INSOLOGI: Jurnal Sains dan Teknologi
https://journal.literasisains.id/index.php/INSOLOGI
ISSN 2828-4984 (Media Online) | ISSN 2828-4992 (Media Cetak)
Vol. 5 No. 2 (April 2026) 582-596
DOI: 10.55123/insologi.v5i2.7940
Submitted: 15-02-2026 | Accepted: 20-03-2026 | Published: 15-04-2026

Efektivitas Pengendalian Jaringan Wi-Fi dengan Metode *Evil Limiter* Linux di UKM PT Bimuda Karya Teknik

Azzam Aziandani Hidayat[1], Johan Pamungkas[2*], Alfa Yuliana Dewi[3]
[1,2,3]Program studi Teknik Elektro, Fakultas Teknik, Universitas Tidar, Kota Magelang, Indonesia
Email: [1*]azzam.aziandani.hidayat@students.untidar.ac.id, [2]johan@untidar.ac.id, [3]alfayuliana@gmail.com

Abstract

Limitations in traffic management features on ISP-provided routers are a common issue in industrial Wi-Fi networks, particularly in maintaining the stability of production network connections. The absence of bandwidth control mechanisms allows non-priority devices to consume excessive bandwidth, thereby degrading the quality of operational network services. This study aims to analyze the effectiveness of Evil Limiter as a software-based bandwidth management solution by utilizing the ARP redirection mechanism without requiring administrative access to the router or modifications to the network infrastructure. The research employs an experimental approach conducted on a production Wi-Fi network at PT Bimuda Karya Teknik using three testing scenarios: baseline, limiting, and blocking. Network performance is evaluated based on Quality of Service (QoS) parameters referring to the TIPHON standard, including throughput, delay, jitter, and packet loss. The results indicate that Evil Limiter is effective in controlling traffic from non-priority devices, where in the blocking scenario, target devices are completely isolated with a throughput of 0 Mbps and a packet loss of 100%, while the limiting scenario significantly reduces internet access for non-priority devices. Overall, the proposed method is proven to improve network stability for priority devices, particularly under high network load conditions.

Keywords: *Evil Limiter, Bandwidth Management, Quality of Service (QoS), ARP Redirection, Industrial Wi-Fi Network.*

Abstrak

Keterbatasan fitur manajemen trafik pada router bawaan ISP menjadi permasalahan umum pada jaringan Wi-Fi industri, khususnya dalam menjaga stabilitas koneksi jaringan produksi. Ketiadaan mekanisme pengendalian bandwidth menyebabkan perangkat non-prioritas berpotensi mengonsumsi bandwidth secara berlebihan, sehingga menurunkan kualitas layanan jaringan operasional. Penelitian ini bertujuan menganalisis efektivitas Evil limiter sebagai solusi manajemen bandwidth berbasis perangkat lunak dengan memanfaatkan mekanisme ARP *redirection* tanpa memerlukan akses administrator router maupun perubahan infrastruktur jaringan. Metode penelitian menggunakan pendekatan eksperimental pada jaringan Wi-Fi produksi dengan tiga skenario pengujian, yaitu *baseline*, *limiting*, dan *blocking*. Kinerja jaringan dianalisis berdasarkan parameter Quality of Service (QoS) mengacu pada standar TIPHON, meliputi throughput, *delay*, *jitter*, dan *packet loss*. Hasil penelitian menunjukkan bahwa Evil limiter efektif mengendalikan trafik perangkat non-prioritas. Pada skenario *blocking*, perangkat target berhasil diisolasi sepenuhnya dengan throughput 0 Mbps dan *packet loss* 100%. Sementara itu, skenario *limiting* mampu menurunkan akses internet perangkat non-prioritas secara signifikan. Secara keseluruhan, metode ini terbukti meningkatkan stabilitas jaringan bagi perangkat prioritas, terutama pada kondisi beban jaringan tinggi.

Kata Kunci: *Evil Limiter*, Manajemen *Bandwidth, Quality of Service*, ARP *Redirection*, Wi-Fi Industri.

2.1.1 PENDAHULUAN

Jaringan Wi-Fi telah menjadi infrastruktur penting dalam mendukung aktivitas operasional industri, khususnya dalam proses pertukaran data dan pemantauan sistem produksi secara *real-time*. Seiring dengan meningkatnya jumlah perangkat yang terhubung, kebutuhan akan pengelolaan *bandwidth* yang efektif menjadi semakin krusial (Renaldi Kurniawan 2025). Tanpa mekanisme pengendalian yang memadai, penggunaan bandwidth yang tidak terkendali dapat menyebabkan degradasi kualitas layanan jaringan, yang ditandai dengan penurunan *throughput* serta peningkatan *delay*, *jitter*, dan *packet loss*, terutama pada perangkat prioritas (Syafrudin 2025).

Permasalahan tersebut umumnya terjadi pada industri kecil dan menengah yang masih mengandalkan router bawaan *Internet Service Provider* (ISP). Perangkat ini umumnya memiliki keterbatasan dalam fitur manajemen lalu lintas jaringan, seperti traffic shaping dan pengaturan prioritas *bandwidth* (Imam Riadi 2020). Akibatnya, perangkat non-prioritas dapat mengonsumsi sumber daya jaringan secara berlebihan dan berdampak langsung terhadap stabilitas koneksi perangkat operasional. Meskipun perangkat jaringan kelas enterprise mampu mengatasi permasalahan tersebut, implementasinya membutuhkan biaya yang tinggi serta perubahan infrastruktur yang tidak selalu layak dilakukan (Rafinaldo 2023).

Dalam konteks sistem industri yang bergantung pada komunikasi data secara real-time, terjadinya *bottleneck bandwidt*h dapat menimbulkan risiko yang signifikan, seperti keterlambatan pengiriman *data monitoring*, terganggunya sinkronisasi antar perangkat produksi, hingga potensi terhentinya proses operasional (Julian 2025). Kondisi ini tidak hanya menurunkan efisiensi sistem, tetapi juga dapat berdampak pada kerugian finansial dan menurunkan tingkat keandalan sistem produksi secara keseluruhan. Oleh karena itu, diperlukan suatu metode pengendalian jaringan yang mampu menjaga kestabilan *Quality of Service* (QoS) secara adaptif tanpa mengganggu infrastruktur yang telah berjalan (Imam Santoso 2025).

Pendekatan manajemen *bandwidth* konvensional, seperti penggunaan *queue* pada *router* (misalnya Mikrotik), umumnya memerlukan akses administratif serta konfigurasi langsung pada perangkat jaringan inti. Hal ini menjadi kendala pada lingkungan industri menengah yang memiliki keterbatasan akses terhadap perangkat tersebut. Selain itu, perubahan konfigurasi pada jaringan produksi berisiko mengganggu layanan yang sedang berjalan. Oleh karena itu, diperlukan pendekatan alternatif yang lebih fleksibel dan non-invasif.

Seiring dengan perkembangan penelitian global dalam bidang pengendalian jaringan, pendekatan berbasis perangkat lunak dengan teknik manipulasi trafik, seperti ARP *redirection*, mulai banyak digunakan sebagai solusi alternatif dalam manajemen bandwidth. Beberapa penelitian menunjukkan bahwa metode ini mampu melakukan pengendalian lalu lintas jaringan tanpa memerlukan perubahan pada infrastruktur fisik maupun akses ke perangkat gateway utama. Pendekatan ini juga dinilai lebih adaptif dan *cost-efficient*, terutama pada lingkungan dengan keterbatasan kontrol jaringan.

