Analisa Kinerja Jaringan Komputer Kampus: Dinamika Lalu Lintas Paket Dan Beban Pemrosesan Di Lantai 8 Dan 9 TULT

1st Ramos Wilfred Situmorang
School of Industrial Engineering
Telkom University
Bandung, Indonesia
ramoswilfred@student.telkomuniversity.ac.id

2nd Rd. Rohmat Saedudin
School of Industrial Engineering
Telkom University
Bandung, Indonesia
rdrohmat@telkomuniversity.ac.id

3rd Umar Yunan Kurnia Septo H
School of Industrial Engineering
Telkom University
Bandung, Indonesia
umaryunan@telkomuniversity.ac.id

***Abstrak* — Penelitian ini menganalisis kinerja jaringan pada level *paket* di lantai 8 dan 9 Gedung Telkom University Landmark Tower (TULT) untuk mengidentifikasi masalah yang tidak terdeteksi oleh pemantauan umum. Dengan menggunakan metode *packet capturing* dengan Wireshark pada jam sibuk dan senggang, lalu lintas dianalisis untuk memahami dinamika dan beban pemrosesan jaringan. Hasilnya menunjukkan performa yang kontras. Jaringan Lantai 9 sangat stabil dan mampu menangani *traffic burst* ekstrem tanpa *TCP errors*, namun menunjukkan anomali lalu lintas latar belakang yang sangat tinggi saat jam senggang. Sebaliknya, jaringan Lantai 8 menunjukkan penurunan stabilitas dengan munculnya *TCP errors* saat beban puncak di jam sibuk. Di satu sisi, jaringan Lantai 8 menunjukkan risiko ketidakstabilan teknis; meskipun memiliki *Packet Rate* rata-rata yang stabil antara jam sibuk 261 pps dan senggang 259 pps, jaringan ini menghasilkan *TCP errors* saat terjadi lonjakan lalu lintas di jam sibuk. Di sisi lain, jaringan Lantai 9 terbukti sangat tangguh tanpa *TCP errors*, namun mengungkap risiko operasional dari beban anomali yang masif, di mana *Packet Rate* saat jam senggang 775,3 pps melonjak lebih dari tiga kali lipat dibandingkan jam sibuk 225,4 pps. Kesimpulannya, analisis ini berhasil mengungkap dan membedakan dua profil risiko kinerja yang fundamental berbeda: risiko keterbatasan fisik dan risiko operasional. Temuan ini menjadi dasar untuk rekomendasi optimasi yang spesifik dan tepat sasaran.**

***Kata kunci*— Kinerja Jaringan, Analisis Paket, Dinamika Lalu Lintas, Wireshark, Beban Pemrosesan**

I. PENDAHULUAN

Di era digital, infrastruktur jaringan yang andal adalah aset vital bagi institusi pendidikan tinggi seperti Telkom University. Kinerja jaringan yang optimal menopang seluruh kegiatan akademik dan operasional, sebuah tantangan yang juga dihadapi di lingkungan kampus lainnya [1]. Untuk menjaga kualitas layanan, sistem pemantauan seperti Zabbix yang memanfaatkan *Simple Network Management Protocol* (SNMP) telah diimplementasikan secara luas [2], [3], [4]. Sistem ini efektif untuk memberikan gambaran agregat mengenai utilisasi jaringan dan memberikan peringatan dini saat terjadi anomali. Namun, metrik umum ini seringkali gagal mendiagnosis akar masalah yang tersembunyi, terutama yang berkaitan dengan tekanan pada kapasitas pemrosesan perangkat akibat lonjakan lalu lintas *paket* yang intens dan sesaat. Tantangan modern seperti pemrosesan *paket* berkecepatan tinggi menunjukkan bahwa beban sesungguhnya pada perangkat jaringan tidak hanya berasal dari volume data (*bandwidth*), tetapi juga dari laju *paket* (*packet rate*) [10].

Kesenjangan diagnostik inilah yang menjadi fokus penelitian ini. Analisis pada tingkat *paket* diperlukan untuk memahami dinamika lalu lintas yang sebenarnya, sebuah pendekatan yang relevansinya terus meningkat untuk diagnosis akurat [6], [7]. Penelitian ini bertujuan melakukan analisis mendalam terhadap karakteristik lalu lintas di lantai 8 dan 9 Gedung Telkom Landmark Tower (TULT) untuk: (1) menganalisis karakteristik kepadatan *paket* dan beban pemrosesan *paket* antara kondisi jaringan sibuk dan jam senggang; serta (2) mengidentifikasi potensi risiko dan penyebab masalah kinerja berdasarkan pola lalu lintas yang teramati.

