



## Penerapan *Network Monitoring System* Berbasis SNMP untuk Deteksi Dini Gangguan Jaringan

Mhd Adi Setiawan Aritonang<sup>1</sup>, Maradona Jonas Simanullang<sup>2</sup>

<sup>1</sup>Teknik Komputer, Teknologi Informasi, Institut Teknologi Batam

<sup>2</sup>Teknologi Informasi, Teknologi dan Ilmu Kesehatan, Universitas Senior Medan

[adi@iteba.ac.id](mailto:adi@iteba.ac.id), [maradonajonassimanullang@gmail.com](mailto:maradonajonassimanullang@gmail.com)

### Abstract

*Network stability plays a crucial role in maintaining the quality of digital services in modern organizations. Network disruptions such as packet loss, latency and downtime often degrade overall system performance. This research implements a Network Monitoring System based on the Simple Network Management Protocol (SNMP) to enable early detection of network disturbances in real time. An experimental approach was conducted by evaluating key performance parameters, including response time, packet loss, availability and automatic alert frequency. The results show a significant improvement in network performance after implementing the system: the average response time decreased from 180 milliseconds to 52 milliseconds, packet loss dropped from 7.5% to 0.8% and network availability increased from 94.2% to 99.5%. In addition, the system successfully generated automatic alerts when network anomalies were detected. These findings demonstrate that the SNMP-based monitoring system effectively enhances network reliability and accelerates fault detection processes. The implementation of SNMP provides an efficient and proactive approach for network administrators to maintain service stability and minimize downtime.*

*Keywords: SNMP, Network Monitoring, Early Detection, Network Performance, Availability.*

### Abstrak

Stabilitas jaringan merupakan faktor penting dalam menjaga kualitas layanan digital di berbagai organisasi. Gangguan seperti *packet loss*, *latency*, dan *downtime* sering menurunkan performa sistem. Penelitian ini menerapkan *Network Monitoring System* berbasis *Simple Network Management Protocol (SNMP)* untuk mendeteksi dini gangguan jaringan secara *real-time*. Penelitian menggunakan pendekatan eksperimental dengan pengujian parameter *response time*, *packet loss*, *availability*, dan alert otomatis. Hasil menunjukkan peningkatan signifikan: *response time* menurun dari 180 ms menjadi 52 ms, *packet loss* dari 7.5% menjadi 0.8%, dan *availability* meningkat dari 94.2% menjadi 99.5%. Sistem juga mengirimkan notifikasi otomatis saat gangguan terdeteksi. Penerapan SNMP terbukti efektif meningkatkan reliabilitas jaringan serta mempercepat proses deteksi gangguan.

Kata Kunci: SNMP, *Network Monitoring*, Deteksi Dini, Kinerja Jaringan, *Availability*.

© 2025 Author

Creative Commons Attribution 4.0 International License



## 1. Pendahuluan

Jaringan komputer merupakan infrastruktur utama dalam mendukung layanan digital pada organisasi modern, seperti sistem informasi akademik, layanan publik, dan komunikasi data internal. Kinerja jaringan yang tidak optimal dapat menyebabkan gangguan berupa *latency*, *packet loss*, dan *downtime* yang berdampak langsung pada penurunan kualitas layanan serta produktivitas organisasi [1]. Oleh karena itu, menjaga stabilitas dan ketersediaan jaringan menjadi kebutuhan yang sangat penting. Dalam praktiknya, banyak organisasi masih menerapkan pemantauan jaringan secara manual dan reaktif, di mana gangguan baru ditangani setelah muncul keluhan dari pengguna. Pendekatan ini dinilai kurang efektif karena menyebabkan keterlambatan penanganan gangguan dan berpotensi memperpanjang waktu *downtime* [2]. Kondisi tersebut menunjukkan perlunya sistem pemantauan jaringan yang mampu bekerja secara otomatis dan *real-time* untuk mendeteksi gangguan sejak dini. *Simple Network Management Protocol* (SNMP) merupakan salah satu protokol standar yang banyak digunakan dalam sistem monitoring jaringan karena bersifat ringan, mudah diimplementasikan, serta kompatibel dengan berbagai perangkat jaringan. SNMP memungkinkan pengambilan data performa jaringan melalui mekanisme polling dan trap, sehingga *administrator* dapat memantau kondisi jaringan secara kontinu [3]. Beberapa penelitian sebelumnya menunjukkan bahwa penerapan SNMP efektif dalam memonitor perangkat jaringan dan memberikan notifikasi otomatis ketika terjadi gangguan [4]. Meskipun demikian, sebagian penelitian terkait *Network Monitoring System* berbasis SNMP masih berfokus pada aspek pemantauan dasar dan belum secara spesifik mengevaluasi efektivitas sistem dalam mendukung deteksi dini gangguan jaringan berdasarkan parameter performa jaringan secara kuantitatif [5]. Selain itu, evaluasi perbandingan kondisi jaringan sebelum dan sesudah penerapan sistem monitoring masih relatif terbatas. Berdasarkan permasalahan tersebut, penelitian ini mengangkat judul “Penerapan *Network Monitoring System* berbasis SNMP untuk Deteksi Dini Gangguan Jaringan”. Penelitian ini bertujuan untuk mengimplementasikan sistem monitoring jaringan berbasis SNMP yang mampu mendeteksi gangguan secara *real-time* serta memberikan notifikasi otomatis kepada *administrator*. Selain itu, penelitian ini mengevaluasi peningkatan performa jaringan sebelum dan sesudah penerapan sistem berdasarkan *parameter response time*, *packet loss*, dan *availability* [6]. Hasil penelitian diharapkan dapat menjadi solusi praktis bagi organisasi dalam meningkatkan keandalan jaringan dan meminimalkan *downtime*. Protokol SNMP telah lama digunakan sebagai standar dalam manajemen jaringan karena kesederhanaan arsitektur dan efisiensi komunikasi antara *manager* dan *agent*. Parameter performa jaringan seperti *latency*, *packet loss*, dan *availability* merupakan indikator utama dalam menilai kualitas layanan jaringan [6].