Berdasarkan permasalahan tersebut, penelitian ini mengusulkan pemanfaatan *Evil Limiter* sebagai solusi pengendalian *bandwidth* berbasis perangkat lunak dengan memanfaatkan mekanisme ARP *redirection*. Metode ini memungkinkan proses pembatasan (*limiting*) dan pemutusan koneksi (*blocking*) pada perangkat tertentu tanpa memerlukan akses administrator router maupun perubahan konfigurasi jaringan. Dengan demikian, pendekatan ini diharapkan mampu menjadi solusi yang efektif, fleksibel, dan mudah diterapkan pada jaringan Wi-Fi industri dengan keterbatasan infrastruktur (Nabil A'isy 2024).

Penelitian ini bertujuan untuk menganalisis efektivitas penggunaan *Evil Limiter* dalam pengendalian bandwidth pada jaringan Wi-Fi industri, serta mengevaluasi dampaknya terhadap parameter *Quality of Service* (QoS) yang meliputi throughput, *delay*, *jitter*, dan *packet loss*. Selain itu, penelitian ini juga memberikan kontribusi dalam menunjukkan bahwa teknik ARP *redirection* dapat digunakan sebagai metode pengendalian jaringan yang non-invasif dan efisien, khususnya pada lingkungan industri dengan keterbatasan akses terhadap perangkat jaringan inti.

2. METODOLOGI PENELITIAN

Penelitian ini menggunakan metode eksperimen dengan pendekatan kuantitatif Meode ini juga untuk menganalisis pengaruh penerapan pengendalian *bandwidth* berbasis perangkat lunak terhadap kinerja jaringan Wi-Fi produksi (Amrullah & Wijayanto, 2024). Metode eksperimen dipilih karena penelitian melibatkan perlakuan langsung pada sistem jaringan, sehingga memungkinkan pengamatan terhadap perubahan performa sebelum dan sesudah penerapan kontrol *bandwidth* (Muh Akbar Al Maruf 2023). Pendekatan kuantitatif digunakan untuk memastikan bahwa evaluasi dilakukan secara objektif berdasarkan data numerik.

Pengukuran kinerja jaringan dilakukan menggunakan *parameter Quality of Service (*QoS), yaitu *throughput, delay* (latensi), *jitter*, dan *packet loss* (Safitri 2025). Data diperoleh melalui proses pengujian pada beberapa kondisi jaringan, kemudian dianalisis untuk mengidentifikasi perubahan kualitas layanan secara terukur (J. Dan 2018). Parameter-parameter tersebut digunakan sebagai indikator utama dalam menilai stabilitas dan performa jaringan (Muslim and Prihandoko 2019).

Rancangan penelitian terdiri dari tiga skenario pengujian, yaitu *baseline, limiting*, dan *blocking*. Skenario *baseline* merepresentasikan kondisi awal jaringan tanpa pengendalian *bandwidth*, sedangkan *limiting* dan *blocking* masing-masing merepresentasikan kondisi pembatasan dan penghentian lalu lintas pada perangkat non-prioritas. Pengendalian *bandwidth* dilakukan menggunakan perangkat lunak *Evil Limiter* yang memanfaatkan mekanisme ARP *redirection,* sehingga dapat mengatur lalu lintas jaringan tanpa memerlukan akses administratif ke *router* atau perubahan infrastruktur.

Penelitian dilaksanakan melalui dua tahapan, yaitu pengujian awal pada jaringan lokal untuk memverifikasi fungsi sistem, serta pengujian implementasi pada jaringan Wi-Fi produksi di lingkungan operasional nyata. Hasil dari setiap skenario dianalisis secara komparatif untuk mengevaluasi efektivitas metode dalam meningkatkan kualitas layanan jaringan dan stabilitas koneksi perangkat prioritas.

2.1 Alat dan Bahan

Perangkat keras dan perangkat lunak yang digunakan untuk membantu dalam melakukan penelitian ini adalah alat dan bahan yang digunakan di dalam penelitian ini.

2.1.1 Perangkat Lunak (*Software*)

Penelitian ini menggunakan empat perangkat lunak yang terintegrasi: (1) *VirtualBox* untuk menjalankan distribusi Linux, (2) *Nmap* dan *Evil Limiter* yang dijalankan di dalam lingkungan Linux. Pertama, *VirtualBox* digunakan untuk menciptakan lingkungan *virtual* yang terisolasi untuk pengujian. Dalam lingkungan *virtual* ini, *Nmap* digunakan untuk melakukan *network scanning* dan mengumpulkan informasi perangkat yang terhubung. Informasi ini kemudian digunakan oleh *Evil Limiter* untuk menerapkan kebijakan akses yang selektif, membatasi dan memblokir akses perangkat yang tidak dikenal. Berikut rincian dari perangkat lunak yang digunakan saat penelitian.

Tabel 1 Daftar perangkat lunak.

No	Perangkat Lunak	Versi	Keterangan
1.	*Oracle VirtualBox*	v7.1.10	Digunakan untuk menjalankan sistem operasi Kali Linux.
2.	Kali Linux	v2025.2	Digunakan sebagai sistem operasi pada komputer pengendali karena menyediakan dukungan perangkat lunak jaringan yang lengkap untuk kebutuhan pengujian.
3.	*Evil Limiter*	v1.5.0	Digunakan sebagai perangkat lunak utama untuk menerapkan manajemen *bandwidth* berbasis perangkat lunak melalui mekanisme ARP *redirection*, dengan fitur pembatasan (*limiting*) dan pemutusan koneksi (*blocking*)
4.	*Nmap*	v7.95	Digunakan untuk mengidentifikasi perangkat yang terhubung pada jaringan Wi-Fi produksi, termasuk informasi alamat IP dan alamat MAC perangkat
5.	*Wireshark*	v.4.2.3	Digunakan sebagai alat bantu untuk memantau dan memverifikasi lalu lintas jaringan, khususnya paket ARP, guna memastikan bahwa mekanisme *ARP redirection* berjalan sesuai dengan skenario pengujian.
6.	*Iperf3*	19.1	Digunakan untuk mengukur kinerja jaringan lokal, terutama parameter *throughput* antara perangkat klien dan sistem pengendali.
7.	*Cloudflare Speedtest*	*Website*	Digunakan untuk mengukur kualitas akses internet, termasuk kecepatan unduh, kecepatan unggah, dan latensi pada masing-masing skenario pengujian.

2.1.2 Perangkat keras

Beberapa perangkat keras digunakan dalam penelitian ini, bertujuan untuk memastikan perangkat lunak dapat berfungsi optimal sesuai dengan target yang ditetapkan. Penggunaan perangkat-perangkat ini juga memastikan bahwa tidak ada gangguan terhadap operasional perangkat lain saat perangkat lunak dijalankan. Adapun daftar perangkat keras yang digunakan dalam jaringan lokal penulis tersaji dalam tabel berikut.