II. KAJIAN TEORI

A. Konsep Dasar Analisis Kinerja Jaringan

Analisis kinerja pada level *paket* adalah pendekatan fundamental yang presisi untuk memahami perilaku jaringan yang sesungguhnya. Di saat metrik agregat yang biasa ditampilkan oleh sistem pemantauan umum seringkali tidak cukup untuk mendiagnosis masalah tersembunyi, analisis *paket* memberikan wawasan *granular* dengan memeriksa setiap unit data yang ditransmisikan [11]. Metrik umum seperti utilisasi *bandwidth* rata-rata dalam beberapa menit dapat menyembunyikan masalah-masalah kritis yang terjadi dalam hitungan detik, seperti lonjakan lalu lintas sesaat (*micro-burst*) yang bisa menyebabkan degradasi layanan.

Pendekatan analisis *paket* mengatasi keterbatasan ini dengan melakukan inspeksi mendalam pada komponen-komponen setiap *paket*. Dengan menganalisis *header*, *payload*, dan *timestamp* kedatangan setiap *paket* secara individual, akar penyebab degradasi kinerja dapat diidentifikasi secara akurat [11]. *Header* berisi informasi kontrol yang vital seperti alamat IP sumber dan tujuan, nomor *port*, dan jenis protokol, yang memungkinkan pelacakan aliran data spesifik [8]. Ukuran *payload* memberikan petunjuk tentang jenis aplikasi yang berjalan, sementara *timestamp* yang presisi menjadi dasar untuk menghitung metrik vital seperti *jitter* (variasi jeda) dan waktu antar-

kedatangan, yang secara langsung berkaitan dengan stabilitas dan kelancaran koneksi [9].

Oleh karena itu, pemahaman tentang bagaimana *paket-paket* ini bergerak, karakteristiknya, dan dinamika temporal kedatangannya sangat krusial untuk menilai stabilitas, efisiensi, dan kapasitas jaringan secara akurat dari perspektif yang paling dasar. Ini menjadi fondasi untuk proses *troubleshooting* yang efektif dan optimasi jaringan yang sesungguhnya, melampaui apa yang bisa ditawarkan oleh pemantauan tingkat tinggi [6], [7].

B. Parameter Kuantitatif Analisis Berbasis *Paket*

Untuk menganalisis kinerja jaringan secara kuantitatif, penelitian ini berfokus pada dua parameter utama yang saling melengkapi dalam memberikan gambaran tentang kepadatan dan beban lalu lintas.

Parameter pertama, Rata-rata Interval Waktu Antar-Kedatangan (*Average Inter-Arrival Interval*), mengukur rata-rata selang waktu yang berlalu antara kedatangan dua *paket* yang berurutan. Diukur dalam satuan detik per *paket* (*seconds per packet*), metrik ini merupakan indikator langsung dari kepadatan temporal aliran data. Interval yang lebih pendek secara logis menunjukkan kepadatan *paket* yang lebih tinggi, yang memberikan tekanan yang lebih besar pada antrean dan kapasitas *buffer* pada perangkat jaringan seperti *switch* dan *router*. Analisis terhadap interval waktu antar-kedatangan sangat berguna untuk memahami karakteristik dan stabilitas aliran data, serta dapat mengidentifikasi pola lalu lintas yang bergelombang atau *bursty* [9].

Parameter pelengkapnya adalah Rata-rata Beban Pemrosesan *Paket* (*Packet Rate* / PPS), sebuah metrik fundamental yang mengukur jumlah *paket* yang harus diproses oleh perangkat jaringan setiap detiknya. *Packet Rate* adalah metrik yang krusial karena perangkat jaringan memiliki batas kapasitas pemrosesan *paket* (*forwarding rate*) yang terpisah dari kapasitas *bandwidth* (*Bps*). Beban pemrosesan *paket* yang tinggi dapat menyebabkan *bottleneck* berbasis pemrosesan, bahkan jika *bandwidth link* masih sangat lapang [10]. Oleh karena itu, metrik ini sangat penting untuk mendiagnosis masalah performa yang terkait dengan keterbatasan komputasi perangkat itu sendiri.

