ANALISIS DETEKSI GANGGUAN JARINGAN DENGAN SISTEM MONITORING BERBASIS SNMP : INTEGRASI NOTIFIKASI TELEGRAM MENGGUNAKAN ZABBIX

1st Nabilla Noor Rizqi
Fakultas Rekayasa Industri
Telkom University
Bandung, Indonesia
nabillanr@student.telkomuniversity.ac.id

2nd Rd. Rohmat Saedudin S.T., M.T., Ph.D.
Fakultas Rekayasa Industri
Telkom University
Bandung, Indonesia
rdrohmat@telkomuniversity.ac.id

3rd Umar Yunan Kurnia Septo Hediyanto, S.T., M.T.
Fakultas Rekayasa Industri
Telkom University
Bandung, Indonesia
umaryunan@student.telkomuniversity.ac.id

***Abstrak* — Dalam lingkungan institusi pendidikan tinggi, kebutuhan terhadap sistem jaringan yang andal dan responsif menjadi sangat penting seiring meningkatnya penggunaan layanan digital. Penelitian ini bertujuan untuk menganalisis efektivitas sistem monitoring jaringan berbasis SNMP (Simple Network Management Protocol) dengan integrasi notifikasi real-time melalui Telegram menggunakan tools Zabbix. Metode yang digunakan adalah PPDIOO (Prepare, Plan, Design, Implement, Operate, Optimize) yang mencakup perencanaan, desain, implementasi, hingga optimalisasi sistem monitoring pada perangkat jaringan di Gedung TULT Universitas Telkom. Objek pemantauan meliputi perangkat komputer laboratorium dan laptop pribadi, dengan parameter utama berupa status interface, penggunaan memori, dan respons ping. Hasil pengujian menunjukkan bahwa sistem mampu mendeteksi gangguan seperti link down, penggunaan memori tinggi, dan restart perangkat, serta memberikan notifikasi ke Telegram dengan jeda waktu 1–5 menit. Namun, keterbatasan dalam akses OID perangkat switch menghambat pemantauan secara menyeluruh pada perangkat inti. Kesimpulannya, sistem monitoring berbasis SNMP menggunakan Zabbix memberikan kontribusi positif terhadap kecepatan deteksi gangguan jaringan dan meningkatkan efisiensi manajemen jaringan, terutama pada perangkat endpoint. Saran diberikan untuk peningkatan kapabilitas pemantauan melalui integrasi MIB dan pengujian skenario gangguan aktif.**

Kata kunci*— *Zabbix, Simple Network Management Protocols, Monitoring Jaringan, Manajemen Keamanan Jaringan, Notifikasi Telegram.

I. PENDAHULUAN

Sejauh ini, Simp*le Network Management Protocol (SNMP)* termasuk salah satu pendekatan yang paling populer untuk mengelola kinerja jaringan. Yang mana akan memudahkan dalam pengumpulan data terkait performa, konfigurasi, maupun tingkat keamanannya. Meskipun penggunaan SNMP dapat mengoptimalkan kinerja jaringan, namun penggunaan protokol tersebut masih terdapat beberapa kekurangan dalam hal *response time*. Hal ini disebabkan oleh faktor seperti interval pengambilan data yang memiliki volume besar dan cenderung lebih lambat. Sehingga dampaknya akan mengakibatkan terjadinya downtime pada kinerja operasional.

Dengan adanya penelitian ini, pemanfaatan protokol SNMP memungkinkan proses monitoring dengan baik, dari segi manajemen keamanan jaringannya. Dengan demikian, penelitian ini akan ditujukan untuk menganalisis implementasi SNMP sebagai sistem monitoring jaringan yang berfokus pada pemantauan/peningkatan guna menangani persoalan gangguan dalam pemantauan jaringan.

II. KAJIAN TEORI

A. Simple Network Management Protocols

Simple Network Management Protocol (SNMP) adalah sebuah sistem protokol yang didesain sedemikian rupa untuk memberikan akses pengelolaan jaringan komputer kepada pemakai dari jarak jauh atau biasa disebut dengan *remote*.

B. Zabbix

Zabbix merupakan software yang bersifat *open-source* dan digunakan sebagai pelaksanaan monitoring pada jaringan, server, aplikasi, dan layanan secara *real-time*. Selain itu, melalui Zabbix administrator dapat mengetahui status server dan jaringan dengan mudah serta menerima pemberitahuan jika terjadi masalah (Cahyo et al., 2020).

