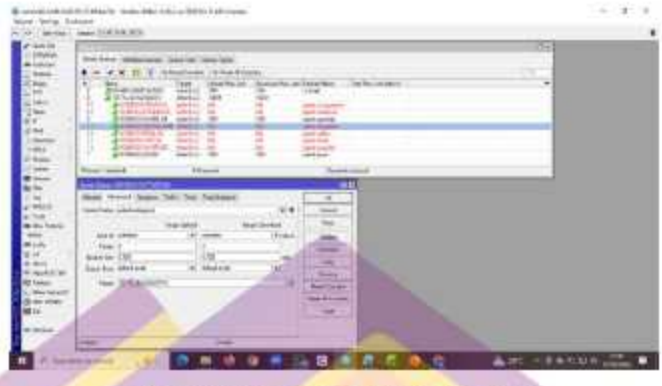


Gambar 4.5.3.2 Simple *Queues* Youtube

Langkah berikutnya dilakukan untuk aplikasi Instagram. Administrator kembali memilih tombol Add (+) pada menu Simple *Queues*, kemudian pada kolom Name diisi dengan nama KONEKSI-INSTAGRAM. Pada bagian Target dipilih *Ether3*-LAB SMK, sedangkan nilai Max Limit diatur sebesar 64k/64k. Selanjutnya pada bagian Time diatur mulai pukul 07:00:00 hingga 14:00:00, kemudian pada bagian Days dipilih hari Sabtu–Kamis. Setelah itu pada tab Advanced, bagian Packet Marks dipilih paket-instagram. *Konfigurasi* ini bertujuan untuk membatasi penggunaan Instagram selama jam aktif pembelajaran berlangsung.

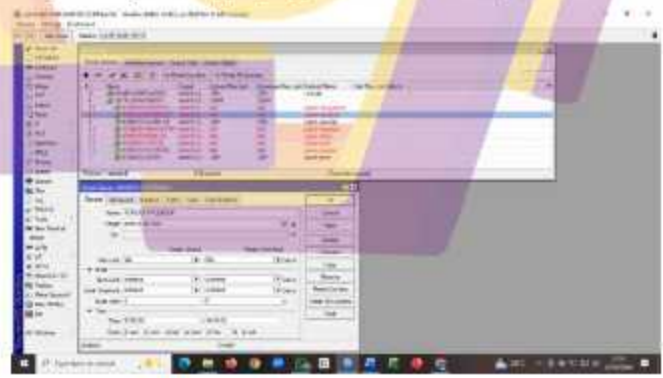


Gambar 4.5.3.2 Simple *Queues* Instagram

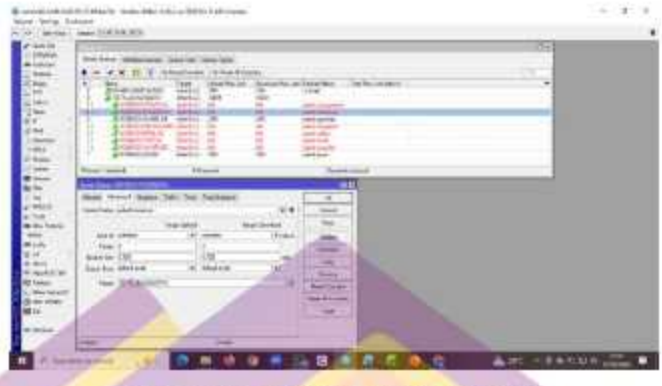


Gambar 4.5.3.2 Simple *Queues* Instagram

Konfigurasi selanjutnya dilakukan untuk aplikasi Facebook. Administrator membuat queue baru dengan nama KONEKSI-FACEBOOK, kemudian memilih interface *Ether3*-LAB SMK pada bagian Target. Nilai Max Limit diatur sebesar 64k/64k, kemudian pada bagian Time diaktifkan mulai pukul 07:00:00 sampai 14:00:00 dan pada bagian Days dipilih hari Sabtu–Kamis. Setelah itu pada tab Advanced, bagian Packet Marks dipilih paket-facebook. Dengan *Konfigurasi* tersebut, trafik Facebook akan dibatasi selama jam belajar sehingga penggunaan *bandwidth* dapat lebih terkendali.

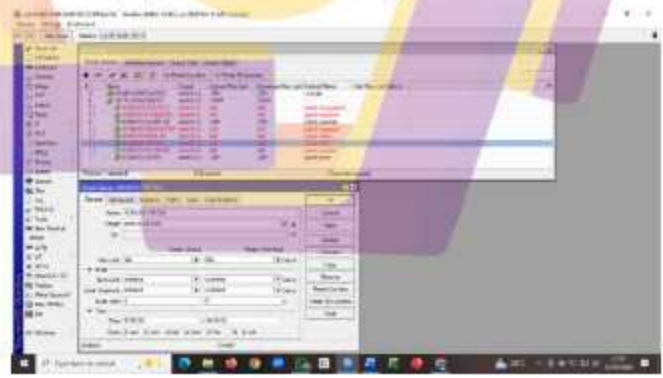


Gambar 4.5.3.2 Simple *Queues* Facebook

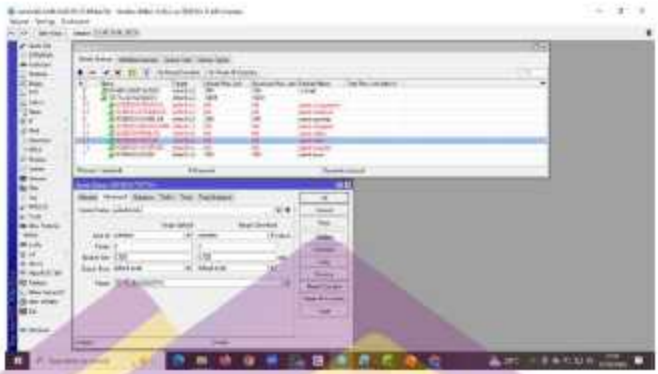


Gambar 4.5.3.2 Simple *Queues* Facebook

Tahap terakhir dilakukan untuk aplikasi TikTok. Administrator kembali membuat queue baru dengan nama KONEKSI-TIKTOK pada menu Simple *Queues*. Selanjutnya pada bagian Target dipilih *Ether3*-LAB SMK, kemudian nilai Max Limit diatur sebesar 64k/64k. Pada bagian Time, pembatasan diaktifkan pada rentang waktu 07:00:00–14:00:00, sedangkan pada bagian Days dipilih hari Sabtu–Kamis. Setelah itu pada tab Advanced, bagian Packet Marks dipilih paket-tiktok agar queue hanya bekerja pada trafik TikTok yang telah ditandai sebelumnya.



Gambar 4.5.3.2 Simple *Queues* Tiktok



Gambar 4.5.3.2 Simple *Queues* Tiktok

Penerapan *Konfigurasi* Simple *Queues* pada media sosial memberikan manfaat dalam menjaga kestabilan jaringan sekolah dan meningkatkan efektivitas penggunaan *internet*. Pembatasan *bandwidth* pada jam dan hari aktif belajar membuat akses media sosial menjadi lebih terkendali sehingga *bandwidth internet* dapat diprioritaskan untuk kegiatan pembelajaran daring, akses materi pendidikan, dan layanan akademik lainnya. Dengan demikian, manajemen *bandwidth* jaringan laboratorium sekolah dapat berjalan lebih optimal, efisien, dan sesuai dengan kebutuhan proses belajar mengajar.

4.5.3.3 *Konfigurasi* Simple *Queues* Games *Online*

Konfigurasi Simple *Queues* pada *Mikrotik* digunakan untuk melakukan pembatasan *bandwidth* terhadap akses games *online* pada jaringan laboratorium sekolah. Pembatasan ini bertujuan untuk mengurangi penggunaan *internet* yang tidak berkaitan dengan kegiatan pembelajaran sehingga kualitas layanan jaringan (*Quality Of Service*/*QoS*) tetap stabil dan *bandwidth* dapat diprioritaskan untuk aktivitas akademik. Pada implementasi ini, games *online* yang dibatasi meliputi CrazyGames dan Roblox. Seluruh pengaturan diterapkan pada interface *Ether3*-LAB SMK yang menjadi jalur distribusi jaringan laboratorium sekolah.