C. Alat Analisis

Untuk melakukan analisis mendalam pada tingkat *paket*, perangkat lunak seperti Wireshark menjadi instrumen esensial dalam penelitian ini. Wireshark adalah sebuah *network protocol analyzer* berbasis *open-source* yang diakui secara luas di industri dan akademik karena kemampuannya yang sangat detail [11]. Perangkat lunak ini dapat digunakan untuk menangkap dan menganalisis lalu lintas data yang melewati sebuah *interface* jaringan secara *real-time*, atau menganalisis data dari *file capture* yang sudah ada (dalam format *.pcap* atau *.pcapng*).

Kemampuan utama Wireshark yang sangat relevan untuk penelitian ini adalah kemampuannya untuk menampilkan detail setiap *paket* secara individual, termasuk inspeksi mendalam pada *header*, *payload*, dan *timestamp* kedatangan yang presisi. Hal ini menjadikannya *tool* yang ideal untuk melakukan analisis kinerja jaringan secara *granular*. Dalam penelitian ini, Wireshark digunakan sebagai *tool* utama untuk tahap *packet capturing* dan ekstraksi data mentah. Selain itu, fitur filter yang canggih serta fitur visualisasi melalui *I/O Graphs* sangat krusial untuk analisis dinamika lalu lintas, identifikasi anomali, dan korelasi antara *traffic burst* dengan *error* protokol yang tidak terlihat dari metrik rata-rata sederhana [12].

III. METODE

A. Kerangka dan Lingkungan Penelitian

Penelitian ini menerapkan *Framework* Analisis Kinerja Jaringan Berbasis Data *Paket*, sebuah pendekatan sistematis untuk pengukuran dan interpretasi lalu lintas *paket*. Objek penelitian adalah infrastruktur jaringan aktif di lantai 8 dan 9 Gedung TULT, Telkom University. Lingkungan penelitian didukung oleh perangkat keras yang perannya krusial dalam distribusi lalu lintas, dirangkum pada Tabel 1.

TABEL 1
(A)

Perangkat	Spesifikasi Utama / Fungsi
Ruijie S2910 Series	Layer 2 Switch dengan port 1G, mendukung SNMP, berfungsi sebagai titik distribusi trafik di setiap lantai.
H3C SR6604	Router utama yang berfungsi sebagai gateway dari ISP ke jaringan kampus, dengan kapasitas routing besar.
Laptop Asus TUF Gaming	Digunakan sebagai host untuk menjalankan Wireshark dan merekam data lalu lintas dari jaringan.

B. Prosedur Penelitian

Pengumpulan data primer dilakukan melalui *packet capturing* menggunakan Wireshark. Untuk merekam lalu lintas secara pasif tanpa mengganggu operasional jaringan, laptop dihubungkan ke jaringan yang tersedia dilantai tersebut. Pengambilan data dilakukan pada dua skenario: Jam Sibuk (periode aktivitas pengguna intensif) dan Jam Senggang (periode aktivitas pengguna minimal).

Data mentah (.pcapng) diekspor ke format CSV dengan menyertakan kolom relevan seperti *No.*, *Time*, *Source*, *Destination*, *Length*, dan *Protocol*. Data kemudian diolah di Microsoft Excel. Kolom turunan *Inter-Arrival Time* dibuat dengan menghitung selisih *timestamp* antar *paket* berurutan. Parameter kinerja kuantitatif dihitung menggunakan rumus berikut:

1. Rata-rata Interval Waktu Antar-Kedatangan, yang mengukur kepadatan paket, dihitung dengan rumus:

$$Rata-rata\ Interval\ Waktu\ Antar-Kedatangan = \frac{\sum_{i=1}^{N} IATi}{N} \quad (1)$$