C. Alert atau Notifikasi

Alert atau notifikasi merupakan pemberitahuan terkait informasi yang disajikan dalam *pop-up* dari media yang telah dihubungkan melalui software Zabbix. Media type tersedia dalam perangkat lunak tersebut terdiri dari *Brevis.one, Discord, Email, Github, Gmail, Sms, Telegram* dan lain sebagainya. Dengan adanya integrasi pihak ketiga yang terhubung ke Zabbix, maka pengguna dapat memperoleh informasi penting terkait notifikasi berupa gangguan-gangguan yang terdeteksi oleh sistem Zabbix.

D. Manajemen Jaringan

Manajemen jaringan berkaitan dengan proses menjaga jaringan supaya tetap stabil dan berjalan dengan baik (Khasanah & Utami, 2018). Biasanya dalam proses manajemen jaringan ini mencakup pengawasan jaringan yang berperan untuk mengetahui setiap permasalahan yang muncul.

E. Keamanan Jaringan

Keamanan jaringan berfungsi untuk meminimalisir resiko yang tidak diinginkan pada sebuah jaringan computer. Baik itu berupa bentuk ancaman fisik maupun logik. Pada umumnya, prinsip keamanan jaringan disebut dengan CIA *(Confidentiality, Integrity, Availability)*

F. Jaringan Komputer

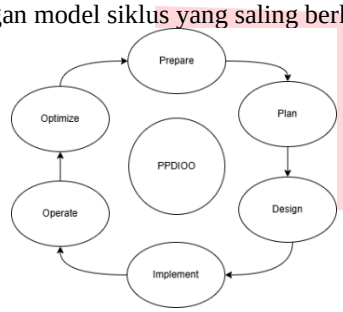
Jaringan komputer merupakan sistem yang terdiri dari sejumlah komputer yang saling terhubung dengan tujuan

saling bertukar data dan sumber daya (Doni, 2016). Jaringan dibentuk melalui media komunikasi, baik kabel maupun nirkabel, untuk mendukung berbagai aktivitas operasional seperti komunikasi, pertukaran data hingga pengelolaan sistem informasi.

III. METODE

A. Metode PPDIOO

Dalam penelitian ini menggunakan metode atau metodologi PPDIOO untuk mendukung sistem monitoring berbasis SNMP menggunakan tools Zabbix. Metode ini diperkenalkan oleh cisco dengan beberapa tahapan yang terdiri dari prepare, plan design, implement, operate, dan optimize. Setiap tahapan dalam metode ini meemberikan penjelasan dengan model siklus yang saling berkaitan.



Gambar III. 1 Metode PPDIOO

1. PREPARE

Tahapan ini merupakan tahapan persiapan dengan tujuan dapat mengetahui latar belakang dari masalah yang ada. Selain itu juga mencakup identifikasi kebutuhan awal yang diperlukan.

2. PLAN

Tahap plan merupakan tahapan perancangan dengan menghasilkan blueprint teknis yang akan menjadi dasar dalam perancangan sistem. Selain itu, pada tahap ini juga mencakup rencana terhadap perangkat yang digunakan.

Tabel III. 1 Perancangan Perangkat

Perangkat	Windows OS 11 Computer PC Lab 8 PC Lab 9
Perangkat yang dimonitoring	Switch Lantai 8 dan 9 TULT
Media Penyimpanan	Google Drive 100Gb, Hard Disk
Perangkat Lunak	Zabbix Appliance, Hyper-V, dan Telegram Desktop

3. DESIGN

Pada tahap design ini mencakup pengembangan arsitektur teknis jaringan secara menyeluruh, termasuk dalam gambaran topologi, arsitektur sistem dan lainnya.

4. IMPLEMENT

Tahap implement yaitu proses pelaksanaan dari tahap desain kedalam bentuk nyata. Setiap langkah dalam implementasi harus menyertakan deskripsi, rincian pedoman pelaksanaan, perkiraan waktu untuk penerapan dan informasi lainnya sebagai informasti tambahan.

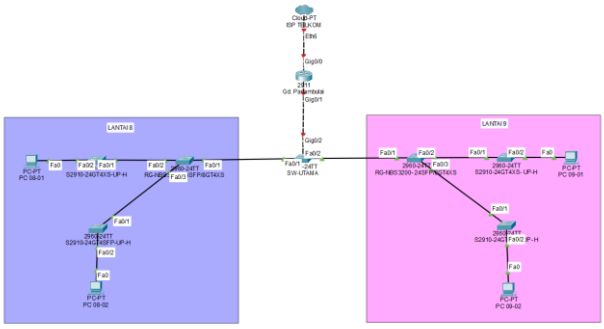
5. OPERATE

Tahap operate merupakan tahapan dimana sistem jaringan yang telah di implementasikan berhasil dijalankan dan dipantau. Melalui penelitian yang berjalan dengan baik, data kemudian dikumpulkan dan dilakukannya pemantauan kondisi jaringan.