Tabel 2 Daftar perangkat keras jaringan lokal penulis.

no	Perangkat Keras	Keterangan
1	Laptop / komputer pengendali	Digunakan sebagai sistem pengendali yang menjalankan perangkat lunak manajemen *bandwidth* dan alat bantu pengujian jaringan.
2	*Handphone* / perangkat karyawan.	Berupa smartphone dan/atau laptop yang terhubung ke jaringan Wi-Fi produksi. Perangkat ini diklasifikasikan sebagai perangkat prioritas dan perangkat non-prioritas sesuai dengan skenario pengujian.
3	*Router* bawaan ISP.	Digunakan sebagai perangkat jaringan utama yang menyediakan akses internet dan layanan Wi-Fi pada jaringan produksi. *Router* ini tidak dilakukan perubahan konfigurasi selama penelitian.
4.	Perangkat Jaringan Pendukung.	Meliputi media jaringan dan perangkat pendukung lain yang telah tersedia pada infrastruktur *existing* di lokasi penelitian.

2.2 Skenario Pengujian

Pengujian dilakukan pada jaringan Wi-Fi produksi dengan Pengujian dilakukan pada jaringan Wi-Fi produksi dengan tiga skenario, yaitu kondisi *baseline*, *limiting*, dan *blocking*. Pada skenario *baseline*, seluruh perangkat terhubung ke jaringan tanpa penerapan pengendalian *bandwidth* untuk memperoleh nilai awal kinerja jaringan. Skenario *limiting* diterapkan dengan membatasi *bandwidth* perangkat non-prioritas

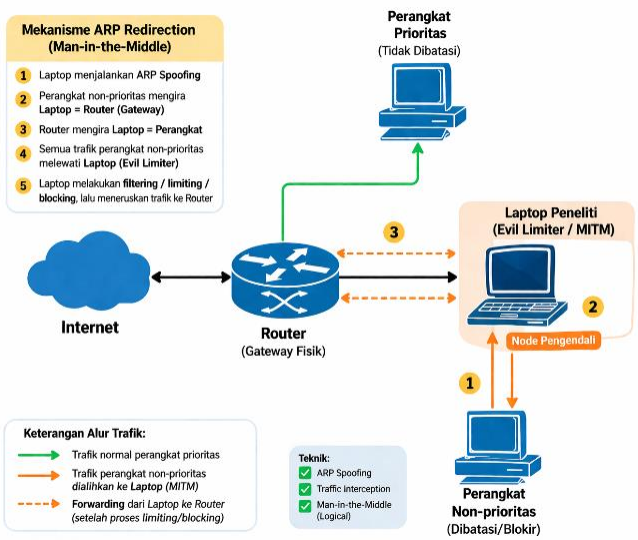
menggunakan *Evil limiter*, sedangkan pada skenario *blocking* dilakukan pemutusan akses internet perangkat non-prioritas secara penuh (Abramova, 2021). Ketiga skenario diuji pada kondisi jaringan yang sama untuk memastikan konsistensi hasil pengukuran.

Pengukuran parameter *Quality of Service* (QoS) dalam kecepatan akses internet pada perangkat non-prioritas dilakukan menggunakan *Cloudflare Speedtest* untuk memperoleh nilai *throughput* sebelum dan sesudah penerapan pengendalian *bandwidth*. Pengujian ini bertujuan untuk mengevaluasi perubahan kecepatan unduh dan unggah akibat penerapan mekanisme *limiting* dan *blocking*. Seluruh pengukuran dilakukan dari sisi perangkat non-prioritas sebagai klien pengujian.(Ismail Puji Saputra 2024)

Selain pengujian koneksi internet, pengukuran kinerja jaringan Wi-Fi lokal dilakukan menggunakan *Iperf3* dengan skema *client–server*. Pada pengujian ini, laptop peneliti berperan sebagai *server Iperf3*, sedangkan perangkat non-prioritas berupa smartphone bertindak sebagai klien. Pengujian *Iperf3* digunakan untuk mengukur kecepatan transfer data dan bitrate jaringan Wi-Fi pada masing-masing skenario pengujian, sehingga pengaruh penerapan pembatasan dan pemutusan koneksi menggunakan *Evil limiter* terhadap kinerja jaringan lokal dapat dianalisis secara lebih terkontrol.

2.3 Topologi jaringan

Berikut adalah gambar topologi jaringan pada saat penelitian



Gambar 1. Topologi Jaringan
Sumber : Dokumen Pribadi

Topologi jaringan yang digunakan dalam gambar 1 terdiri dari *router* bawaan ISP sebagai *gateway* utama, perangkat klien yang dibedakan menjadi perangkat prioritas dan non-prioritas, serta sebuah laptop peneliti yang menjalankan *Evil Limiter* sebagai node pengendali. Secara fisik, seluruh perangkat tetap terhubung langsung ke router melalui jaringan Wi-Fi yang sama tanpa adanya perubahan struktur topologi jaringan.

Namun, secara logis, mekanisme pengendalian dilakukan menggunakan teknik ARP *redirection* yang memanfaatkan metode ARP *spoofing* untuk menciptakan kondisi *Man-in-the-Middle* (MitM). Pada proses ini, node pengendali mengirimkan paket ARP palsu kepada perangkat target dan *router*, sehingga tabel ARP pada kedua sisi mengalami manipulasi. Akibatnya, perangkat non-prioritas menganggap bahwa alamat MAC dari node pengendali merupakan *gateway*, sementara *router* menganggap node pengendali sebagai perangkat klien tersebut.

Dengan kondisi tersebut, seluruh lalu lintas data dari perangkat non-prioritas tidak lagi langsung menuju *router*, melainkan terlebih dahulu dialihkan ke node pengendali. Setelah paket data diterima, node pengendali melakukan proses *filtering*, *limiting*, atau *blocking* sesuai skenario pengujian, kemudian meneruskan kembali paket tersebut ke router. Mekanisme ini memungkinkan pengendalian lalu lintas jaringan dilakukan secara transparan tanpa mengubah konfigurasi *gateway* maupun infrastruktur jaringan yang ada.

Sementara itu, perangkat prioritas tidak menjadi target manipulasi ARP sehingga tetap berkomunikasi langsung dengan *router* tanpa melalui node pengendali. Hal ini menyebabkan perangkat prioritas tidak terpengaruh oleh proses pembatasan maupun pemutusan koneksi yang diterapkan pada perangkat non-prioritas.Dengan demikian, topologi yang digunakan dalam penelitian ini menunjukkan adanya perbedaan antara topologi fisik dan topologi logis, di mana secara fisik jaringan tetap menggunakan arsitektur standar berbasis *router,* namun secara logis terjadi pengalihan jalur komunikasi melalui node pengendali. Pendekatan ini memungkinkan implementasi pengendalian *bandwidth* yang bersifat non-invasif, fleksibel, serta tidak memerlukan akses administratif terhadap perangkat jaringan utama (Luci and Michael 2024).

2.4 Teknik Pengumpulan Data

Teknik pengumpulan data dalam penelitian ini dilakukan untuk memperoleh data kuantitatif yang merepresentasikan kinerja jaringan Wi-Fi produksi pada setiap skenario pengujian (Anwar 2023). Data yang dikumpulkan berupa hasil pengukuran parameter *Quality of Service* (QoS) yang digunakan sebagai dasar analisis efektivitas pengendalian *bandwidth*(Ridwan 2024) .