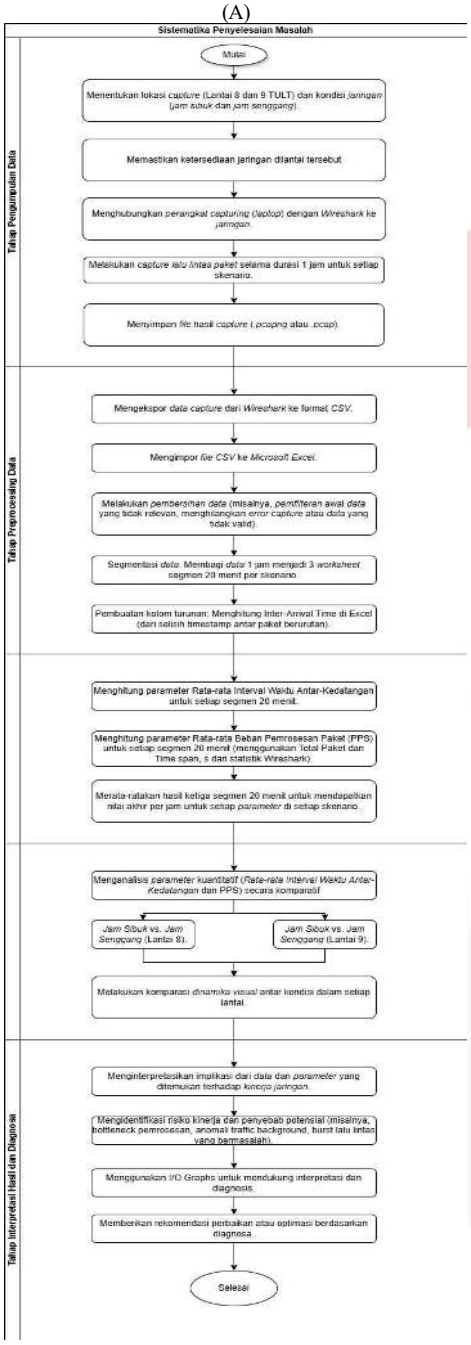
di mana $IATi$ adalah *Inter-Arrival Time* paket ke-i dan N adalah jumlah total paket.

2. Rata-rata Beban Pemrosesan Paket (*Packet Rate*), yang mengukur beban komputasi perangkat , dihitung dengan rumus:

$$PPS = \frac{Total\ Paket}{Total\ Waktu\ Segmen\ (dalam\ detik)} (2)$$

Proses analisis akhir melibatkan komparasi hasil antar skenario dan interpretasi temuan yang didukung dengan bukti visual dari *I/O Graphs*.

GAMBAR 1
(A)



IV. HASIL DAN PEMBAHASAN

Analisis data mengungkap profil kinerja dan risiko yang sangat kontras antara kedua lantai, menyoroti adanya masalah tersembunyi yang berbeda.

A. Hasil Kuantitatif dan Anomali Beban

Tabel 1 menyajikan rangkuman hasil perhitungan parameter kinerja dari kedua lantai. Data menunjukkan anomali yang signifikan, di mana beban lalu lintas di jam senggang secara tak terduga lebih tinggi daripada jam sibuk pada beberapa parameter. Anomali paling ekstrem terlihat pada Lantai 9, di mana *Packet Rate* (PPS) saat Jam Senggang (775 pps) tercatat lebih dari tiga kali lipat lebih tinggi dibandingkan Jam Sibuk (225 pps). Sebaliknya, PPS di Lantai 8 relatif stabil antara kedua kondisi.

TABEL 2
(A)

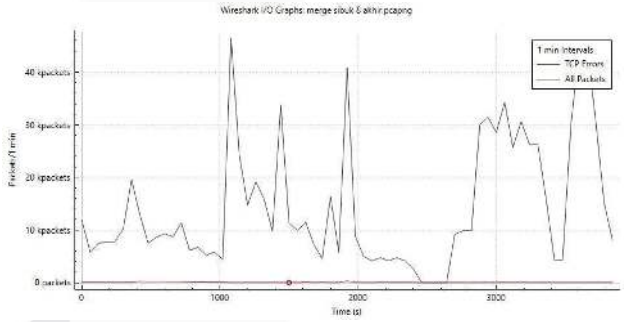
Lokasi	Kondisi	Rata-rata Inter-Arrival Time (detik/paket)	Rata-rata Packet Rate (pps)
Lantai 8	Sibuk	0,004278312	260,905
	Senggang	0,004013255	258,691
Lantai 9	Sibuk	0,004570294	225,422
	Senggang	0,001161591	775,264

B. Pembahasan dan Identifikasi Risiko

Visualisasi *I/O Graphs* memberikan konteks untuk memahami anomali pada Tabel 1.