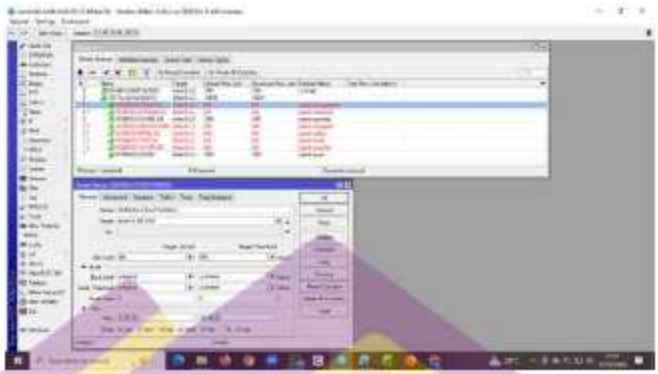
Masing-masing games *online* diberikan batas *bandwidth* maksimum sebesar 64 kbps upload dan 64 kbps download. Nilai *bandwidth* tersebut

sengaja dibuat kecil agar akses games *online* tetap dapat berjalan secara terbatas, namun tidak mengganggu penggunaan jaringan utama sekolah. Selain itu, pembatasan *bandwidth* hanya diaktifkan pada jam aktif belajar sekolah, yaitu mulai pukul 07:00:00 sampai 14:00:00, serta berlaku pada hari Sabtu hingga Kamis. Pengaturan waktu dan hari dilakukan melalui fitur Time dan Days pada menu Simple *Queues Mikrotik*.

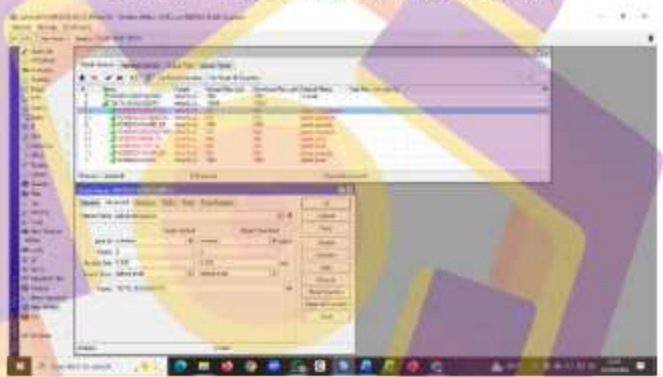
Konfigurasi ini juga menggunakan fitur packet mark yang sebelumnya telah dibuat pada menu *Firewall Mangle*. Penandaan paket dilakukan agar *Mikrotik* dapat mengenali trafik berdasarkan jenis games *online* sehingga proses pembatasan *bandwidth* dapat diterapkan secara lebih spesifik dan efektif. Paket CrazyGames menggunakan packet mark paket-crazygames, sedangkan Roblox menggunakan paket-roblox.

Konfigurasi pertama dilakukan untuk games *online* CrazyGames. Administrator membuka menu *Queues* → Simple *Queues* pada aplikasi *Winbox Mikrotik*, kemudian memilih tombol Add (+) untuk membuat queue baru. Pada tab General, kolom Name diisi dengan nama KONEKSI-CRAZYGAMES sebagai identitas queue. Selanjutnya pada bagian Target dipilih interface *Ether3*-LAB SMK. Pada kolom Max Limit diisikan nilai 64k/64k yang menunjukkan batas maksimum upload dan download sebesar 64 kbps.

Setelah pengaturan *bandwidth* selesai dilakukan, administrator mengaktifkan bagian Time dengan rentang waktu 07:00:00–14:00:00. Selanjutnya pada bagian Days, dipilih hari Sabtu sampai Kamis agar pembatasan hanya berlaku pada hari aktif sekolah. Setelah itu *Konfigurasi* dilanjutkan pada tab Advanced, kemudian pada bagian Packet Marks dipilih paket-crazygames agar queue hanya bekerja pada trafik CrazyGames yang telah ditandai sebelumnya melalui *Konfigurasi Firewall Mangle*. Setelah seluruh *Konfigurasi* selesai, pengaturan disimpan dengan menekan tombol Apply dan OK.

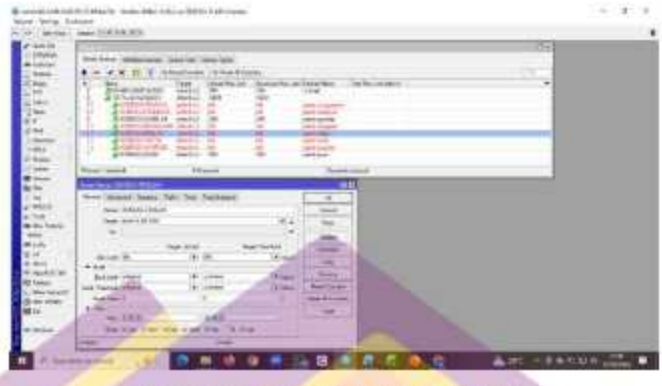


Gambar 4.5.3.3 Simple *Queues* Crazygames

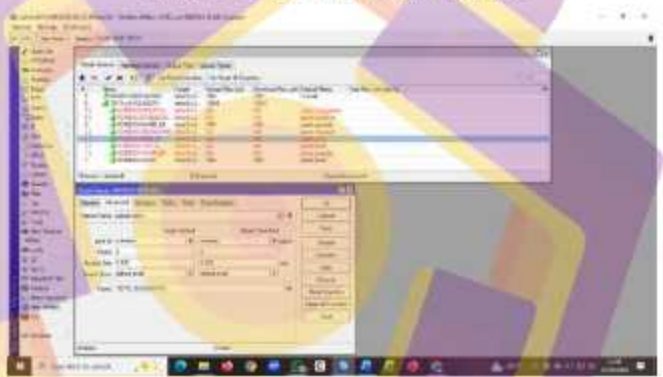


Gambar 4.5.3.3 Simple *Queues* Crazygames

Langkah berikutnya dilakukan untuk games *online* Roblox. Administrator kembali memilih tombol Add (+) pada menu Simple *Queues*, kemudian pada kolom Name diisi dengan nama KONEKSI-ROBLOX. Pada bagian Target dipilih *Ether3*-LAB SMK, sedangkan nilai Max Limit diatur sebesar 64k/64k. Selanjutnya pada bagian Time diatur mulai pukul 07:00:00 hingga 14:00:00, kemudian pada bagian Days dipilih hari Sabtu–Kamis. Setelah itu pada tab Advanced, bagian Packet Marks dipilih paket-roblox. *Konfigurasi* ini bertujuan untuk membatasi penggunaan Roblox selama jam aktif pembelajaran berlangsung.



Gambar 4.5.3.3 Simple *Queues* Roblox



Gambar 4.5.3.3 Simple *Queues* Roblox

Penerapan *Konfigurasi* Simple *Queues* pada games *online* memberikan manfaat dalam menjaga kestabilan jaringan sekolah dan meningkatkan efektivitas penggunaan *bandwidth internet*. Pembatasan *bandwidth* pada CrazyGames dan Roblox membuat penggunaan jaringan menjadi lebih terkendali sehingga kapasitas *internet* dapat diprioritaskan untuk kegiatan pembelajaran daring, akses materi pendidikan, dan layanan akademik lainnya. Dengan demikian, manajemen *bandwidth* pada jaringan laboratorium sekolah dapat berjalan lebih optimal, efisien, dan sesuai dengan kebutuhan proses belajar mengajar.

4.6 Hasil Pengujian

Pengujian dilakukan untuk mengetahui pengaruh penerapan *Packet Filtering* dan *Quality Of Service (QoS)* terhadap kualitas jaringan *Mikrotik*. Parameter yang diuji meliputi *Throughput, Delay*, *Jitter*, dan *Packet Loss*. Pengujian dilakukan dalam tiga kondisi, yaitu kondisi awal tanpa *Konfigurasi* (*Baseline*), kondisi setelah penerapan filtering, dan kondisi setelah penerapan *QoS* + Filtering. Proses pengujian dilakukan menggunakan perangkat komputer client, *Router Mikrotik*, koneksi *internet*, serta aplikasi pengujian jaringan seperti *Wireshark*, Ping, dan Speedtest.