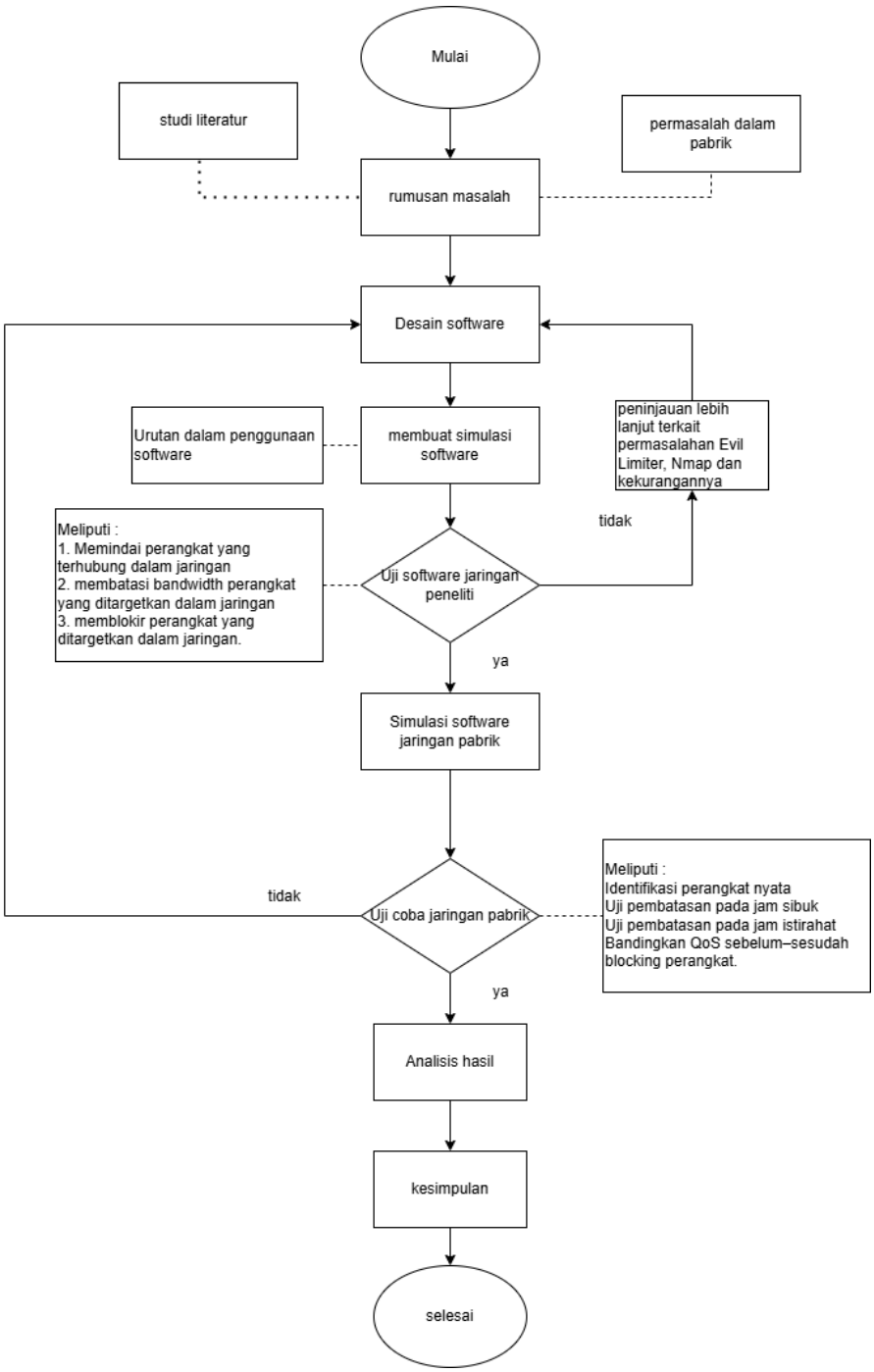
Pengumpulan data dilakukan secara langsung melalui pengujian eksperimental pada jaringan Wi-Fi produksi dengan menggunakan perangkat lunak pengukuran jaringan. Parameter throughput jaringan lokal dikumpulkan menggunakan *Iperf3*, sedangkan parameter kualitas akses internet, seperti kecepatan unduh, kecepatan unggah, dan latensi, dikumpulkan menggunakan *Cloudflare Speedtest* (Saputra, 2024). Pengukuran dilakukan pada perangkat prioritas dan perangkat non-prioritas sesuai dengan skenario pengujian yang diterapkan (Iman Setiawan 2025).

Selain itu, *Wireshark* digunakan sebagai alat bantu untuk memantau lalu lintas jaringan dan memverifikasi keberhasilan mekanisme *ARP redirection* selama proses pengujian (Sudirman 2021). Data yang diperoleh dari hasil pemantauan ini digunakan sebagai data pendukung untuk memastikan bahwa alur komunikasi jaringan berjalan sesuai dengan rancangan sistem (Renaldi Kurniawan 2025).

Seluruh data pengukuran dikumpulkan pada masing-masing kondisi pengujian, yaitu *baseline*, *limiting*, dan *blocking*, serta pada dua kondisi waktu operasional, yaitu jam sibuk dan jam istirahat. Data yang diperoleh kemudian dicatat dan disusun dalam bentuk tabel dan grafik untuk memudahkan proses analisis pada tahap selanjutnya (Zailan Harsin 2021).

2.5 Prosedur Penelitian

Penelitian yang dilakukan memerlukan beberapa tahapan agar mencapai tujuan yang diinginkan. Pada gambar dibawah ini akan menunjukkan alur dari penelitian yang akan dilakukan pada perusahaan PT Bimuda Karya Teknik, mulai dari peninjauan di area pabrik, menganalisis suatu permasalahan, hingga penggunaan alat untuk meminimalisir pada permasalahan di perusahaan. Berikut adalah gambaran dari alur penelitian yang akan dilakukan.



Gambar 2 Diagram alir penelitan
Sumber : Dokumen Pribadi

Penelitian ini diawali dengan kegiatan studi literatur dan identifikasi permasalahan pada jaringan Wi-Fi di lingkungan pabrik. Studi literatur dilakukan untuk memperoleh landasan teori mengenai *Evil Limiter*, *Nmap*, manajemen *bandwidth*, serta parameter kualitas layanan jaringan, sedangkan identifikasi masalah bertujuan merumuskan kendala nyata yang terjadi pada jaringan pabrik.

Berdasarkan hasil identifikasi tersebut, peneliti menyusun rumusan masalah yang kemudian menjadi dasar dalam tahap desain perangkat lunak. Pada tahap desain ini ditentukan kebutuhan fungsional *software*, alur kerja pembatasan dan pemblokiran perangkat, serta pemanfaatan *Nma*p untuk pemindaian perangkat yang terhubung ke jaringan.

Setelah desain disusun, peneliti membuat simulasi *software* sesuai rancangan dan menyusun urutan penggunaan software secara sistematis. Simulasi ini mencakup tiga fungsi utama, yaitu memindai perangkat yang terhubung ke jaringan, membatasi *bandwidt*h perangkat yang ditargetkan, dan memblokir perangkat yang dianggap mengganggu jaringan. Apabila pada tahap ini ditemukan kekurangan, dilakukan peninjauan lebih lanjut terkait permasalahan *Evil Limiter, Nmap*, serta keterbatasan implementasinya sebelum melanjutkan ke tahap berikutnya.

Tahap selanjutnya adalah pengujian *software* pada jaringan peneliti. Pada tahap ini peneliti menerapkan fungsi pemindaian, pembatasan, dan pemblokiran terhadap perangkat uji pada jaringan lokal milik peneliti untuk memastikan *software* berjalan sesuai rancangan. Jika hasil pengujian belum sesuai, maka simulasi dan desain software disesuaikan kembali hingga memenuhi kebutuhan penelitian.