6. OPTIMIZE

Tahap akhir ini merupakan tahapan yang ditujukan untuk melakukan evaluasi performa jaringan serta meningkatkan efektivitas sistem.

B. Topologi Jaringan



Gambar III. 2 Topologi Jaringan

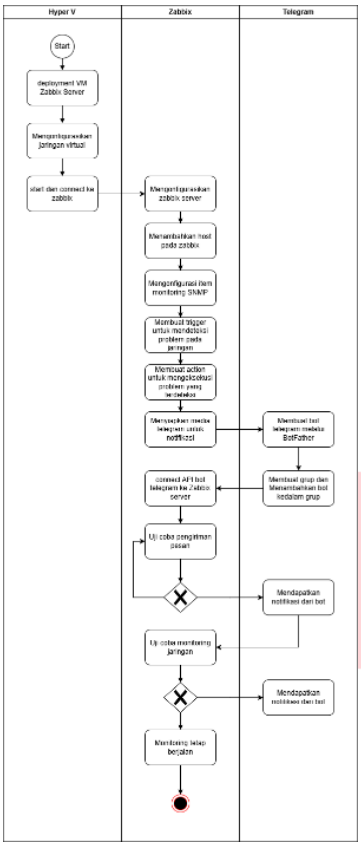
Topologi jaringan diatas menggambarkan rancangan struktur monitoring yang diterapkan pada lantai 8 dan lantai 9 di Gedung TULT, Universitas Telkom. Topologi ini dirancang untuk mendukung pemantauan jaringan secara *real-time* menggunakan aplikasi Zabbix yang terintegrasi dengan protokol SNMP.

Secara keseluruhan, topologi ini menggambarkan implementasi sistem monitoring yang terintegrasi, mencakup pemantauan pada level distribusi dan akses di lingkungan kampus. Selain itu, mendukung keberlangsungan layanan jaringan, rancangan ini juga menjadi fondasi untuk pengembangan sistem manajemen jaringan yang lebih cerdas dan proaktif, sesuai dengan kebutuhan operasional dan keamanan infrastruktur IT di lingkungan kampus.

IV. HASIL DAN PEMBAHASAN

A. Cara kerja integrasi Zabbix dengan telegram

Agar sistem monitoring yang dibangun mampu memberikan notifikasi secara real-time kepada administrator jaringan, diperlukan integrasi antara Zabbix dengan aplikasi pihak ketiga yang mendukung, yaitu telegram. Melalui penelitian ini, melalui fitur bot pada telegram dapat mendukung otomatisasi notifikasi informasi yang dikirimkan oleh Zabbix melalui API token Bot Telegram. Dengan penggambaran flowchart sebagai berikut:



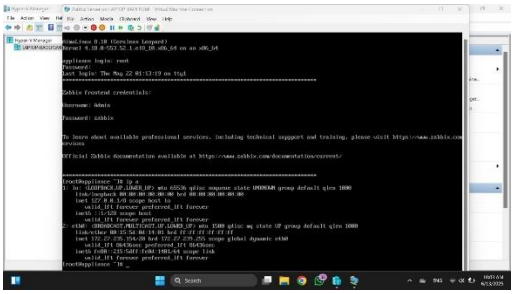
Gambar IV. 1 Flowchart Alur Kerja Integrasi Zabbix dengan Telegram

Dengan penjelasan alur kerja sistem monitoring yang terintegrasi dari Zabbix ke Telegram selama kurun waktu 5 hari adalah sebagai berikut:

1. zabbix perlu dikonfigurasikan terlebih dahulu dengan mulai menyalakan *virtual machine* dan mengoneksikannya.

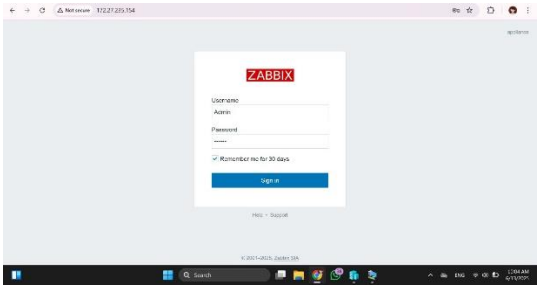
Gambar IV. 2 Konfigurasi VM Zabbix

2. Untuk mengetahui alamat ip Zabbix web bisa dilakukan dengan command ip a, Zabbix secara otomatis akan memberikan ip address untuk masuk ke halaman websitenya.