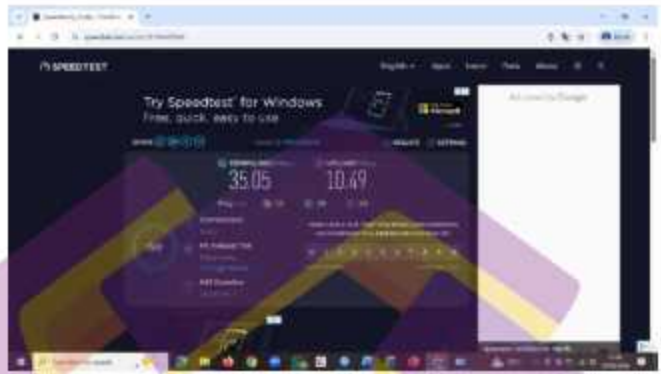
Langkah pertama dalam pengujian adalah menyiapkan topologi jaringan yang terdiri dari koneksi ISP menuju *Router Mikrotik*, kemudian diteruskan ke *switch* atau hub dan perangkat client. Setelah jaringan terhubung, administrator memastikan seluruh perangkat dapat mengakses *internet* dengan normal. Selanjutnya dilakukan pengujian awal atau *Baseline* tanpa menerapkan *Konfigurasi firewall mangle* maupun *QoS*. Pada tahap ini beberapa client melakukan aktivitas jaringan secara bersamaan seperti membuka YouTube, TikTok, Instagram, Zoom, dan game *online* untuk mensimulasikan kondisi trafik jaringan yang padat. Kemudian administrator melakukan pengukuran *Throughput* menggunakan Speedtest atau torch *Mikrotik*, melakukan pengujian *Delay* menggunakan perintah ping ke server *internet*, mengukur *Jitter* menggunakan aplikasi monitoring jaringan, serta melihat *Packet Loss* berdasarkan hasil ping dan capture paket pada *Wireshark*. Hasil pengujian dicatat sebagai data kondisi awal jaringan.

Gambar 4.6 Hasil Pengujian Menggunakan Speedtest

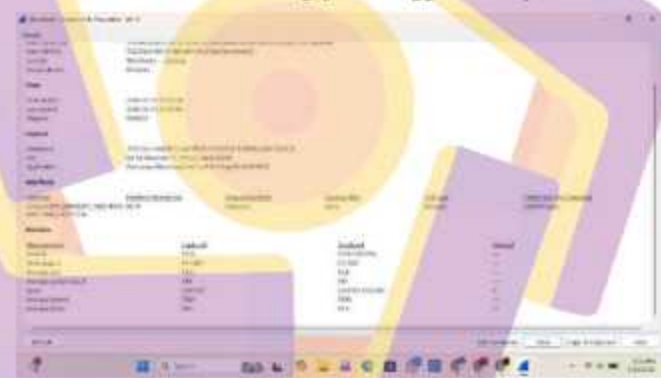
Gambar 4.6 Hasil Pengujian Menggunakan *Wireshark*

Langkah kedua adalah melakukan pengujian setelah penerapan *firewall* filtering. Pada tahap ini administrator meng*Konfigurasi firewall mangle* pada *Mikrotik* untuk menandai trafik aplikasi tertentu berdasarkan *Protocol TCP, UDP*, dan *Destination Port*. Trafik aplikasi pembelajaran, media sosial, dan game *online* dimasukkan ke dalam *Address List* yang berbeda menggunakan action add-dst-to-address-list. Setelah *Konfigurasi* selesai, pengujian dilakukan kembali dengan skenario penggunaan jaringan yang sama seperti tahap *Baseline*. Selanjutnya administrator kembali mengukur *Throughput, Delay*, *Jitter*, dan *Packet Loss* untuk mengetahui perubahan performa jaringan setelah diterapkan filtering. Hasil pengujian kemudian dibandingkan dengan

kondisi sebelumnya untuk melihat pengaruh filtering terhadap kualitas jaringan.



Gambar 4.6 Hasil Pengujian Menggunakan Speedtest

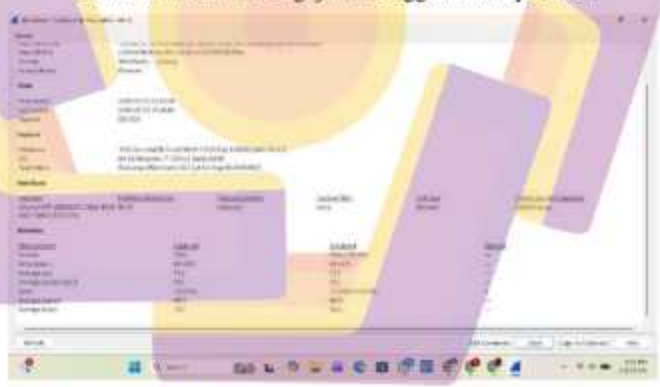


Gambar 4.6 Hasil Pengujian Menggunakan *Wireshark*

Langkah ketiga adalah melakukan pengujian setelah penerapan *QoS* + Filtering. Pada tahap ini administrator menambahkan *Konfigurasi Queue Tree* atau Simple Queue pada *Mikrotik* untuk mengatur prioritas *bandwidth* berdasarkan packet *marking* yang telah dibuat sebelumnya. Trafik pembelajaran daring seperti Zoom dan *Gamelab* diberikan prioritas *bandwidth* lebih tinggi dibandingkan trafik media sosial dan game *online*. Setelah *Konfigurasi QoS* diterapkan, dilakukan pengujian kembali menggunakan aktivitas jaringan yang sama agar hasil pengujian tetap konsisten.

Administrator kemudian mengukur *Throughput, Delay*, *Jitter*, dan *Packet Loss* menggunakan metode yang sama seperti pengujian sebelumnya. Hasil pengujian menunjukkan bahwa penerapan *QoS* dan filtering mampu meningkatkan *Throughput* jaringan serta menurunkan *Delay*, *Jitter*, dan *Packet Loss* sehingga kualitas layanan jaringan menjadi lebih stabil dan optimal.

Gambar 4.6 Hasil Pengujian Menggunakan Speedtest



Gambar 4.6 Hasil Pengujian Menggunakan *Wireshark*

Berdasarkan hasil pengujian yang telah dilakukan, diperoleh perbandingan parameter jaringan sebagai berikut:

Tabel 4.6 Perbandingan Parameter Jaringan

No	Parameter	*Baseline*	Filtering	*QoS* + Filtering
1.	*Throughput*	Rendah	Sedang	Tinggi
2.	*Delay*	Tinggi	Sedang	Rendah
3.	*Jitter*	Tinggi	Sedang	Rendah
4.	*Packet Loss*	Tinggi	Sedang	Rendah

Hasil tersebut menunjukkan bahwa penerapan *firewall* filtering dan *QoS* pada *Mikrotik* memberikan pengaruh positif terhadap peningkatan performa dan kualitas jaringan *internet*.

4.7 Data Hasil Pengukuran QoS

Berikut adalah data kuantitatif hasil pengukuran pada tiga skenario pengujian menggunakan Wireshark dan Speedtest:

Tabel 4.7 Data Hasil Pengukuran QoS

No	Parameter	Baseline	Filtering	QoS+Filtering	Satuan
1.	*Throughput*	25.92	35.05	38.35	Mbps
2.	*Delay*	38	35	34	ms
3.	*Jitter*	37	30	28	ms
4.	*Packet Loss*	2.5	1.2	0.5	%

4.8 Analisis Peningkatan Kuantitatif (Perhitungan Matematis)

Analisis peningkatan kinerja dihitung menggunakan rumus persentase peningkatan/penurunan relatif terhadap baseline. Formula yang digunakan adalah:

a. *% Peningkatan = ((Nilai_Baru - Nilai_Baseline) / Nilai_Baseline) × 100%*

b. *% Penurunan = ((Nilai_Baseline - Nilai_Baru) / Nilai_Baseline) × 100%*

4.8.1 Analisis *Throughput*

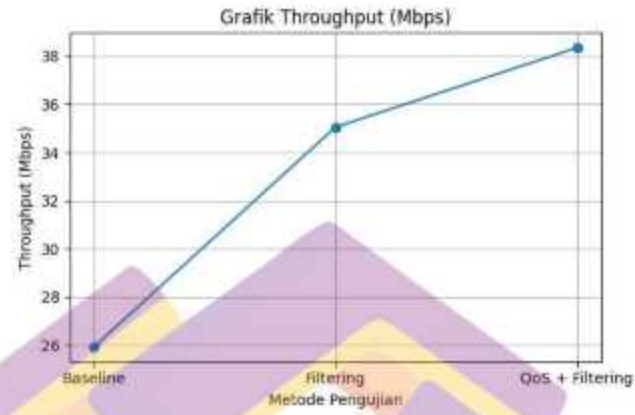
Throughput merepresentasikan kapasitas transfer data efektif. Peningkatan *Throughput* mengindikasikan berkurangnya congestion pada antrian (buffer) router akibat mitigasi *Bufferbloat*.