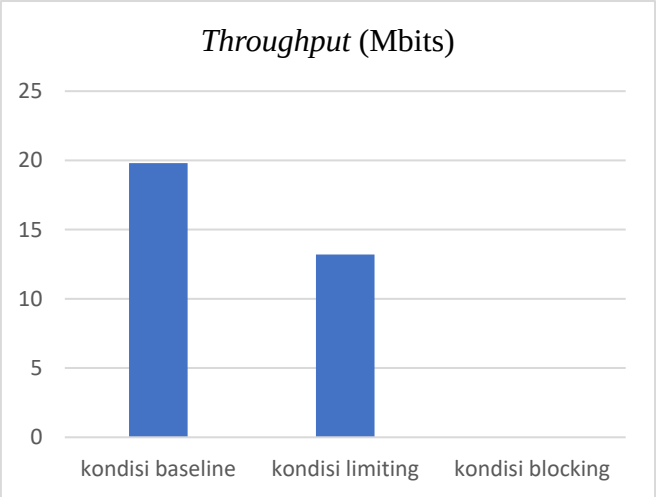
Setelah *software* dinyatakan berjalan dengan baik, dilakukan simulasi penerapan *software* pada jaringan pabrik. Simulasi ini kemudian dilanjutkan dengan uji coba langsung pada jaringan pabrik yang sesungguhnya, meliputi identifikasi perangkat nyata, uji pembatasan pada jam sibuk, uji pembatasan pada jam istirahat, serta perbandingan kualitas layanan (QoS) sebelum dan sesudah tindakan *blocking* perangkat. Hasil uji coba dianalisis untuk menilai efektivitas *software* dalam mengendalikan perangkat pengganggu dan meningkatkan stabilitas jaringan, kemudian dari analisis tersebut disusun kesimpulan sebagai akhir dari keseluruhan rangkaian penelitian

3. HASIL DAN PEMBAHASAN

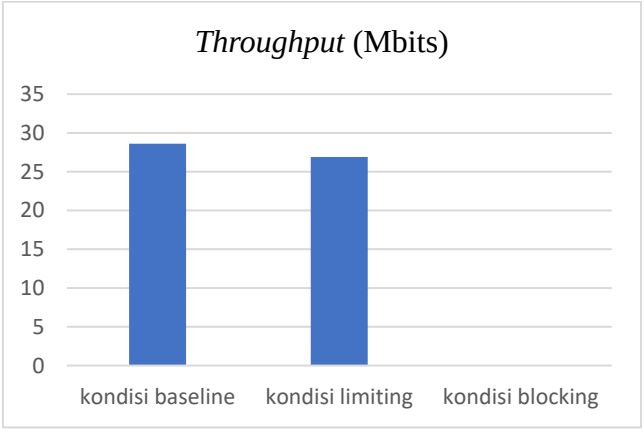
Bagian ini menyajikan hasil pengujian *Quality of Service* (QoS) jaringan yang diperoleh pada seluruh skenario pengujian, yaitu *baseline*, *limiting*, dan *blocking* dalam bentuk grafik. Ringkasan ini bertujuan untuk memberikan gambaran komparatif mengenai perubahan kinerja jaringan berdasarkan parameter QoS yang mengacu pada standar TIPHON, sebelum dilakukan analisis lebih lanjut pada subbab pembahasan

3.1 *Throughput*

Subbab ini menyajikan perbandingan nilai throughput sebagai salah satu parameter *Quality of Service* (QoS) pada jaringan Wi-Fi peneliti dan jaringan Wi-Fi di lingkungan pabrik. Pengukuran dilakukan pada kondisi *baseline*, *limiting*, dan *blocking* untuk menggambarkan perubahan kinerja transfer data pada setiap skenario pengujian.



Gambar 2. Pengujian total *throughput* pada perangkat di jaringan Wi-Fi peneliti
Sumber : Dokumen Pribadi



Gambar 3. Pengujian total *throughput* pada perangkat di jaringan Wi-Fi lingkungan pabrik
Sumber : Dokumen Pribadi

Berdasarkan grafik *throughput* dari gambar 2 dan 3 yang ditampilkan, kondisi *baseline* menunjukkan nilai transfer data yang stabil pada kedua lokasi pengujian. Pada kondisi *limiting* terjadi penurunan nilai *throughput* dibandingkan *baseline* sebagai akibat pembatasan *bandwidth* pada perangkat target. Sementara itu, pada kondisi *blocking* nilai *throughput* mendekati nol, yang menunjukkan bahwa layanan jaringan pada perangkat target tidak tersedia. Adapun hasil penurunan persentase dari hasil pengukuran *throughput* dari 3 kondisi tersebut ditunjukkan pada tabel dibawah ini

Tabel 1. Hasil peresetase penurunan nilai *throughput* dari kondisi *baseline* ke *limiting* dan *blocking*

Lokasi	Kondisi *baseline* => *limiting* (%)	Kondisi *baseline* => *blocking* (%)
Wi-Fi peneliti	33,33	100
Wi-Fi di lingkungan pabriik	5,94	100

Berdasarkan hasil pengujian, kondisi *baseline* menunjukkan nilai throughput yang stabil karena tidak terdapat pembatasan maupun intervensi terhadap aliran trafik jaringan. Pada kondisi ini, komunikasi berlangsung secara langsung antara perangkat dan router sehingga efisiensi transfer data berada pada kondisi optimal.

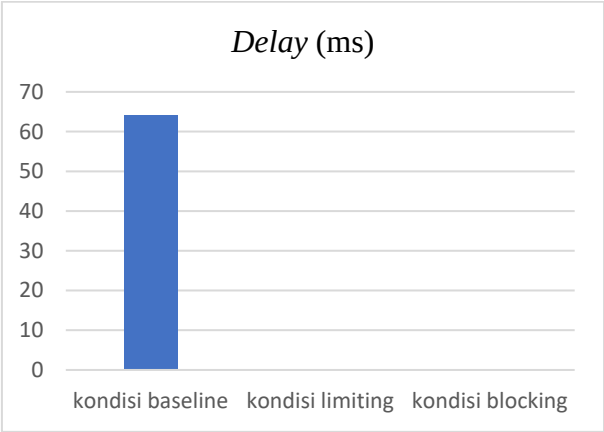
Pada skenario *limiting*, terjadi penurunan throughput yang signifikan dibandingkan kondisi *baseline*. Hal ini disebabkan oleh dua faktor utama, yaitu pembatasan bandwidth yang diterapkan oleh Evil Limiter serta perubahan jalur komunikasi akibat mekanisme ARP *redirection*. Proses intersepsi paket oleh node pengendali menyebabkan tambahan overhead dalam forwarding data, sehingga laju transfer efektif menjadi lebih rendah.

Sementara itu, pada skenario *blocking*, nilai throughput mendekati nol. Kondisi ini menunjukkan bahwa perangkat non-prioritas tidak lagi dapat mengakses jaringan karena seluruh paket yang dikirim tidak diteruskan oleh node pengendali. Dengan demikian, tidak terjadi proses transfer data yang valid antara perangkat dan jaringan.