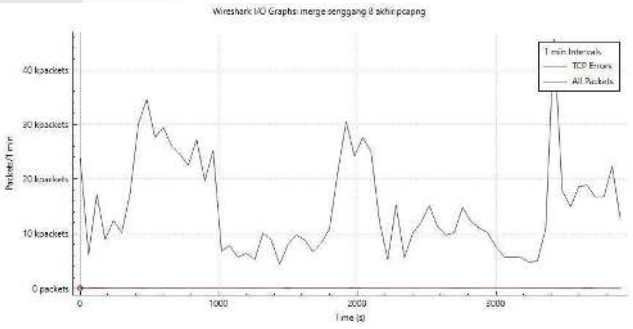
1. Lantai 8: Risiko Keterbatasan Fisik. Pada jam sibuk, jaringan Lantai 8 menunjukkan beberapa *traffic burst* yang berkorelasi langsung dengan munculnya *TCP Errors*.

GAMBAR 2
(A)



Sebaliknya, pada jam senggang, meskipun juga terjadi *burst*, tidak ada *TCP Errors* yang terdeteksi sama sekali.

GAMBAR 3
(B)



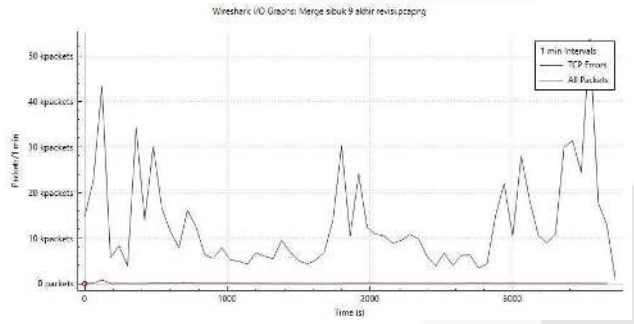
Kombinasi dari berbagai temuan yang diperoleh selama analisis mengarah pada satu kesimpulan yang spesifik: risiko utama yang dihadapi oleh jaringan di Lantai 8 adalah penurunan stabilitas akibat keterbatasan *buffer* pada

perangkat keras, yang membuatnya tidak mampu menyerap lonjakan *paket* sesaat saat jaringan sedang sibuk. Kesimpulan ini ditarik dari beberapa bukti yang saling menguatkan. Data kuantitatif rata-rata, terutama *Packet Rate* (PPS), pada awalnya menunjukkan bahwa jaringan beroperasi jauh di bawah kapasitasnya dan terlihat stabil. Namun, bukti visual dari *I/O Graphs* menyajikan cerita yang berbeda, dengan secara jelas menampilkan adanya *traffic burst* yang sangat intens dan terjadi secara periodik. Bukti paling krusial adalah munculnya *TCP Errors* yang signifikan dan hanya terjadi pada saat-saat lonjakan *burst* tersebut, menunjukkan korelasi temporal yang sangat kuat antara beban kejut sesaat dengan kegagalan pada level protokol.

Dengan menghubungkan bukti-bukti tersebut, kita dapat mendiagnosis akar masalahnya. Korelasi yang kuat membuktikan bahwa masalahnya bukan pada beban rata-rata, melainkan pada ketidakmampuan infrastruktur menangani "banjir" *paket* dalam waktu yang sangat singkat. Fenomena ini adalah gejala klasik dari *buffer overflow*, di mana memori antrean (*buffer*) pada *switch* terisi penuh oleh lonjakan *paket*, sehingga *paket-paket* baru yang datang terpaksa dibuang (*dropped*). *Packet loss* inilah yang kemudian memicu mekanisme pengiriman ulang pada protokol TCP, yang akhirnya tercatat sebagai *TCP Errors* oleh Wireshark. Bagi pengguna akhir, keterbatasan fisik ini bermanifestasi secara nyata dalam bentuk degradasi kualitas layanan, seperti peningkatan latensi dan respons aplikasi yang melambat selama periode aktivitas tinggi.

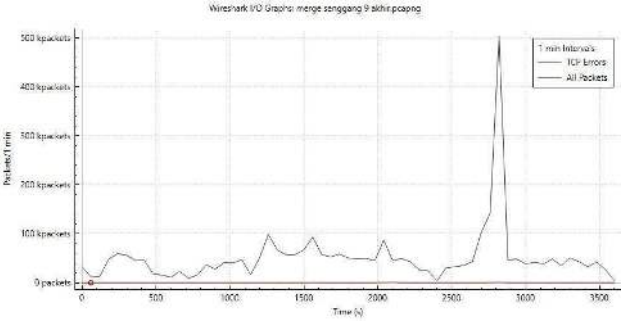
2. Lantai 9: Risiko Operasional. Jaringan Lantai 9 menunjukkan resiliensi yang superior. Selama jam sibuk, jaringan mampu menangani *burst* ekstrem tanpa *error*.