Tabel 4.8.1 Analisis *Throughput*

No	Perbandingan	Nilai Awal (Mbps)	Nilai Akhir (Mbps)	% Peningkatan
1.	Baseline → Filtering	25.92	35.05	+35.2%
2.	Baseline → QoS+Filtering	25.92	38.35	+47.9%
3.	Filtering → QoS+Filtering	35.05	38.35	+9.4%

Perhitungan detail: Peningkatan *Throughput* Baseline→Filtering = ((35.05 - 25.92) / 25.92) × 100% = (9.13 / 25.92) × 100% = 35.2%. Peningkatan Baseline→QoS+Filtering = ((38.35 - 25.92) / 25.92) × 100% = (12.43 / 25.92) × 100% = 47.9%.

Peningkatan *Throughput* sebesar 47.9% dari baseline ke QoS+Filtering merupakan bukti langsung berkurangnya dampak *Bufferbloat*: ketika buffer tidak lagi terisi oleh trafik non-prioritas yang berkompetisi, bandwidth efektif yang tersedia untuk trafik produktif meningkat signifikan. Hasil ini lebih tinggi dari temuan Gumeular & Akbi (2025) yang melaporkan peningkatan *Throughput* sekitar 30-40% dengan metode PCQ+FQ_CoDel, mengkonfirmasi efektivitas pendekatan yang digunakan.



Gambar 4.8.1 Grafik *Throughput*

4.8.2 Analisis *Delay*

Delay (latensi) merupakan parameter yang paling sensitif terhadap *Bufferbloat*. Buffer yang terisi penuh langsung menyebabkan lonjakan *Delay*.

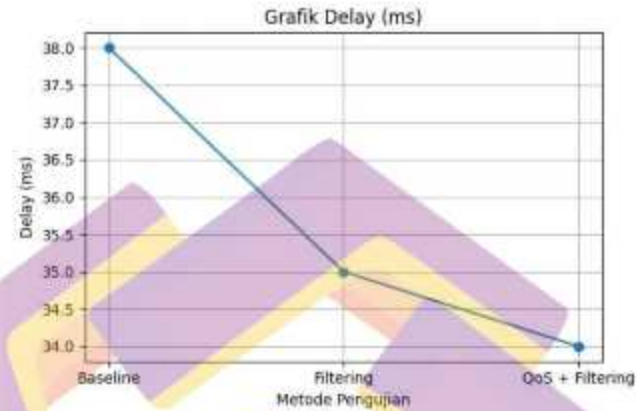
Tabel 4.8.2 Analisis *Delay*

No	Perbandingan	Nilai Awal (ms)	Nilai Akhir (ms)	% Penurunan
1.	Baseline → Filtering	38	35	-7.9%
2.	Baseline → QoS+Filtering	38	34	-10.5%
3.	Filtering → QoS+Filtering	35	34	-2.9%

Perhitungan detail: Penurunan *Delay* Baseline→QoS+Filtering = ((38 - 34) / 38) × 100% = (4 / 38) × 100% = 10.5%. Meskipun nilai *Delay* absolut sudah dalam kategori 'sangat baik' (< 150 ms) pada kondisi baseline, penurunan 10.5% tetap signifikan untuk aplikasi real-time seperti video *conference* di mana setiap milidetik memengaruhi kualitas pengalaman.

Perbandingan dengan Barczyk & Chydzinski (2022) yang melaporkan penurunan *Delay* 40% dengan AQM di jaringan universitas menunjukkan bahwa implementasi AQM algoritmik (CoDel/CAKE) berpotensi memberikan penurunan *Delay* yang lebih besar. Namun, penurunan 10.5% yang dicapai dalam penelitian ini relevan untuk konteks infrastruktur

Mikrotik yang umum digunakan di sekolah Indonesia tanpa perlu upgrade hardware.



Gambar 4.8.2 Grafik *Delay*

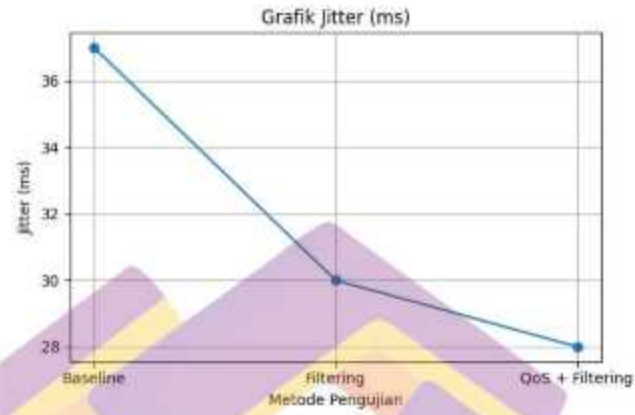
4.8.3 Analisis *Jitter*

Jitter merupakan variasi waktu kedatangan paket data pada jaringan. Nilai *Jitter* yang tinggi dapat menyebabkan koneksi tidak stabil, terutama pada layanan *streaming* dan komunikasi suara.

Tabel 4.8.3 Analisis *Jitter*

No	Perbandingan	Nilai Awal (ms)	Nilai Akhir (ms)	% Penurunan
1.	Baseline → Filtering	37	30	-18.9%
2.	Baseline → QoS+Filtering	37	28	-24.3%
3.	Filtering → QoS+Filtering	30	28	-6.7%

Perhitungan detail: Penurunan *Jitter* Baseline→QoS+Filtering = ((37 - 28) / 37) × 100% = (9 / 37) × 100% = 24.3%. Penurunan *Jitter* sebesar 24.3% sangat bermakna dalam konteks komunikasi real-time. Pada kondisi baseline (37 ms), *Jitter* sudah mendekati ambang batas 'sedang' menurut standar TIPHON (20-50 ms). Dengan mitigasi QoS+Filtering, nilai 28 ms masih dalam kategori 'baik' namun lebih stabil karena *Queue Tree* mengurangi variabilitas antrian.



Gambar 4.8.3 Grafik *Jitter*

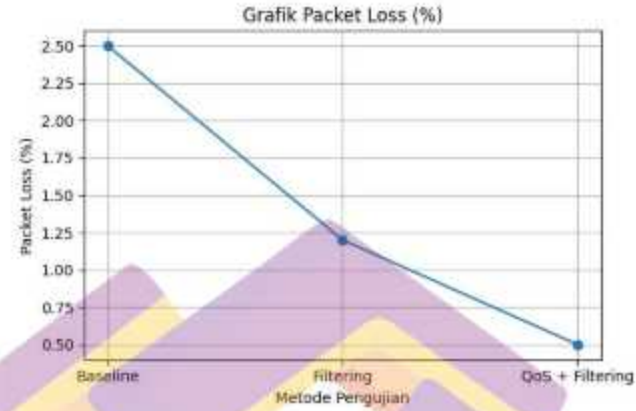
4.8.4 Analisis *Packet Loss*

Packet Loss merupakan jumlah paket data yang hilang selama proses transmisi. Pada kondisi *Baseline*, *Packet Loss* mencapai 2,5%, yang menunjukkan masih adanya paket data yang gagal diterima oleh tujuan.

Tabel 4.8.4 Analisis *Packet Loss*

No	Perbandingan	Nilai Awal (%)	Nilai Akhir (%)	% Penurunan
1.	Baseline → Filtering	2.5	1.2	-52.0%
2.	Baseline → QoS+Filtering	2.5	0.5	-80.0%
3.	Filtering → QoS+Filtering	1.2	0.5	-58.3%

Perhitungan detail: Penurunan *Packet Loss* Baseline→QoS+Filtering = ((2.5 - 0.5) / 2.5) × 100% = (2.0 / 2.5) × 100% = 80.0%. Penurunan *Packet Loss* sebesar 80% merupakan peningkatan yang paling dramatis dan secara langsung mencerminkan keberhasilan mitigasi *Bufferbloat*: ketika buffer tidak terisi penuh oleh trafik bersaing, mekanisme tail drop yang menyebabkan burst *Packet Loss* dapat dihindari.