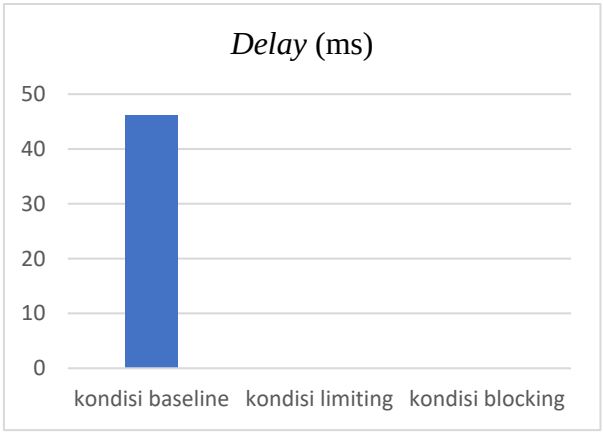
Berdasarkan standar TIPHON, kondisi *baseline* termasuk dalam kategori “Sangat Bagus”, sedangkan kondisi *limiting* mengalami penurunan ke kategori “Sedang” hingga “Buruk” tergantung tingkat pembatasan. Pada kondisi *blocking*, kualitas layanan masuk dalam kategori “Buruk” karena tidak tersedianya layanan jaringan

3.2 *Delay*

Subbab ini menyajikan hasil pengukuran *delay* sebagai parameter *Quality of Service* (QoS) yang merepresentasikan waktu tunda pengiriman paket data dalam jaringan. Perbandingan dilakukan pada kondisi *baseline*, *limiting*, dan *blocking* pada kedua lokasi pengujian untuk melihat perubahan karakteristik waktu respons jaringan.



Gambar 4. Pengujian total *delay* pada perangkat di jaringan Wi-Fi peneliti
Sumber : Dokumen Pribadi



Gambar 5. Pengujian total *delay* pada perangkat di jaringan Wi-Fi lingkungan pabrik
Sumber : Dokumen Pribadi

Grafik dari pengukuran *delay* yang ditunjukkan pada gambar 4 gambar 5 menunjukkan bahwa pada kondisi *baseline* waktu tunda pengiriman paket masih dapat diukur secara normal. Pada kondisi *limiting* ekstrem dan *blocking*, nilai *delay* tidak dapat dievaluasi karena perangkat tidak memperoleh respons dari jaringan eksternal. Kondisi ini menunjukkan bahwa parameter *delay* hanya dapat diukur pada saat layanan jaringan tersedia. Adapun nilai persentase perubahan pada nilai *delay* dari kondisi *baseline* ke *limiting* dan *blocking* tidak dapat dihitung karena parameter tidak terukur akibat tidak tersedianya layanan jaringan pada kondisi *limiting* ekstrem dan *blocking.*

Tabel 2 Hasil peresetase kenaikan nilai *delay* dari kondisi *baseline* ke *limiting* dan *blocking*

Lokasi	Kondisi *baseline* => *limiting* (%)	Kondisi *baseline* => *blocking* (%)
Wi-Fi peneliti	100	100
Wi-Fi di lingkungan pabriik	100	100

Hasil pengujian menunjukkan bahwa *delay* pada kondisi *baseline* masih berada dalam rentang normal karena komunikasi berlangsung secara langsung tanpa adanya intervensi tambahan pada jalur komunikasi.

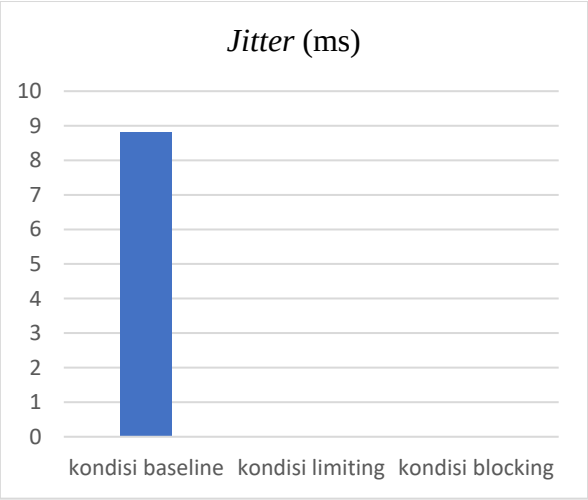
Pada kondisi *limiting*, terutama pada pembatasan ekstrem, nilai *delay* tidak dapat diukur secara valid karena perangkat mengalami kesulitan dalam memperoleh respons dari server. Hal ini disebabkan oleh pembatasan bandwidth yang terlalu rendah serta adanya antrian paket pada node pengendali akibat proses filtering dan forwarding.

Pada kondisi *blocking*, *delay* tidak dapat diukur sama sekali karena tidak terjadi komunikasi jaringan yang valid. Seluruh paket yang dikirim oleh perangkat tidak mendapatkan respons, sehingga parameter *delay* menjadi tidak terdefinisi.

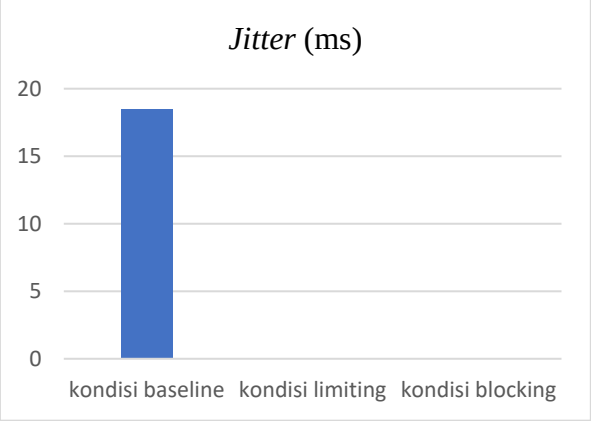
Mengacu pada standar TIPHON, *delay* pada kondisi *baseline* masih dapat dikategorikan "Bagus", sedangkan pada kondisi *limiting* ekstrem dan *blocking* tidak dapat diklasifikasikan karena tidak tersedianya layanan jaringan.

3.3 *Jitter*

Subbab ini menyajikan hasil pengukuran *jitter* sebagai bagian dari *parameter Quality of Service* (QoS) yang menggambarkan variasi waktu kedatangan paket data. Pengujian dilakukan pada jaringan Wi-Fi peneliti dan jaringan Wi-Fi di lingkungan pabrik untuk membandingkan kestabilan jaringan pada kondisi *baseline*, *limiting*, dan *blocking*.



Gambar 6 Pengujian total *jitter* pada perangkat di jaringan Wi-Fi peneliti



Gambar 7 Pengujian total *jitter* pada perangkat di jaringan Wi-Fi lingkungan pabrik

Berdasarkan grafik *jitter* yang ditunjukkan pada gambar 6 dan 7, kondisi *baseline* memperlihatkan variasi waktu kedatangan paket yang masih dalam batas wajar. Pada kondisi *limiting* ekstrem dan *blocking*, nilai *jitter* tidak dapat diukur karena tidak terjadi komunikasi paket yang valid dengan jaringan eksternal. Hal ini menunjukkan bahwa kestabilan jaringan hanya dapat dievaluasi ketika koneksi aktif tersedia. Adapun nilai persentase perubahan pada nilai *jitter* dari kondisi *baseline* ke *limiting* dan *blocking* tidak dapat dihitung karena parameter tidak terukur akibat tidak tersedianya layanan jaringan pada kondisi *limiting* ekstrem dan *blocking*.

Tabel 3 Hasil peresetase kenaikan nilai *jitter* dari kondisi *baseline* ke *limiting* dan *blocking*.