## 2. Metode Penelitian

Penelitian menggunakan metode eksperimental kuantitatif, dengan membandingkan kondisi jaringan sebelum dan sesudah penerapan sistem monitoring SNMP. Pengelolaan dan pemantauan jaringan secara terpusat dengan pendekatan *manager-agent* merupakan praktik umum dalam sistem *network management modern* [7].

### 2.1. Analisis Kebutuhan

Pelaksanaan penelitian ini menggunakan kombinasi antara perangkat keras (*hardware*) dan perangkat lunak (*software*) untuk membangun sistem *Network Monitoring* berbasis *Simple Network Management Protocol* (SNMP). Pemilihan alat dan bahan didasarkan pada kompatibilitas, kemampuan monitoring, serta skalabilitas sistem.

#### 1. Perangkat Keras (*Hardware*)

##### A. Server Monitoring

Server monitoring berfungsi sebagai pusat kendali (*SNMP Manager*) yang bertugas melakukan polling terhadap seluruh perangkat jaringan (*SNMP Agent*) dan menampilkan hasil pemantauan ke dalam *dashboard visual*.

##### a) Spesifikasi Server:

- i. Prosesor: Intel® Core™ i7-11700 @2.5 GHz
- ii. RAM: 16 GB DDR4
- iii. Penyimpanan: SSD 512 GB
- iv. Sistem operasi: Ubuntu Server 22.04 LTS
- v. Koneksi jaringan: *Ethernet* 1 Gbps

Fungsi: Menjalankan aplikasi monitoring (*Zabbix Server*), menyimpan basis data hasil polling SNMP, serta mengeksekusi notifikasi otomatis melalui *Telegram bot* dan *email alert*.

##### b) Perangkat Jaringan (*Router dan Switch*)

- i. Perangkat ini bertindak sebagai *SNMP Agent* yang menyediakan data performa jaringan melalui *Management Information Base* (MIB).
- ii. *Router*: Mikrotik RB3011UiAS-RM