Gambar 4.8.4 Grafik *Packet Loss*

4.9 Rekapitulasi Peningkatan Kinerja

Berdasarkan hasil pengujian yang telah dilakukan, diperoleh peningkatan kinerja pada setiap parameter *Quality Of Service* (QoS) setelah penerapan mekanisme mitigasi *Bufferbloat*. Rekapitulasi ini menunjukkan perbandingan nilai QoS pada kondisi baseline, filtering, dan QoS+Filtering, sehingga dapat memberikan gambaran kuantitatif mengenai efektivitas metode yang diusulkan dalam meningkatkan kualitas layanan jaringan pendidikan berbasis *Mikrotik*. Improvement dihitung dari Baseline ke QoS+Filtering

Tabel 4.9 Rekapitulasi Peningkatan Kinerja

No	Parameter	Baseline	Filtering	QoS+Filtering	Improvement	Kategori TIPHON
1.	*Throughput*	25.92 Mbps	35.05 Mbps	38.35 Mbps	+47.9%	Sangat Baik
2.	*Delay*	38 ms	35 ms	34 ms	-10.5%	Sangat Baik
3.	*Jitter*	37 ms	30 ms	28 ms	-24.3%	Baik
4.	*Packet Loss*	2.5%	1.2%	0.5%	-80.0%	Sangat Baik

4.10 Validasi Dengan Penelitian Terdahulu

Tabel berikut membandingkan hasil penelitian ini dengan temuan dari riset-riset terkait yang telah dipublikasikan:

Tabel 4.10 Validasi Dengan Penelitian Terdahulu

No	Peneliti	Metode	*ΔThroughput*	*ΔDelay/Jitter*	*ΔPacket Loss*
1.	Alamsyah & Somantri (2022)	HTB+*Queue Tree*/*Mikrotik*	+Tidak dkuantifikasi	Menurun	Menurun
2.	Barczyk & Chydzinski (2022)	AQM/Universitas	Stabil	-40% *Delay*	Menurun
3.	Gumeular & Akbi (2025)	PCQ+FQ_CoDel/*Mikrotik*	+30–40%	Menurun signifikan	-Signifikan
4.	MEKAR Journal (2025)	*FQ-CoDel/Mikrotik RouterOS7*	Tertinggi	Terendah	Terendah
5.	Penelitian Ini (2026)	Filtering+QoS+PCQ/*Mikrotik*	+47.9%	-10.5% *Delay*, -24.3% *Jitter*	-80.0%

Dari perbandingan ini, penelitian ini menunjukkan konsistensi dengan temuan penelitian terdahulu bahwa manajemen bandwidth berbasis *Mikrotik* mampu meningkatkan QoS secara signifikan. Peningkatan *Throughput* 47.9% yang dicapai sebanding dengan hasil Gumeular & Akbi (2025) menggunakan FQ_CoDel. Penurunan *Packet Loss* 80% merupakan hasil tertinggi di antara penelitian-penelitian yang dibandingkan, mengindikasikan efektivitas khusus kombinasi filtering dan HTB dalam mencegah burst *Packet Loss* akibat *Bufferbloat*.

4.11 Dampak Kenaikan Kinerja Terhadap Pembelajaran

Peningkatan parameter QoS yang terukur dalam penelitian ini memiliki dampak langsung terhadap kualitas pembelajaran di lingkungan pendidikan. Pertama, penurunan *Delay* dari 38 ms ke 34 ms (10.5%) berdampak pada pengurangan one-way *Delay* pada sesi video *conference* (Zoom/Google Meet). ITU-T G.114 merekomendasikan one-way *Delay* maksimum 150 ms untuk komunikasi interaktif; nilai 34 ms berada sangat jauh di bawah batas ini, mengimplikasikan kualitas komunikasi yang sangat baik.

Kedua, penurunan *Jitter* dari 37 ms ke 28 ms (24.3%) secara langsung meningkatkan stabilitas audio-video pada platform *e-learning*. Studi oleh Cisco (2024) menunjukkan bahwa *Jitter* di atas 30 ms mulai menyebabkan artefak audio yang mengganggu pemahaman. Dengan nilai 28 ms, jaringan berada di bawah ambang batas tersebut.

Ketiga, penurunan *Packet Loss* dari 2.5% ke 0.5% (80%) sangat signifikan untuk layanan TCP seperti download materi, upload tugas, dan akses LMS. *Packet Loss* 2.5% pada kondisi baseline menyebabkan retransmisi TCP yang menambah beban ekstra pada buffer (memperparah *Bufferbloat*), sedangkan *Packet Loss* 0.5% secara praktis tidak mengakibatkan gangguan layanan.

Keempat, peningkatan *Throughput* efektif dari 25.92 Mbps ke 38.35 Mbps (47.9%) memungkinkan lebih banyak pengguna simultan menikmati layanan berkualitas baik. Jika diasumsikan setiap pengguna membutuhkan minimal 1 Mbps untuk streaming pembelajaran, peningkatan ini secara teoritis mengizinkan penambahan ~12 pengguna simultan tanpa degradasi kualitas.

4.12 Generalisasi Hasil Penelitian

Penelitian ini dilaksanakan di SMKS Al-Islam Joresan Mlarak Ponorogo, namun temuan dapat digeneralisasikan ke konteks yang lebih luas berdasarkan kondisi berikut:

a. Institusi Pendidikan dengan *Mikrotik* sebagai Core Router: Seluruh SMK, SMA, SMP, dan perguruan tinggi yang menggunakan Router *Mikrotik* sebagai pusat manajemen jaringan dapat menerapkan framework mitigasi yang sama. Dominasi *Mikrotik* di institusi pendidikan Indonesia (khususnya SMK TKJ/TJKT) menjadikan temuan ini sangat relevan secara nasional.
b. Jaringan dengan Multi-Pengguna Simultan: Fenomena *Bufferbloat* paling kuat terjadi ketika banyak pengguna mengakses *internet* bersamaan. Kondisi ini umum di sekolah, dormitory/asrama, perpustakaan kampus,

dan pusat layanan masyarakat—semua lingkungan ini dapat memperoleh manfaat serupa.

c. Jaringan dengan Beban Trafik Heterogen: Di mana trafik produktif (*e-learning*, video *conference*) bersaing dengan trafik non-produktif (game online, social media) untuk bandwidth yang terbatas, *Packet Filtering* sebagai mekanisme pertahanan pertama akan efektif.

d. Limitasi Generalisasi: Hasil kuantitatif spesifik (47.9% peningkatan *Throughput*, dll.) adalah fungsi dari kapasitas bandwidth dasar, spesifikasi hardware *Mikrotik*, dan jumlah pengguna. Institusi dengan bandwidth lebih tinggi atau lebih rendah akan mendapatkan nilai absolut yang berbeda, namun tren peningkatan dan framework yang digunakan diperkirakan konsisten.

4.13 Framework Mitigasi *Bufferbloat* Berbasis *Mikrotik*

Berdasarkan hasil penelitian dan analisis komparatif, berikut adalah framework mitigasi *Bufferbloat* yang direkomendasikan untuk jaringan pendidikan berbasis *Mikrotik*:

a. Lapisan 1: Identifikasi dan Pengukuran (Assessment)

Sebelum implementasi mitigasi, lakukan pengukuran baseline parameter QoS (*Throughput*, *Delay*, *Jitter*, *Packet Loss*) menggunakan Wireshark dan Speedtest pada kondisi jam puncak. Identifikasi apakah *Delay/Jitter* tinggi terjadi hanya saat jaringan penuh (indikator *Bufferbloat*) atau juga pada kondisi jaringan kosong (indikator masalah fisik/ISP).

b. Lapisan 2: Mitigasi Tingkat Pertama – *Packet Filtering*

Implementasikan Firewall Filter pada *Mikrotik* untuk memblokir atau membatasi trafik non-pendidikan (game online, P2P, high-bandwidth streaming). Layer ini berfungsi mengurangi volume trafik yang berkompetisi mengisi buffer, secara langsung menurunkan probabilitas buffer overflow. Berdasarkan penelitian ini, filtering saja mampu meningkatkan *Throughput* 35.2% dan menurunkan *Packet Loss* 52%.

c. Lapisan 3: Mitigasi Tingkat Kedua – Traffic Classification

Implementasikan Firewall Mangle untuk packet marking berdasarkan kategori layanan: Prioritas Tinggi: video *conference*, VoIP, LMS real-time, Prioritas Normal: browsing, email, download akademik, Prioritas Rendah: trafik yang lolos dari filter tapi bukan prioritas. Klasifikasi ini mempersiapkan dasar bagi *Queue Tree* untuk alokasi bandwidth berprioritas.

d. Lapisan 4: Mitigasi Tingkat Ketiga – Queue Management

Implementasikan *Queue Tree* + PCQ untuk membatasi burst traffic dari setiap kategori melalui Token Bucket mencegah trafik burst mengisi buffer secara tiba-tiba, mendistribusikan bandwidth secara adil melalui PCQ sehingga tidak ada pengguna tunggal yang mendominasi buffer, memastikan trafik prioritas mendapatkan bandwidth yang dijamin bahkan saat jaringan penuh.

e. Lapisan 5: Monitoring dan Evaluasi Berkelanjutan

Lakukan pengukuran berkala (bulanan) untuk memvalidasi efektivitas konfigurasi dan mengidentifikasi perubahan pola trafik yang mungkin memerlukan penyesuaian. Gunakan The Dude (tool monitoring *Mikrotik*) atau Grafana dengan data dari RouterOS untuk monitoring real-time.