Lokasi	Kondisi *baseline* => *limiting* (%)	Kondisi *baseline* => *blocking* (%)
Wi-Fi peneliti	100	100
Wi-Fi di lingkungan pabriik	100	100

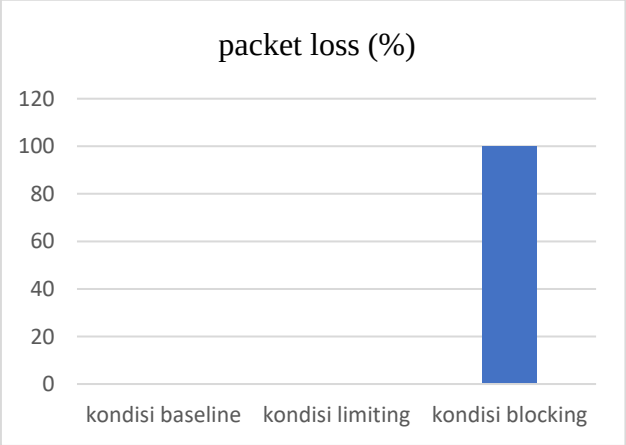
Pada kondisi *baseline*, nilai *jitter* relatif stabil karena variasi waktu kedatangan paket masih dalam batas wajar. Hal ini menunjukkan bahwa jaringan memiliki kestabilan yang baik dalam kondisi tanpa intervensi.

Namun, pada kondisi *limiting* ekstrem dan *blocking*, nilai *jitter* tidak dapat diukur. Hal ini terjadi karena tidak adanya aliran paket yang konsisten akibat pembatasan atau pemutusan koneksi. Tanpa adanya paket yang diterima secara kontinu, variasi waktu kedatangan tidak dapat dihitung.

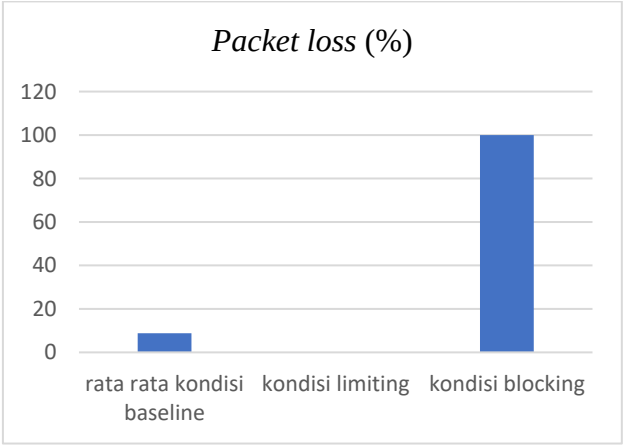
Dengan demikian, *jitter* hanya relevan dianalisis pada kondisi jaringan aktif (*baseline*), sedangkan pada kondisi *limiting* ekstrem dan *blocking*, parameter ini tidak dapat digunakan sebagai indikator kualitas jaringan.

3.4 *Packet loss*

Subbab ini menyajikan hasil pengukuran *packet loss* sebagai parameter Quality of Service (QoS) yang menunjukkan persentase paket data yang hilang selama proses transmisi. Perbandingan nilai *packet loss* dilakukan pada kondisi *baseline*, *limiting*, dan *blocking* untuk mengevaluasi tingkat reliabilitas layanan jaringan pada kedua lokasi pengujian



Gambar 8 Pengujian total *packet loss* pada perangkat di jaringan Wi-Fi peneliti



Gambar 9 Pengujian total *packet loss* pada perangkat di jaringan Wi-Fi lingkungan pabrik

Grafik dari gambar 8 dan gambar 9, *packet loss* menunjukkan bahwa pada kondisi *baseline* persentase kehilangan paket relatif rendah. Pada kondisi *limiting* terjadi perubahan nilai *packet loss* sesuai tingkat pembatasan yang diterapkan. Sementara pada kondisi *blocking*, *packet loss* meningkat signifikan hingga mendekati 100%, yang mengindikasikan tidak tersedianya layanan jaringan bagi perangkat target. Adapun nilai persentase perubahan pada nilai *packet loss* dari kondisi *baseline* ke *limiting* dan *blocking* tidak dapat dihitung karena parameter tidak terukur akibat tidak tersedianya layanan jaringan pada kondisi *limiting* ekstrem dan *blocking*.

Tabel 4 Hasil peresetase kenaikan nilai *packet loss* dari kondisi *baseline* ke *limiting* dan *blocking*.

Lokasi	Kondisi *baseline => limiting* (%)	Kondisi *baseline => blocking* (%)
Wi-Fi peneliti	100	100
Wi-Fi di lingkungan pabriik	100	100

Pada kondisi *baseline*, nilai *packet loss* relatif rendah yang menunjukkan bahwa sebagian besar paket berhasil dikirim dan diterima dengan baik.

Pada kondisi *limiting*, *packet loss* dapat meningkat tergantung tingkat pembatasan yang diterapkan. Hal ini disebabkan oleh adanya pembatasan bandwidth yang menyebabkan sebagian paket dibuang (*packet drop*) akibat keterbatasan kapasitas transmisi.

Pada kondisi *blocking*, nilai *packet loss* mencapai 100%, yang menunjukkan bahwa seluruh paket yang dikirim tidak berhasil mencapai tujuan. Hal ini terjadi karena node pengendali secara aktif memutus aliran komunikasi perangkat non-prioritas.

Berdasarkan standar TIPHON, kondisi *baseline* termasuk kategori "Sangat Bagus", sedangkan *limiting* berada pada kategori "Sedang hingga Buruk", dan *blocking* termasuk dalam kategori "Buruk"

3.5 Penjelasan

Nilai 100% yang muncul pada tabel 2, 3, dan 4 pada pengukuran *delay*, *jitter*, dan *packet loss* pada skenario *limiting* menunjukkan kondisi di mana pengukuran tidak dapat dilakukan secara valid, bukan peningkatan performa jaringan. Hal ini terjadi ketika pembatasan *bandwidth* yang diterapkan berada pada tingkat yang sangat rendah (*extreme limiting*), sehingga perangkat tidak mampu mengirim maupun menerima paket data secara efektif.

Pada kondisi tersebut, mekanisme ARP *redirection* yang dikombinasikan dengan pembatasan *bandwidth* menyebabkan sebagian besar atau seluruh paket data mengalami kegagalan transmisi. Akibatnya, tidak terdapat respons dari jaringan (*timeout*), sehingga alat ukur seperti *Cloudflare Speedtest* tidak dapat menghitung nilai *delay* dan *jitter* secara normal. Dalam sistem pengukuran, kondisi ini sering direpresentasikan sebagai nilai maksimum (100%) untuk menunjukkan kegagalan komunikasi.

Secara teknis, kondisi ini memiliki karakteristik yang mendekati skenario *blocking*, meskipun secara konfigurasi masih berada pada mode *limiting*. Hal ini menunjukkan bahwa batas bawah bandwidth yang diterapkan telah melewati ambang minimum layanan (*service threshold*), sehingga koneksi menjadi tidak *usable (*tidak dapat digunakan).

Oleh karena itu, nilai 100% pada parameter *delay*, *jitter*, dan *packet loss* dalam skenario *limiting* lebih tepat diinterpretasikan sebagai keterbatasan pengukuran (measurement *limitation*) akibat tidak tersedianya komunikasi jaringan yang valid, bukan sebagai indikator kualitas jaringan yang sebenarnya. Temuan ini juga menunjukkan bahwa penerapan *limiting* perlu mempertimbangkan batas *minimum bandwidth* agar tidak menyebabkan degradasi layanan yang setara dengan kondisi *blocking*.