GAMBAR 3
(A)



Yang paling signifikan, saat jam senggang terjadi "*super-burst*" anomali yang puncaknya melebihi 500 kpackets/menit, namun jaringan tetap stabil tanpa satu pun *TCP Errors*.

GAMBAR 4
(B)



Ketiadaan *TCP errors* secara absolut di Lantai 9, bahkan saat menghadapi *traffic burst* ekstrem, membuktikan bahwa infrastruktur jaringan di sana sangat tangguh dan memiliki kapasitas yang besar (*over-provisioned*). Baik selama lonjakan akibat aktivitas pengguna di jam sibuk maupun saat dihantam "*super-burst*" anomali di jam senggang, jaringan tidak menunjukkan tanda-tanda kegagalan pada lapisan TCP. Hal ini menegaskan bahwa dari perspektif perangkat keras, jaringan ini dirancang dengan sangat baik dan mampu menangani beban jauh di atas kebutuhan normal sehari-hari.

Namun, di balik ketangguhan ini, data lalu lintas mengungkap adanya risiko operasional yang signifikan. Anomali di mana *Packet Rate* pada jam senggang lebih dari tiga kali lipat lebih tinggi dari jam sibuk menunjukkan bahwa beban puncak sesungguhnya berasal dari proses sistem otomatis yang sangat intensif dan tidak terkelola dengan baik. Risiko ini bersifat manajerial: jika proses masif ini (seperti *backup* data) keliru dijadwalkan dan berjalan pada jam kerja, ia berpotensi mengganggu layanan utama. Selain itu, fenomena ini dapat menyebabkan perencanaan kapasitas di masa depan menjadi tidak akurat jika hanya mengandalkan data jam sibuk sebagai acuan.

C. Implikasi dan Penelitian Selanjutnya

Temuan ini berimplikasi bahwa setiap segmen jaringan memiliki profil risiko unik yang tidak terlihat dari monitoring umum. Untuk pengembangan ke depan, disarankan beberapa langkah. Bagi pengelola jaringan, perlu dilakukan investigasi untuk mengkonfirmasi keterbatasan *buffer* di Lantai 8 dan mengidentifikasi serta menjadwalkan ulang proses otomatis di Lantai 9. Bagi peneliti selanjutnya, penelitian dapat diperluas dengan menganalisis lalu lintas berdasarkan aplikasi spesifik atau mengkorelasikan temuan teknis dengan survei persepsi kualitas koneksi dari pengguna.

V. KESIMPULAN

Berdasarkan analisis data dan pembahasan yang telah dilaksanakan, penelitian ini berhasil menarik beberapa kesimpulan penting. Kontribusi utama dari penelitian ini adalah keberhasilannya dalam menunjukkan bahwa analisis tingkat *paket* mampu mengungkap dan membedakan profil risiko kinerja jaringan yang fundamental berbeda, yang tidak terdeteksi oleh sistem pemantauan umum.

Pertama, ditemukan adanya variasi karakteristik lalu lintas yang signifikan dan kontra-intuitif. Secara spesifik pada Lantai 9, beban jaringan sesungguhnya, yang diukur melalui *Packet Rate* (PPS), justru terjadi pada jam senggang dengan nilai lebih dari tiga kali lipat dibandingkan jam sibuk. Hal ini membuktikan bahwa beban dominan pada segmen jaringan tersebut tidak didorong oleh aktivitas pengguna interaktif, melainkan oleh proses sistem otomatis non-interaktif.

Kedua, teridentifikasi adanya risiko keterbatasan fisik pada jaringan Lantai 8. Risiko ini bermanifestasi sebagai penurunan stabilitas saat jaringan berada di bawah tekanan beban puncak di jam sibuk. Bukti utamanya adalah munculnya *TCP Errors* yang berkorelasi langsung dengan lonjakan lalu lintas (*traffic burst*), yang mengindikasikan bahwa kapasitas *buffer* pada perangkat keras kemungkinan besar tidak memadai untuk menyerap beban kejut sesaat.