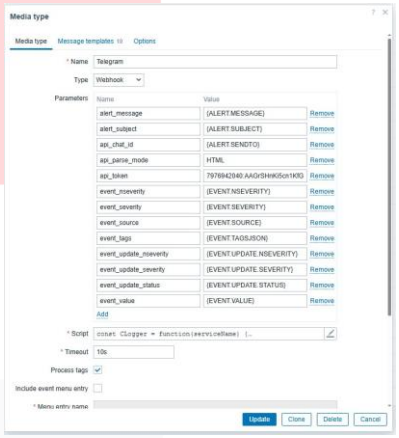
Gambar IV. 3 Ip Address Zabbix

3. User akan diarahkan ke halaman *login* dengan *username* dan *password*



Gambar IV. 4 Zabbix Webpage

4. *User* juga perlu menyiapkan media berupa aplikasi Telegram untuk memberikan notifikasi/*alert*.



Gambar IV. 5 Zabbix Media Type

5. Kemudian membuat grup sebagai platform untuk alert Zabbix dengan menambahkan @ZabbixBot.

Gambar IV. 6 Grup Notifikasi Zabbid di Telegram

6. Setelah itu, mengkoneksikan API bot Telegram pada Zabbix server dan menguji coba pengiriman pesan informasi untuk melakukan testing apakah bot berhasil terkoneksi dengan baik.

Gambar IV. 7 Notification Testing

7. Apabila sistem mendeteksi adanya permasalahan pada jaringan, zabbix akan mengirimkan pesan secara otomatis melalui telegram yang sudah disambungkan sebelumnya. Apabila tidak terdeteksi permasalahan atau gangguan, pemantauan jaringan tetap berlangsung hingga durasi yang ditetapkan selesai.

Gambar IV. 8 Hasil Testing Notifikasi

B. Kriteria severity

Pada implementasi sistem monitoring jaringan dengan tools Zabbix, diperlukan klasifikasi tingkat keparahan/level severity untuk setiap kondisi gangguan yang terdeteksi. Adapun kriteria severity yang digunakan dalam penelitian ini dijabarkan pada table berikut:

Tabel IV. 1 Kriteria Severity

No.	Level Severity	Deskripsi
1.	Not classified	Status interface dikatakan normal atau belum dikategorikan sebagai gangguan.
2.	Information	Informasi awal terkait perubahan kecil atau status monitoring jaringan.
3.	Warning	Indikasi awal yang dikatakan sebagai potensi gangguan.
4.	Average	Gangguan sedang yang berdampak pada koneksi terbatas.
5.	High	Gangguan besar yang dikatakan sebagai ancaman dan bisa berdampak pada lebih dari satu layanan atau lebih.
6.	Disaster	Gangguan kritis yang dapat menyebabkan jaringan utama tidak berfungsi bahkan dapat merugikan layanan tersebut jika tidak segera diatasi.

C. Pola gangguan yang terjadi

Berdasarkan hasil monitoring yang dilakukan pada beberapa perangkat khususnya penggunaan laptop pribadi, PC Lab Integra R3, dan PC Lab Integra R5, serta perangkat jaringan yang terhubung yaitu switch lantai 8 dan lantai 9 melalui server Zabbix. Dengan beberapa jenis gangguan yang teridentifikasi sebagai berikut:

Jenis Gangguan	Jumlah Kejadian	Frekuensi	Severity	Perangkat yang Dominan Terjadi	Analisis	Implikasi Teknis
Penurunan kecepatan *interface ethernet*	> 100	Sangat sering	*Information*	Laptop	Kecepatan turun drastic dari 10-45 Mbps, terjadi pada bridge adapter laptop. Sering terjadi umumnya pada penggunaan laptop pribadi, disebabkan karena konfigurasi *bridge* yang tidak optimal atau *link ethernet* mengalami renegosiasi ke kecepatan yang lebih rendah.	Gangguan ringan namun sering menandakan indikasi koneksi tidak stabil.
Link down pada *interface ethernet* atau Wi-Fi	5	Cukup sering	*Average*	PC Lab Integra R3, dan R5	Koneksi pada interface jaringan terputus total yang terjadi pada Wi-Fi dan *Ethernet*. Sering terjadi pada PC lab, khususnya pada R3 yang tiba-tiba hilang koneksi.	Koneksi jaringan bisa terputus dan perangkat tidak bisa diakses.
High memory utilization (>90%)	10	Sering	*Average*	Laptop	Pemakaian RAM melebihi 90%, dan yang tertinggi diangka 93,25%. Hal ini berdampak pada performa saat monitoring aktif. Umumnya sering terjadi pada laptop pribadi, namun pada PC Lab Integra R3 juga sempat mengalami permasalahan dari *memory utilization*.	Respon dari sistem menurun, dan laptop menjadi lambat.
High disk read/write latency (read/write > 20 ms)	1	Jarang	*Warning*	Zabbix Server (Pc Lab Integra R3)	*Disk response time* > 20ms selama 15 menit. Terjadi sekali pada PC Lab.	Ada potensi delay pencatatan log dan notifikasi.
ICMP response time tinggi (> 190ms)	1	Jarang	*Warning*	Switch Lantai 8	Waktu respon ping mencapai 190 ms pada jam sibuk, namun selang waktu 3 menit kembali normal. Sempat terjadi diawal percobaan monitoring, tepatnya pada Switch lantai 8.	Latensi tinggi dan adanya potensi bottleneck jaringan.
System name change (name:NULL)	6	Cukup sering	*Information*	Switch Lantai 8 dan Lantai 9	Nama sistem switch yang berubah menjadi NULL atau default menandakan SNMP gagal membaca system name, atau switch reset. Terkadang muncul pada switch lantai 8 dan 9.	Sulit mengidentifikasikan perangkat yang terdapat gangguan identifikasi log.
Restarting Zabbix server	3	Kadang	*Warning*	Zabbix Server (PC Lab Integra R3 dan Laptop)	Restart Zabbix yang terdeteksi dengan uptime <10 menit. Sempat terjadi ketika awal pelaksanaan monitoring.	Monitoring *delay* atau berhenti sesaat, ada potensi beberapa data tidak tercatat.