4. KESIMPULAN

Berdasarkan hasil penelitian, penerapan *Evil Limiter* berbasis mekanisme ARP *redirection* terbukti efektif dalam mengendalikan penggunaan *bandwidth* pada jaringan Wi-Fi industri tanpa memerlukan perubahan konfigurasi pada router maupun infrastruktur jaringan. Metode ini bekerja secara non-invasif melalui teknik *Man-in-the-Middle* (MitM) dengan mengalihkan lalu lintas perangkat non-prioritas ke *node* pengendali. Hasil pengujian menunjukkan bahwa pada kondisi *limiting* terjadi penurunan *throughput* secara signifikan, sedangkan pada kondisi *blocking* perangkat non-prioritas tidak dapat mengakses jaringan dengan *throughput* mendekati nol dan *packet loss* mencapai 100%. Kondisi ini menunjukkan bahwa sistem mampu melakukan pembatasan dan pemutusan akses secara selektif sesuai kebutuhan.

Penerapan metode ini juga memberikan dampak positif terhadap kualitas layanan jaringan (QoS) pada perangkat prioritas, yang ditandai dengan meningkatnya stabilitas throughput serta menurunnya *delay, jitter,* dan *packet loss* akibat berkurangnya kompetisi *bandwidth*. Namun, pada kondisi *limiting* ekstrem, parameter QoS tidak dapat diukur secara valid karena koneksi berada di bawah ambang minimum layanan, sehingga perlu diperhatikan penentuan batas *minimum bandwidth* agar tetap menjaga keberlangsungan komunikasi. Dengan demikian, metode ARP *redirection* menggunakan *Evil Limiter* dapat menjadi solusi pengendalian jaringan yang fleksibel, efisien, dan sesuai untuk lingkungan industri dengan keterbatasan akses terhadap perangkat jaringan utama.

REFERENCES

A'isy, N. A., Sitorus, D. Z. R., Lubis, M. H. F., & Neyman, S. N. (2024). Kontrol Lalu Lintas Jaringan Wi-Fi menggunakan Evil Limiter pada Kali Linux. *Journal of Internet and Software Engineering*, *1*(3), 9. https://doi.org/10.47134/pjise.v1i3.2650

Abramova, E. A. (2021). *Analysis of the Impact of Priority Traffic Control Mechanisms on Network Quality of Service*. 0–2.

Ac, D. W., Transmisi, U., Penguji, T. I. M., & Skripsi, U. (2021). *ANALISA PERBANDINGAN KINERJA W-LAN 802 . 11 / N PADA SERVER E-LEARNING PROGRAM STUDI TEKNIK INFORMATIKA UNIVERSITAS ISLAM RIAU*.

Amrullah, M., & Wijayanto, D. (2024). *Manajemen bandwidth menggunakan mikrotik routerboard untuk optimalisasi layanan wifi koin (Meeting , Browsing , dan YouTube) Bandwidth Management Using Mikrotik Routerboard to Optimize Koin WiFi Services (Meeting , Browsing , and YouTube)*. *2*(September), 1410–1417.

Anwar, S., Informatika, F., Telkom, U., Karimah, S. A., Informatika, F., Telkom, U., Jadied, E. M., Informatika, F., & Telkom, U. (2023). *Deteksi ARP Spoofing pada Jaringan Wireless Menggunakan Metode String Matching dengan Algoritma Boyer Moore dan Brute Force*. *10*(3), 3450–3454.

Cetak, I., Online, I., Laboratorium, P., Komputer, T., & Jaringan, D. A. N. (2023). *DECODE : Jurnal Pendidikan Teknologi Informasi*. *3*(2), 246–256.

Dan, J. P. (2018). *PENGATURAN PEMAKAIAN BANDWIDTH DAN AKSES JARINGAN*. *3*(2), 167–172.

Julian, A., Nababan, N., & Lasut, D. (2025). *ANALISIS KUALITAS JARINGAN INTERNET BERBASIS WIRELESS LAN MENGGUNAKAN METODE QOS (QUALITY OF SERVICE)*. *2*.

Jurnal, I., Saputra, I. P., Komputer, F. I., Metro, U. M., & Security, C. (2024). *EFEKTIVITAS CLOUDFLARE GATEWAY DALAM MEMBATASI AKSES PORNOGRAFI*. *8*(April).

Kantor, D. I., & Mesuji, K. (2025). *ANALISIS KINERJA JARINGAN INTERNET MENGGUNAKAN METODE QOS (QUALITY OF SEVICE)*. *6*(2).

Kasus, S., Pembangunan, U., & Budi, P. (2019). *Analisis dan Implementasi Bandwidth Management Menggunakan Mikrotik OS untuk Optimalisasi Penggunaan Jaringan Internet*. *6*, 25–30.

Korespondensi, E., Naskah, R., Santoso, I., Nursiaga, R., Firmansyah, H., Teknologi, U., Jakarta, M., Jaringan, S., & Factory, S. (2025). *DESAIN SISTEM JARINGAN UNTUK SMART FACTORY BERBASIS INDUSTRIAL INTERNET OF THINGS (IIOT)*. *01*(01), 62–68.

Multidisiplin, J., & Volume, S. (2025). *1 2 3 4*. *9*(1).

No, V., Riadi, I., Fadlil, A., Hafizh, M. N., Studi, P., Informasi, S., & Dahlan, U. A. (2020). *Edumatic : Jurnal Pendidikan Informatika*. *4*(1), 21–29. https://doi.org/10.29408/edumatic.v4i1.2046

Oleh, D. S., Luci, S., & Michael, G. (2024). *BLOCKING IP dan LIMIT BANDWITH MENGGUNAKAN EVILLIMITER dan P2POWER Mata Kuliah : Network Fundamental na Santa*.

Rafinaldo, M. S., Iskandar, I., Harahap, N. S., & Candra, R. M. (2023). *Analisis Kualitas Jaringan Internet pada SMK Menggunakan Metode Quality of Service*. *3*(6), 977–984. https://doi.org/10.30865/klik.v3i6.903

Ridwan, M. H., Solehudin, A., & Rozikin, C. (2024). *ANALISIS QUALITY OF SERVICE (QOS) JARINGAN WIRELESS DENGAN PENERAPAN PCQ (STUDI KASUS : KANTOR KECAMATAN KEMANG)*. *8*(3), 3293–3309.

Safitri, T. I., Juwita, K., Rihadian, P., Fitria, N. D., Zulfa, I. A., & Yulia, I. D. (2025). *Analisis QoS Menggunakan Standar TIPHON pada Jaringan Wi-Fi SMK Dharma Bahari Surabaya*. *4*(4), 2433–2443.

Sudirman, D., & Akma Nurul Yaqin. (2021). Network Penetration dan Security Audit Menggunakan Nmap. *SATIN - Sains Dan Teknologi Informasi*, *7*(1), 32–44. https://doi.org/10.33372/stn.v7i1.702

Syafrudin, T., Rianto, R., Ujianto, E. I. H., Informasi, M. T., & Yogyakarta, U. T. (2025). *Analisis Kualitas Layanan Jaringan Wlan Berdasarkan Parameter Throughput , Delay , Jitter , dan Packet loss di Universitas X Analysis of Wlan Network Service Quality Based on Throughput , Delay , Jitter , and Packet loss Parameters at University X*. *5*(8), 2143–2151.

.