Ketiga, teridentifikasi adanya risiko operasional pada jaringan Lantai 9. Meskipun infrastrukturnya terbukti sangat tangguh karena mampu menangani *super-burst* anomali tanpa *error*, keberadaan beban masif yang tidak terkelola dari proses otomatis ini menjadi risiko tersendiri. Hal ini dapat mengganggu layanan lain jika jadwalnya keliru dan menyebabkan perencanaan kapasitas di masa depan menjadi tidak akurat.

Pada akhirnya, kesimpulan ini menegaskan bahwa untuk manajemen jaringan yang efektif, diagnosis mendalam yang spesifik untuk setiap segmen jaringan adalah suatu keharusan, karena setiap segmen dapat memiliki tantangan dan profil risiko yang unik.

REFERENSI

[1] L. A. Kolinug, T. K. Sendow, F. Jansen, and M. R. E. Manoppo, "ANALISA KINERJA JARINGAN JALAN DALAM KAMPUS UNIVERSITAS SAM RATULANGI," Jurnal Ilmiah Media Engineering, vol. 3, no. 2, 2013.

[2] A. Pradana, I. R. Widiasari, and R. Efendi, "Implementasi Sistem Monitoring Jaringan Menggunakan Zabbix Berbasis SNMP," AITI, vol. 19, no. 2, pp. 248–262, 2022.

[3] R. Rosalina, R. B. Huwae, D. Ratnasari, A. H. Jatmika, and I. G. P. W. W. Wirawan, "Implementasi Sistem Monitoring Jaringan Menggunakan Zabbix Berbasis SNMP pada UPT Pusat Teknologi Informasi dan Komputer (PUSTIK) Universitas Mataram," Jurnal Begawe Teknologi Informasi (JBegaTI), vol. 5, no. 1, pp. 115–125, 2024.

[4] P. F. Malik and B. P. Josaphat, "Desain dan Implementasi Sistem Monitoring Jaringan Menggunakan Zabbix dan Telegram," in Seminar Nasional Official Statistics, 2024, vol. 2024, no. 1, pp. 711–722.

[5] A. R. Marsa, "Analisis Kinerja Jaringan Internet Menggunakan Mikrotik dengan Backbone Fiber Optik dengan Metode QoS," unpublished.

[6] A. Z. Nusri and R. Erwin Syah, "Analisis Trafik Jaringan Menggunakan Wireshark Untuk Meningkatkan Kinerja Jaringan Pada Smk 3 Soppeng," Jurnal Ilmiah Sistem Informasi dan Teknik Informatika (JISTI), vol. 8, no. 1, pp. 114–122, 2025.

[7] I. Ubaedila, O. Nurdiawan, Y. A. Wijaya, and J. Sidik, "Layanan Jaringan Menggunakan Metode Sniffing Berbasis Wireshark," INFORMATICS FOR EDUCATORS AND PROFESSIONAL : Journal of Informatics, vol. 6, no. 1, p. 95, 2022.

[8] Y. Delvika, "SISTEM INFORMASI MANAJEMEN PERSEDIAAN SUKU CADANG PADA PERUSAHAAN PENYEWAAN KENDARAAN," Jurnal Sistem Teknik Industri, vol. 18, no. 2, pp. 84–89, 2018.

[9] E. Garsva, N. Paulauskas, G. Grazulevicius, and L. Gulbinovic, "Packet Inter-arrival Time Distribution in Academic Computer Network," Electronics and Electrical Engineering, vol. 20, no. 3, pp. 87–90, 2014.

[10] H. Ghasemirahni, A. Farshin, M. Scazzariello, G. Q. Maguire, D. Kostić, and M. Chiesa, "FAJITA: Stateful Packet Processing at 100 Million pps," Proceedings of the ACM on Networking, vol. 2, no. CoNEXT3, pp. 1–22, 2024.

[11] R. Tuli, "Analyzing Network Performance Parameters using Wireshark," International Journal of Network Security & Its Applications, vol. 15, no. 01, pp. 01–13, 2023.

[12] G. Jain and Anubha, "Application of SNORT and Wireshark in Network Traffic Analysis," IOP Conference Series: Materials Science and Engineering, vol. 1119, no. 1, p. 012007, 2021.