Tabel 4.13 Framework Mitigasi *Bufferbloat* Berbasis *Mikrotik*

No	Lapisan	Komponen	Tool *Mikrotik*	Dampak Utama
1.	1	Assessment	Wireshark, Speedtest	Identifikasi baseline *Bufferbloat*
2.	2	*Packet Filtering*	Firewall Filter	+35.2% *Throughput*, -52% *Packet Loss*
3.	3	Traffic Classification	Firewall Mangle	Dasar prioritas trafik
4.	4	Queue Management	*Queue Tree* + PCQ	+47.9% *Throughput*, -80% *Packet Loss* total
5.	5	Monitoring	The Dude / Grafana	Validasi berkelanjutan

BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan penelitian tentang analisis mitigasi *Bufferbloat* untuk peningkatan *Quality Of Service* pada jaringan pendidikan berbasis *Mikrotik* di SMKS Al-Islam Joresan Mlarak Ponorogo, diperoleh kesimpulan sebagai berikut:

1. Penerapan *Packet Filtering* dan QoS berbasis *Mikrotik* terbukti secara kuantitatif memberikan mitigasi efektif terhadap dampak *Bufferbloat*. Hal ini ditunjukkan oleh peningkatan *Throughput* sebesar 47.9% (dari 25.92 Mbps ke 38.35 Mbps), penurunan *Delay* 10.5% (dari 38 ms ke 34 ms), penurunan *Jitter* 24.3% (dari 37 ms ke 28 ms), dan penurunan *Packet Loss* 80.0% (dari 2.5% ke 0.5%) dari kondisi baseline ke kondisi QoS+Filtering.
2. *Packet Filtering* sebagai tahap pertama mitigasi memberikan kontribusi signifikan: peningkatan *Throughput* 35.2% (25.92→35.05 Mbps), penurunan *Packet Loss* 52.0% (2.5%→1.2%), penurunan *Jitter* 18.9% (37→30 ms), dan penurunan *Delay* 7.9% (38→35 ms). Penambahan QoS (*Queue Tree*+PCQ) pada tahap kedua memberikan kontribusi inkremental: *Throughput* +9.4% (35.05→38.35 Mbps), *Packet Loss* -58.3% (1.2%→0.5%), *Jitter* -6.7% (30→28 ms), *Delay* -2.9% (35→34 ms). Ini mengkonfirmasi bahwa filtering adalah intervensi yang paling cost-effective sebagai langkah pertama.
3. Hasil penelitian ini konsisten dan kompetitif dengan riset terdahulu. Peningkatan *Throughput* 47.9% sebanding dengan Gumeular & Akbi (2025) yang mencapai 30–40% menggunakan FQ_CoDel. Penurunan *Packet Loss* 80% merupakan yang tertinggi di antara penelitian pembanding, mengkonfirmasi bahwa kombinasi filtering + HTB sangat efektif dalam mencegah burst *Packet Loss* akibat *Bufferbloat*.
4. Framework mitigasi *Bufferbloat* 5 lapisan yang dikembangkan Assessment, *Packet Filtering*, Traffic Classification, Queue Management, dan Monitoring Berkelanjutan dapat diterapkan di institusi pendidikan lain yang

menggunakan infrastruktur *Mikrotik*. Framework ini bersifat platform-independen dalam prinsipnya dan dapat diadaptasi untuk merek router lain dengan mekanisme equivalen.

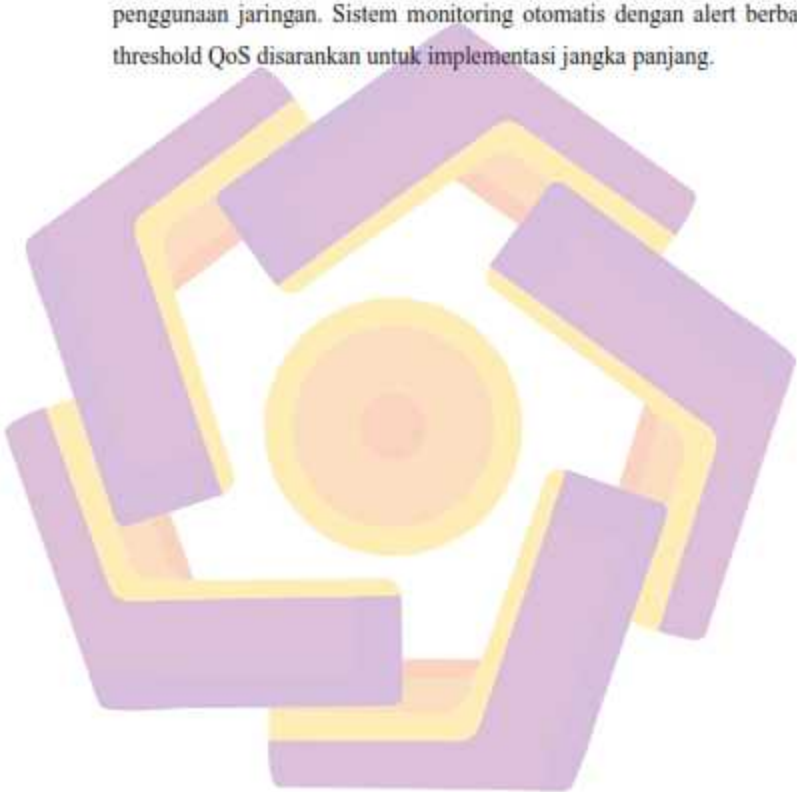
5. Penelitian ini berkontribusi sebagai studi empiris pertama (dalam konteks literatur Indonesia yang disurvei) yang secara eksplisit mengidentifikasi dan mengkuantifikasi mitigasi *Bufferbloat* pada jaringan pendidikan berbasis *Mikrotik*, serta memvalidasi efektivitas pendekatan berbasis filtering dan HTB sebagai alternatif praktis terhadap AQM algoritmik (CoDel/CAKE) yang memerlukan hardware lebih tinggi.

5.2 Saran

Berdasarkan hasil penelitian yang telah dilakukan, masih terdapat peluang untuk pengembangan lebih lanjut guna meningkatkan efektivitas mitigasi *Bufferbloat* pada jaringan pendidikan. Oleh karena itu, beberapa saran yang dapat diberikan adalah sebagai berikut:

1. Penelitian lanjutan disarankan untuk menguji implementasi CAKE atau *FQ-CoDel* pada *Mikrotik RouterOS* 7 di konteks sekolah untuk membandingkan efektivitasnya dengan pendekatan HTB+Filtering yang digunakan dalam penelitian ini. Berdasarkan temuan Barczyk & Chydzinski (2022) dan MEKAR Journal (2025), AQM algoritmik berpotensi memberikan penurunan *Delay* yang lebih besar (>40%) dan mitigasi *Jitter* yang lebih agresif.
2. Administrator jaringan sekolah disarankan mengimplementasikan framework 5 lapisan secara bertahap, dimulai dari Lapisan 2 (*Packet Filtering*) yang memberikan ROI paling tinggi dengan kompleksitas konfigurasi paling rendah. Migrasi ke *Mikrotik RouterOS* 7 yang mendukung CAKE sebagai queue type direkomendasikan untuk institusi yang ingin memaksimalkan mitigasi *Bufferbloat*.
3. Penelitian berikutnya disarankan menambahkan pengukuran *Bufferbloat* score menggunakan tool khusus seperti Flent atau LibreQoS untuk memberikan metrik *Bufferbloat* yang lebih presisi dibandingkan pengukuran *Delay*/*Jitter* konvensional.

4. Replikasi penelitian di beberapa sekolah dengan karakteristik berbeda (kapasitas bandwidth, jumlah pengguna, jenis ISP) akan memperkuat validitas generalisasi framework yang diusulkan.
5. Hasil penelitian ini menunjukkan bahwa konfigurasi QoS yang optimal saat ini mungkin tidak optimal di masa depan seiring perubahan pola penggunaan jaringan. Sistem monitoring otomatis dengan alert berbasis threshold QoS disarankan untuk implementasi jangka panjang.