Gambar IV. 9 Pola Gangguan yang terjadi

Secara keseluruhan, pola gangguan yang ditemukan dalam penelitian ini tidak hanya berhasil diidentifikasikan melalui sistem monitoring menggunakan Zabbix, tetapi juga memberikan bukti yang nyata mengenai peran strategis monitoring jaringan dalam mendeteksi gangguan awal, menganalisis permasalahan dan juga mengantisipasi dampaknya.

D. Responsivitas sistem monitoring

Hasil responsivitas sistem monitoring juga memicu kemampuan yang dihasilkan sistem dalam mendeteksi dan mengirimkan informasi terkait gangguan yang terjadi secara cepat dan akurat.

1. Kecepatan deteksi gangguan

Beberapa kondisi yang terjadi membuktikan bahwa gangguan berupa pemakaian memori tinggi (>90%) pada perangkat laptop pribadi dan PC lab berhasil terdeteksi oleh Zabbix secara cepat. Dengan catatan sekitar 30-60 detik, dan status berubah menjadi *resolved* dalam kurun waktu 5-10 menit. Selain itu, gangguan yang disebabkan karena *link down* pada beberapa interface di PC lab Integra R3 dan R5 terhitung hanya dalam beberapa detik setelah kondisi terdeteksi, meskipun tidak semua gangguan

berhasil diselesaikan *(resolved)*, karena gangguan tersebut tercatat belum membaik setelah pengamatan.

Pada aspek ini, sejalan dengan penelitian dari (Huda, 2024) dan (Saputra et al., n.d.), yang menemukan bahwa sistem monitoring menggunakan Zabbix mampu merespons secara otomatis terhadap parameter jaringan seperti *interface status*, utilisasi memori dan *uptime* perangkat. Kecepatan yang terdeteksi ini diperoleh karena Zabbix menggunakan sistem *active check* dan *triggers* yang dapat memberikan deteksi secara *real-time*. Dalam konteks ini juga didukung berdasarkan teori dari buku yang diterbitkan oleh (Olups, 2016), Zabbix network monitoring yang membahas bahwa sistem monitoring yang efektif dan terukur harus mampu melakukan *threshold-based* alerting untuk menghindari keterlambatan dalam proses mitigasi gangguan.

2. Pengiriman notifikasi real-time

Pada aspek pengiriman notifikasi secara *real-time*, integrasi antara Zabbix dengan Telegram terbukti memberikan jalur komunikasi yang cepat dan stabil dalam menyampaikan informasi kepada administrator. Hal ini membuktikan bahwa sistem dapat digunakan sebagai alat *early warning* yang efektif. Berdasarkan penelitian terdahulu yang dapat memperkuat penelitian ini yaitu hasil penelitian dari (Ichsan Mustafid et al., 2022) yang menyatakan bahwa penggunaan Telegram sebagai media notifikasi dalam sistem monitoring dapat memberikan informasi secara langsung kepada teknisi jaringan dalam waktu nyaris *real-time*. Disisi lain, (Khongsong, 2023) juga menekankan pentingnya penggunaan jalur komunikasi yang ringan dan cepat seperti Telegram untuk mendukung respons teknis dengan cepat terhadap insiden gangguan jaringan.

Secara keseluruhan, sistem Zabbix terbukti responsive dan andal dalam mendeteksi berbagai jenis gangguan secara real-time, dan notifikasi yang dikirimkan sangat cepat. Namun, untuk optimalisasi lebih lanjut akan lebih efektif jika dilenhkapi dengan peraturan trigger recovery yang lebih spesifik.

E. Stabilitas perangkat dan jaringan

Stabilitas perangkat dan jaringan merupakan salah satu aspek yang cukup penting dalam proses penjagaan kontinuitas layanan dan kinerja sistem.

Tabel IV. 2 Stabilitas Perangkat Jaringan

Jenis Perangkat	Keterangan	Stabilitas Perangkat
Laptop	Pada stabilitas laptop pribadi tercatat menunjukkan notifikasi tertinggi dibandingkan perangkat yang lain. Gangguan yang umumnya terjadi antara lain terkait penurunan kecepatan interface ethernet misalnya dari 80Mbs hingga 45Mbps, penggunaan memori fisik yang melebihi 90% selama lebih dari 5 menit, dan interface link down yang sering terjadi pada interface Wi-Fi. Meskipun sifat gangguannya cenderung ringan, namun frekuensi tinggi dan pola berulang menunjukkan ketidakstabilan performa.	Kurang stabil
Perangkat Jaringan	Pada switch lantai 8 dan 9 menunjukkan performa yang lebih stabil dan baik selama periode monitoring berlangsung. Meskipun terdapat gangguan berupa ICMP ping time tinggi, namun gangguan tersebut hanya terjadi sekali dan tidak menyebabkan link down atau gangguan besar pada konektivitas jaringan. Hal ini membuktikan badhwa perangkat jaringan bekerja dengan stabil dan lebih tahan terhadap fluktuasi dibandingkan perangkat endpoint seperti laptop atau PC lab.	Stabil
PC Lab Integra	PC yang digunakan pada Integra R3 dan R5 memiliki performa yang berbeda. PC pada integra R5 memiliki performa yang lebih baik dan tercatat yang paling minim dalam mengalami gangguan dibandingkan dengan PC yang berada di integra R3. Meskipun terdeteksi adanya gangguan seperti link down, dan beberapa gangguan yang belum terselesaikan (not resolved), namun PC lab integra R5 terdeteksi lebih stabil. Sedangkan PC lab integra R3 rentan terhadap beban kerja yang tinggi bahkan terkadang koneksinya tidak stabil.	Stabil, karena performa PC lebih baik dibandingkan dengan perangkat pribadi.

F. Pengaruh sistem monitoring terhadap operasional perangkat di Gedung TULT

Selama periode monitoring berlangsung, sistem berhasil mendeteksi lebih dari 100 kejadian penurunan kecepatan *interface ethernet*, 10 kejadian high memory utilization, dan 5 kejadian *link down* yang terdeteksi dalam notifikasi Telegram secara otomatis. Notifikasi yang dikirimkan dalam waktu rata-rata 30 hingga 60 detik setelah gangguan terdeteksi. Bukti ini menunjukkan bahwa sistem memiliki tingkat responsivitas tinggi dalam operasional jaringan. Respon ini sejalan dengan penelitian (Huda, 2024) dan (Ichsan Mustafid et al., 2022) yang menyatakan bahwa sistem monitoring dengan Zabbix memberikan keuntungan dalam deteksi secara cepat dan penanganan insiden jaringan secara otomatis. Selain aspek mengenai deteksi gangguan, sistem monitoring ini juga terbukti dalam pengambilan keputusan teknis yang tepat sasaran.

Dalam kerangka teoritis, (Academy, 2020) menyatakan bahwa sistem monitoring yang efektif memungkinkan pengambilan keputusan berbasis data *(data driven decision making)*, yaitu semua Tindakan teknis didasari dengan kondisi aktual sistem, bukan hanya asumsi.

G. Solusi

Melalui hasil analisis yang telah dijelaskan dan berdasarkan gangguan yang terdeteksi setelah pelaksanaan

monitoring secara langsung, maka dapat dirancang beberapa solusi secara spesifik terhadap masing-masing pola gangguan dengan mengacu pada standar dan teori jaringan yang relevan. Berikut merupakan solusi dari beberapa gangguan yang telah ditemukan:

1. Apabila terjadi gangguan berupa penurunan kecepatan pada *interface ethernet*, solusinya yaitu memastikan bahwa perangkat dalam jangakauan yang optimal dari *access point*, hal ini didukung oleh (Academy, 2020) yang menyarankan penempatan *access point* dalam radius maksimum 10-15 meter untuk sinyal stabil.
2. Mengupgrade RAM perangkat, atau menjalankan Zabbix *frontend* di server terpisah agar tidak terjadi *error system configuration*. Hal ini dibuktikan pada saat pelaksanaan instalasi dan konfigurasi perangkat secara langsung.
3. Melakukan pengecekan pada fisik kabel atau port koneksi ketika terjadi gangguan berupa link *down*. Hal ini didukung dengan standar Zabbix *documentation* (SIA, 2025) yang merekomendasikan untuk mengaktifkan agent ping agar dapat mendeteksi dengan cepat.
4. Melakukan pemisahan sistem database monitoring kedalam penyimpanan SSD yang lebih memiliki kinerja yang baik. Menurut (Vacche & Lee, 2015), performa Zabbix dapat ditingkatkan dengan memisahkan layanan frontend dengan backend serta menggunakan penyimpanan dengan ukuran lebih besar untuk data historis.
5. Terkait gangguan ICMP respons time tinggi, solusinya yaitu dengan memantau beban lalu lintas jaringan secara spesifik untuk melihat trafik per port, dengan demikian *broadcast* menjadi lebih terkontrol dan menghindari kemacetan trafik. Hal ini didukung dengan (Kurose & Ross, 2017) yang menjelaskan bahwa pembagian beban dan segmentasi jaringan dapat mengurangi latensi serta meningkatkan efisiensi distribusi data.
6. Memperbarui firmware perangkat dan menetapkan identifier statis (custom name) untuk permasalahan pada pembacaan SNMP seperti *system name changed* NULL. Hal ini sejalan dengan (SIA, 2020) yang menyarankan pembuatan *makro fallback* untuk menghindari hilangnya identifikasi perangkat ketika system name tidak terbaca.
7. Menghindari multitasking yang berat di perangkat yang sama ketika terjadi gangguan seperti restarting Zabbix server. Hal ini dibuktikan ketika penelitian secara langsung.

Secara keseluruhan, solusi teknis tersebut didukung tidak hanya berdasarkan hasil temuan, tetapi juga didukung oleh teori dan penelitian terdahulu dari berbagai literatur. Dengan diimplementasikannya solusi ini, diharapkan mampu meningkatkan stabilitas jaringan, mempercepat waktu respons terhadap gangguan, serta mengurangi beban sistem. Sehingga menjadikan sistem lebih andal dan mendukung keberlangsungan operasioanl jaringan dalam lingkungan kampus.

C. KESIMPULAN

A. Kesimpulan

Hasil dari pemantauan yang dilakukan menunjukkan bahwa sistem memiliki responsivitas yang tinggi, hal ini ditandai dengan adanya gangguan yang terdeteksi secara cepat dan pengiriman notifikasi selalu tepat waktu setelah kondisi abnormal terjadi. Dari sisi perangkat, khususnya pada perangkat pada switch di lantai 8 dan 9 menunjukkan stabilitas yang tinggi dengan hanya mengalami gangguan ringan, sedangkan perangkat seperti PC laboratorium dan laptop pribadi cenderung lebih sering mengalami gangguan, biasanya berupa aspek penggunaan memori dan kurangnya stabilitas interface ethernet.

Oleh karena itu, dalam penerapan sistem monitoring berbasis Zabbix mampu memberikan dampak posistif terhadap operasional perangkat di Gedung TULT. Sistem yang mampu meningkatkan efisiensi dalam proses pemantauan, mempercepat deteksi gangguan, dan mendukung pengambilan keputusan secara lebih informatif.

B. Saran

Setelah menyimpulkan hasil dari implementasi sistem monitoring, beberapa saran yang dapat diberikan untuk pengembangan selanjutnya adalah sebagai berikut:

1. Mengoptimalkan spesifikasi perangkat dan lingkungan virtual, dikarenakan instalasi Zabbix membutuhkan alokasi sumber daya yang cukup besar, terutama pada RAM dan CPU. Disarankan untuk menggunakan perangkat dengan minimal 8 GB dan CPU Multi-Core agar proses monitoring berjalan stabil dan meminimalisir gagalnya pembuatan virtual machine.
2. Melakukan eksplorasi lebih lanjut terhadap OID perangkat switch, dikarenakan penelitian ini belum dapat memantau secara menyeluruh kinerja perangkat switch karena keterbatasan informasi mengenai OID yang relevan. Oleh karena itu, disarankan untuk melakukan eksplorasi lanjutan menggunakan dokumentasi resmi dari vendor atau menanyakan secara langsung terkait OID dari perangkat switch. Dengan begitu peneliti akan mendapatkan informasi lebih lengkap mengenai data seperti CPU Utilization, port error, dan lain sebagainya.
3. Untuk penelitian lebih lanjut mengenai parameter keamanan yang lebih dalam seperti deteksi login tidak sah ataupun serangan DoS, disarankan untuk menggunakan *tools* yang lebih canggih. Karena umumnya Zabbix hanya berfokus ke *performance monitoring*, bukan deteksi ancaman secara spesifik seperti IDS.