DAFTAR PUSTAKA

Adji Putra Pamungkas F, Muhammad Reza Putra, M. H. (2021). Analisis Jaringan VPN Menggunakan PPTP dan L2TP Berbasis *Mikrotik* pada Diskominfo Kabupaten Muko Muko. *Analisis Jaringan VPN Menggunakan PPTP Dan L2TP Berbasis Mikrotik Pada Diskominfo Kabupaten Muko Muko*, *5*(1), 1–6. https://scholar.archive.org/work/5fkarcocwbeg5okacrqcqflph4/access/wayback/https://jkomtekinfo.org/ojs/index.php/komtekinfo/article/download/183/132

Aminah, S. (2022). Manajemen Bandwidth dalam Mengoptimalkan Penggunaan Router *Mikrotik* terhadap Pelayanan Koneksi Jaringan. *Jurnal Informatika Ekonomi Bisnis*, *4*, 102–106. https://doi.org/10.37034/infeb.v4i3.144

Andesita Prihantara, Antonius Agung Hartono, H. A. (2026). EFEKTIFITAS IMPLEMENTASI MANGLE FIREWALL PADA MANAJEMEN BANDWIDTH DI POLITEKNIK NEGERI CILACAP MELALUI PENDEKATAN PPDIOO. *JURNAL ELEKTRO & INFORMATIKA SWADHARMA (JEIS), VOLUME 06*.

Arfind, R., Supendar, H., & Fahlapi, R. (2023). Perancangan Virtual Private Network Dengan Metode PPTP Menggunakan *Mikrotik*. *Jurnal Komputer Antartika*, *1*(3), 108–116. https://doi.org/10.70052/jka.v1i3.28

Barczyk, M., & Chydzinski, A. (2022). AQM based on the queue length: A realnetwork study. *PLoS ONE*, *17*(2 February), 1–21. https://doi.org/10.1371/journal.pone.0263407

Gettys, J., & Nichols, K. (2012). *Bufferbloat*: Dark buffers in the *internet*. *Communications of the ACM*, *55*(1), 57–65. https://doi.org/10.1145/2063176.2063196

Gumeular, M. J., & Akbi, D. R. (2025). Optimalisasi QoS Manajemen Bandwidth Menggunakan PCQ dan FQ_Codel Berbasis *Mikrotik*. *Repositor*, *7*(2), 209–218.

Gustiawan, M., Yudianto, R. J., Pratama, J., & Fauzi, A. (2021). Implementasi Jaringan Hotspot Di Perkantoran Guna Meningkatkan Keamanan Jaringan Komputer. *Jurnal Nasional Komputasi Dan Teknologi Informasi (JNKTI)*, *4*(4), 244–247. https://doi.org/10.32672/jnkti.v4i4.3098

Hafizh Ridwan, M., Solehudin, A., & Rozikin, C. (2024). Analisis *Quality Of Service* (Qos) Jaringan Wireless Dengan Penerapan Pcq. *JATI (Jurnal Mahasiswa Teknik Informatika)*, *8*(3), 3293–3309. https://doi.org/10.36040/jati.v8i3.9663

Hamza, S. (2022). Pemanfaatan Firewall Mangle Untuk Pengaturan Packet Data Menggunakan Mark Connection Mark Packet dan Mark Rouring dengan RouterBoard RB941-2nD. *Jurnal Biosainstek*, *4*(2), 27–33. https://doi.org/10.52046/biosainstek.v4i2.1055

Hawari, M. F. (2025). Analisis *Quality Of Service* (Qos) Pada Jaringan *Internet* Di Universitas Mataram. *Journal of Education Method and ...*, *3*(1), 82–93. http://repository.ub.ac.id/147462/

Herawan, R. M., Prihantoro, C., & Arifa, A. B. (2023). *Rancang Bangun Jaringan Komputer Menggunakan Mikrotik untuk Manajemen Keamanan di PT . INKA Multi*. 485–491.

Husnang Anniar. (2022). Jurnal Ilmiah Sistem Informasi dan Teknik Informatika. *Jisti*, *5*(1), 1–7.

Ikhwandi, M. I., Azinar, A. W., & Sumarno. (2025). Implementasi Wireguard Sebagai Koneksi Menggunakan Routing *Mikrotik*. *Smatika Jurnal*, *15*(02), 292–301. https://doi.org/10.32664/smatika.v15i02.1898

Kurniawan, S., & Setiawan, A. (2025). *Perancangan Sistem Keamanan Jaringan Berbasis VLAN, Firewall, Dan Port Security Menggunakan Mikrotik Cisco*. *3*(8), 388–404.

Kusmanto, I., & Al, Z. (2025). Analisis Perbandingan Kualitas Jaringan *Internet* Indihome dan Iconnet Berdasarkan Metode QoS. *Journal of Computer Science Research and Technological Innovation*, *1*(1), 63–70. https://ejurnal.yarukom.com/index.php/OursLogic/article/view/50

Mahbub, A. R., & Srisulistiowati, D. B. (2026). *Penguruh Penggunaan Firewall Generasi Terbaru (NGFW) terhadap Tingkat Keamanan Jaringan di Koperasi Sekolah Bina Mulia (KSBM)*. *6*(2), 69–80.

Mufrot, M., & Sobari, I. A. (2023). Optimalisasi *Quality Of Service* Peer Connection Queue Dengan *Queue Tree* Rw Net Pada Kelurahan Pulau Kelapa Jakarta. *Jurnal Teknik Informatika*, *15*(1), 26–32. https://ejurnal.ulbi.ac.id/index.php/informatika/article/view/2292

Mukhti, D. A., Fitriana, Y. B., Yuwono, D. T., & W., Y. (2025). Analisis Kinerja Layanan RT/RW.NET Robby Media Berbasis Hotspot Menggunakan Metode *Quality Of Service*. *Digital Transformation Technology*, *5*(1), 23–32. https://doi.org/10.47709/digitech.v5i1.5549

Muniraa, Dasrilb, & Abduh, H. (2024). Jurnal Riset Sistem Informasi Membangun Web Filtering Dengan Dns Forwarding Pada Jaringan Wireless Berbasis *Mikrotik* Pada Sma Negeri 1 Palopo. *Denasya: Jurnal RIset Sistem Informasi*, *1*(3), 37–44. https://journal.smartpublisher.id/index.php/jissi/article/view/170

nasir, J., Langitta Setiawan, Y., Sabda Lesmana, L., & Revita, E. (2023). Implementasi Server Berbasis Ubuntu Dan *Mikrotik* Menggunakan Metode *Queue Tree*. *JOISIE Journal Of Information System And Informatics Engineering*, *7*(1), 71–77.

Naufal, L., & Albar, R. (2021). Public Cloud Storage Analysis and Design By Using the Forwarding Network Address Translation Feature Through Virtual Private Network Server Using Microtik. *Banda Aceh, Indonesia 1 Prodi Sistem Informasi*, *7*(2), 56–67.

Novianto, D., Japriadi, Y. S., & Tommy, L. (2023). Optimalisasi Koneksi Local Area Network (LAN) Menggunakan Metode Fasttrack Pada Routerboard *Mikrotik*. *Jurnal Media Infotama*, *19*(1), 224–229. https://doi.org/10.37676/jmi.v19i1.3548

Novianto, D., Japriadi, Y. S., Tommy, L., & Sujono. (2024). Mitigasi Dhcp Starvation Attack Pada Routerboard *Mikrotik* Dan Pengaruhnya Terhadap Performansi. *Jurnal Ilmiah Informatika Global*, *15*(2), 52–57. https://doi.org/10.36982/jiig.v15i2.3930

Nursobah, Pitrasacha Aditya, S. (2023). IMPLEMENTASI JARINGAN PPPOE DAN HOTSPOT SERVER RT/RW NET BERBASIS *MIKROTIK* DENGAN FITUR MIKHMON DI ADINET SAMARINDA SEBERANG. *Jurnal*

INFORMATIKA, *13*(1), 31–39. https://repository.wicida.ac.id/4525/

Paskal, R. A. (2024). Tinjauan Literatur: Implementasi Manajemen Bandwidth. *Innovative: Journal Of Social Science Research*, *4*(4), 8075–8090. https://j-innovative.org/index.php/Innovative/article/view/9670

Pratama, R., Dedy Irawan, J., & Orisa, M. (2022). Analisis *Quality Of Service* Sistem Manajemen Bandwidth Pada Jaringan Laboratorium Teknik Informatika Itn Malang. *JATI (Jurnal Mahasiswa Teknik Informatika)*, *6*(1), 196–204. https://doi.org/10.36040/jati.v6i1.4557

Pratomo, A. B. (2024). PENGEMBANGAN SISTEM FIREWALL PADA JARINGAN KOMPUTER BERBASIS *MIKROTIK ROUTEROS*. *Perancangan Sistem Informasi Kasir Penjualan Berbasis Web-Site Pada Toko V-Mart*, *2*(1), 10–16.