Dengan pemanfaatan sistem monitoring yang dilakukan dalam penelitian ini, diharapkan operasional jaringan di Gedung TULT menjadi lebih adaptif, stabil dan responsif terhadap penggunaan jaringan yang semakin kompleks.

REFERENSI

Academy, C. Networking. (2020). *Enterprise Networking, Security, and Automation Companion Guide*. Pearson Education (US).

Alip, N., Fitri, I., & Nathasia, N. D. (2018). *Network Monitoring System Data Radar Penerbangan berbasis PRTG dan ADSB*.

Aziz, A., & Maghdalena Ambarwati, V. (2018). Implementasi Sistem Monitoring Jaringan Berbasis Zabbix Dan Notifikasi Alert Menggunakan Telegram. In *Prosiding Seminar Nasional Teknik Elektro* (Vol. 3, Issue 2018).

Cahyo, A. B., Hariadi, T. K., & Ardiyanto, Y. (2020). *Implementasi Zabbix Server untuk Memonitor Kondisi Jaringan Komputer di Dinas Komunikasi dan Informatika Kabupaten Pekalongan*.

Carvalho, A., Silva, V., Afonso, F., Cardoso, P., Cabral, J., Ekpanyapong, M., Montenegro, S., & Tavares, A. (2016). *Full Virtualization on Low-End Hardware: a Case Study*.

Doni, F. R. (2016). Jaringan Komputer dengan Router Mikrotik. *Simnasiptek*, 88–93.

Huda, M. A. (2024). *IMPLEMENTASI NETWORK MONITORING SYSTEM MENGGUNAKAN APLIKASI ZABBIX UNTUK SERVER PELAYANAN DI RSU BUNDA MARGONDA DENGAN NOTIFIKASI TELEGRAM*.

Husna, M. A., & Rosyani, P. (2021). Implementasi Sistem Monitoring Jaringan dan Server Menggunakan Zabbix yang Terintegrasi dengan Grafana dan Telegram. *JURIKOM (Jurnal Riset Komputer)*, *8*(6), 247. https://doi.org/10.30865/jurikom.v8i6.3631

Ichsan Mustafid, L., Iqbal, M., & Zero Fomandes, M. (2022). *IMPLEMENTASI SISTEM MONITORING LINK OPTICAL LINE TERMINAL ICONNET BERBASIS ZABBIX SECARA REALTIME DENGAN NOTIFIKASI ALERT TELEGRAM (STUDI KASUS DI PT INDONESIA COMNETS PLUS REGIONAL JAWA BARAT)*.

Khasanah, S. N., & Utami, L. A. (2018). *Implementasi Failover Pada Jaringan WAN Berbasis VPN*.

Khongsong, E. (2023). *A Network Security Solution to Manage and Increase Effectiveness of Servers*.

Kurose, J. F. ., & Ross, K. W. . (2017). *Computer networking : a top-down approach*. Pearson.

Olups, R. (2016). *Zabbix Network Monitoring Second Edition*. www.packtpub.com

Pradana, A., Widiasari, I. R., Efendi, R., & Informatika, T. (2022). Implementasi Sistem Monitoring Jaringan Menggunakan Zabbix Berbasis SNMP. *AITI: Jurnal Teknologi Informasi*, *19*(Agustus), 248–262.

Saputra, R., Rafael, D., & Simamora, S. N. M. P. (n.d.). *IMPLEMENTASI NETWORK MONITORING SYSTEM ZABBIX UNTUK KEAMANAN JARINGAN KOMPUTER PADA STUDI KKASUS PT TRIDAYA SINERGI INDONESIA BANDUNGG*.

SIA, Z. (2025). *Zabbix Documentations*. Https://Www.Zabbix.Com/Documentation/.

Tirumalasetty, C., Chou, C. C., Reddy, N., Gratz, P., & Abouelwafa, A. (2022). *Reducing Minor Page Fault Overheads through Enhanced Page Walker*. http://arxiv.org/abs/2112.14013

Vacche, A. D., & Lee, K. S. (2015). *Zabbix Network Monitoring Essentials*.

Yanda, P. S. (2023). *MEMBANGUN SISTEM MONITORING BERBASIS ZABBIX TERINTEGRASI DENGAN TELEGRAM PADA UNIT NETWORK OPERATION PT. XAPIENS TEKNOLOGI INDONESIA*.