Rafif Abyakto, Naif Baihaqi, M. Aldi Firdaus, Salsabila Aulia, & Didik Aribowo. (2024). Simulasi TCP-IP Menggunakan Topologi Bus. *Uranus : Jurnal Ilmiah Teknik Elektro, Sains Dan Informatika*, *2*(2), 07–14. https://doi.org/10.61132/uranus.v2i2.97

Rahman, N. F. (2026). *Analisis Perbandingan Kinerja Protokol IPv4 dan IPv6 pada Jaringan Komputer Modern*. *2*(01), 2–9.

Randy Ikhsan Ramadhan, & Siti Madinah Ladjamuddin. (2022). Perancangan Sistem Web Filtering Dengan Metode Dns Forwarding Pada Jaringan Komputer Berbasis *Mikrotik RouterOS*. *Jurnal Informatika Dan Tekonologi Komputer (JITEK)*, *2*(2), 146–157. https://doi.org/10.55606/jitek.v2i2.231

Roberts Tamu Umbu, J., Alfa Ray Leo Lede, P., & Marten Doni Ratu, L. (2024). Implementasi Manajemen Bandwith Dan Filtering Firewall. *JATI (Jurnal Mahasiswa Teknik Informatika)*, *8*(3), 4247–4255. https://doi.org/10.36040/jati.v8i3.9885

Rosid, R. A., Ali, I., Studi, P., Informatika, T., Studi, P., Informatika, M., Studi, P., Perangkat, R., Cirebon, K., Komputer, J., Loss, P., *Internet*, A., & Performance, N. (2023). *Analisis Internet Network Performance Menggunakan*. *7*(1), 203–210.

Safira Safra, N. A. (2025). TeJoS: Teewan Journal Solutions. *Publisher: Teewan Journal Solutions*, *0*(0), 14–18. http://teewanjournal.com/index.php/teekes

Samosir, J., Loveri, T., & Sianipar, A. Z. (2026). *ANALISIS QOS JARINGAN PEMERINTAH MENGGUNAKAN TEKNIK DEEP PACKET INSPECTION*. *11*(1), 1799–1808.

Saputra, A., W, Y., & Widiarta, I. M. (2025). Analisis Perbandingan Jaringan *Internet* pada Layanan *Internet* Service Provider (ISP) dengan (Nethome) menggunakan Metode QoS (*Quality Of Service*). *Digital Transformation Technology*, *5*(2), 115–120. https://doi.org/10.47709/digitech.v5i2.6838

Subowo, M. H. (2023). Analisis Kinerja Jaringan Software-Defined Networking (SDN) Berbasis Open Network Operating System (ONOS) dengan Menggunakan Protokol OpenFlow 1.5: Studi Kasus pada Algoritma Flow Scheduling Shortest Path First (SPF) dan Weighted Round Robin (WRR). *Jurnal Teknologi Informatika Dan Komputer*, *9*(1), 266–273. https://doi.org/10.37012/jtik.v9i1.1519

Sundara, K. A., Aspriyono, H., & Supardi, R. (2022). Perancangan Manajemen

Bandwidth Menggunakan *Mikrotik* Router Wireless Pada Sekolah Menegah Kejuruan Negeri 4 Kota Bengkulu. *Jurnal Media Infotama*, *18*(2), 279–290.

Suryaningtyas, P. A., Pangestu, D. A., & Wicaksono, A. N. (2026). *Peran Jaringan Komputer Dalam Mendukung Implementasi Internet of Things Pada Berbagai Sektor Industri*. *1887*.

Syahputri, C. N., Anggraini, C., Anugerah, H. F., Zufria, I., & Nahwi, M. I. (2023). Penerapan Kinerja Filter Rule dengan Metode Raw dan Layer 7 Protocol di Router *Mikrotik*. *Jurnal Kridatama Saïns Dan Teknologi*, *5*(02), 433–447. https://doi.org/10.53863/kst.v5i02.969

Tarina, C., Ismara, N., Mahara, L., Alysa, A., & Azimah, N. (2026). Studi Literatur : Perkembangan Teknologi Firewall Dan Strategi Pertahanan Jaringan Pada Sistem Komputer. *JIKUM: Jurnal Ilmu Komputer*, *2*(1), 53–59. https://doi.org/10.62671/jikum.v2i1.154

Unggul, E. (2025). *11.Rizki+Dwi+Sanjaya+Oke (2) - Copy*. *2*(1), 97–103.

Valia Yoga Pudya Ardhana, & Mulyodiputro, M. D. (2023). Analisis *Quality Of Service* (QoS) Jaringan *Internet* Universitas Menggunakan Metode *Hierarchical Token Bucket (HTB)*. *Journal of Informatics Management and Information Technology*, *3*(2), 70–76. https://doi.org/10.47065/jimat.v3i2.257

Wagimin, A. F. (2024). *Meningkatkan Literasi Teknologi Jaringan di SMK Pangeran Balikpapan dengan Pelatihan Mikrotik*. *3*(3), 32–40.

Wardhana, A. N. W., Yahmin, M., & Aksara, L. F. (2024). *Quality Of Service* (QoS) analysis using Wireshark on the LAN network at An Najiyah High School Surabaya. *Jurnal Mandiri IT*, *12*(4), 222–228.

Wibowo, R. B. S., & Komalasari, Y. (2025). Penerapan *Quality Of Service* Menggunakan Hierarchical Token Bucket Pada Jaringan *Internet* Menggunakan *Mikrotik* di PT. Triwall Indonesia. *Jurnal Komputer Antartika*, *3*(2), 42–46. https://doi.org/10.70052/jka.v3i2.734

Widodo, B. A. (2024). Analisis *Quality Of Service* pemanfaatan Ethernet Over IP(EoIP) Tunnel di *Mikrotik*RouterOS dengan Routing Protocol OSPF. *Journal of Informatics, Information System, Software Engineering and Applications (INISTA)*, *1*(1), 1–8. https://doi.org/10.20895/inista.v1i1.17

Yehezkiel Saputra Wanggi, F. H. (2023). MANAGEMENT BANDWIDTH JARINGAN KOMPUTER DI PUSKESMAS RAMBANGARU MENGGUNAKAN HOTSPOT *MIKROTIK*. *CONTAR: Jurnal Ilmu Komputer*, *1*(1), 17–22. https://journal.unwira.ac.id/index.php/CONTAR/article/view/2373%0Ahttps://journal.unwira.ac.id/index.php/CONTAR/article/download/2373/712

Zaki, F. N. B., & Lukman, L. (2021). Analisis Perbandingan *Quality Of Service* (Qos) Pada Video Streaming Dengan Metode PCQ Dan HTB Menggunakan Router *Mikrotik*. *Respati*, *16*(3), 25. https://doi.org/10.35842/jtir.v16i3.415

Zulkarnain, A. F., Hijriana, N., Awaliyah, A., & Wijaya, E. S. (2025). Analisis *Quality Of Service* Dan Quality of Experience Jaringan *Internet* Berbasis Wireless Pada Layanan Telkomsel Orbit. *Technologia : Jurnal Ilmiah*, *16*(1), 78. https://doi.org/10.31602/tji.v16i1.17022

LAMPIRAN

1. Spesifikasi Perangkat Penelitian

NO	PERANGKAT	SPESIFIKASI
1	*Router*	*Mikrotik* RB951 Ui-2HnD
2	*Switch*	*Tp-Link LS1008*
3	*Access point*	*Tp-Link TL-WR840N*
4	Komputer Administrator	*ASUS Vivobook X1400EA*

NO	PERANGKAT	SPESIFIKASI
1	Komputer Client	*Intel Core i3, RAM 8GB*
2	Media Kabel	*UTP Cat 5e*
3	Koneksi *Internet*	*IndiHome 100 Mbps*
4	Tang	*Crimping Tools Kit*
5	Konektor	*Vascolink RJ45*

2. Dokumentasi Alat Penelitian

- **Dokumentasi *Router Mikrotik RB951 Ui-2HnD***

- **Dokumentasi *Konektor RJ45***

- **Dokumentasi Kabel *LAN***

- **Dokumentasi Tang *Crimping***

- **Dokumentasi Laptop *ASUS Vivobook***

- **Dokumentasi *Modem* (Sumber *Internet*)**

- **Dokumentasi *Konfigurasi Mikrotik***

- **Dokumentasi Keseluruhan Alat *Konfigurasi***

3. **Dokumentasi *Users* (Pengguna)**