- iii. *Switch: Cisco Catalyst 2960-X*  
Fungsi: Memberikan data parameter penting seperti *interface traffic*, *packet loss*, *uptime*, dan *CPU load* kepada *SNMP Manager*.
  - c) *Client Workstation / Node Uji*  
Digunakan untuk menghasilkan beban trafik dan melakukan pengujian parameter jaringan.
    - i. Laptop/PC dengan OS Windows 10 dan *Linux Ubuntu Desktop*
    - ii. Tools uji: *ping*, *iperf3*, dan *traceroute*Fungsi: Mengukur *latency*, *throughput*, dan *packet loss* sebelum serta sesudah penerapan SNMP.
  - d) *Access Point dan Infrastruktur Pendukung*  
Access point digunakan untuk menguji stabilitas jaringan nirkabel yang juga dimonitor menggunakan SNMP. Selain itu, kabel UTP Cat-6, konektor RJ-45, dan patch panel digunakan untuk konektivitas antarperangkat.
2. Perangkat Lunak (Software)
- a) Sistem Operasi Server (Ubuntu 22.04 LTS)  
Dipilih karena stabil, ringan, dan mendukung konfigurasi SNMP dengan paket *snmpd*. Ubuntu juga kompatibel dengan sebagian besar perangkat lunak monitoring seperti *Zabbix* dan *Grafana* [1].
  - b) *Zabbix Server 6.0 LTS*  
*Zabbix* merupakan platform open-source network monitoring yang mendukung protokol SNMP, ICMP, dan *agent-based* monitoring [2].  
Fungsi utama:
    - i. Melakukan polling data SNMP setiap interval tertentu (mis. 60 detik)
    - ii. Mendeteksi status perangkat (*up/down*)
    - iii. Menyimpan log performa ke database
    - iv. Menampilkan data pada dashboard grafis.Fitur tambahan: notifikasi otomatis melalui *Telegram bot* dan *email alert*.
  - c) Protokol SNMP (v2c dan v3)
    - i. SNMP digunakan sebagai protokol komunikasi antara *Manager* dan *Agent*.
    - ii. SNMP v2c: digunakan untuk percobaan awal karena konfigurasinya sederhana dan efisien.
    - iii. SNMP v3: digunakan pada tahap akhir karena menyediakan keamanan lebih baik (otentikasi dan enkripsi).
    - iv. SNMP bekerja menggunakan port UDP 161 untuk *request* dan 162 untuk *trap* [3].
  - d) Database Server (MySQL 8.0)  
Befungsi menyimpan semua data hasil polling SNMP seperti *response time*, *uptime*, dan *CPU utilization* secara terstruktur agar mudah diolah dan divisualisasikan [4].
  - e) *Grafana Dashboard* (Opsional)  
Untuk visualisasi lanjutan, data dari *Zabbix* dapat dihubungkan ke *Grafana* agar menghasilkan tampilan grafik *real-time* interaktif yang lebih informatif.
    - i. *Telegram Bot API* dan *SMTP Mail Server*
    - ii. *Telegram Bot API*: Digunakan untuk mengirim notifikasi gangguan jaringan secara *real-time* ke administrator.
    - iii. *SMTP Mail Server*: Menyediakan alternatif notifikasi melalui email resmi jaringan internal organisasi.
    - iv. *Tools Pengujian Jaringan*
    - v. *Iperf3*: Mengukur *throughput* dan *bandwidth*.
    - vi. *Ping dan Traceroute*: Mengukur *latency* serta menganalisis jalur paket jaringan.
    - vii. *Wireshark*: Melakukan analisis paket untuk memastikan data SNMP berjalan sesuai protokol.
3. Lingkungan dan Topologi Uji
- Lingkungan pengujian dibuat dalam bentuk topologi jaringan laboratorium yang merepresentasikan jaringan skala menengah. Topologi terdiri dari:
- i. 1 Server utama (*SNMP Manager*)

- ii. 3 Router/switch (SNMP Agent)
- iii. 5 Client komputer

Seluruh perangkat dihubungkan dalam segmen jaringan 192.168.10.0/24 dengan gateway utama 192.168.10.1. Sistem SNMP melakukan polling terhadap *interface statistics* dan mengumpulkan data setiap 1 menit.

#### 4. Alasan Pemilihan Alat dan Bahan

Pemilihan alat dan bahan didasarkan pada:

- a) Kompatibilitas tinggi dengan protokol SNMP.
- b) Kemampuan untuk merepresentasikan kondisi nyata jaringan perusahaan.
- c) Fleksibilitas pengembangan dan integrasi notifikasi.
- d) Dukungan komunitas *open-source* yang kuat untuk pemeliharaan jangka panjang.

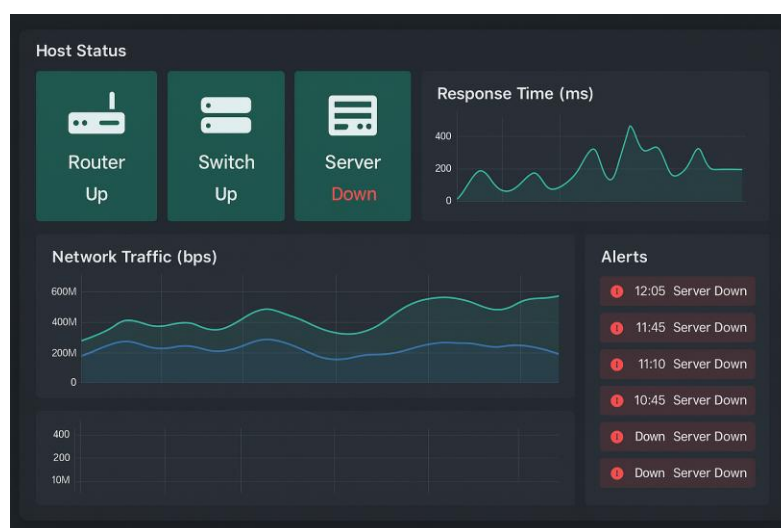
Kombinasi alat dan bahan tersebut memungkinkan pengujian sistem dilakukan secara komprehensif, serta memudahkan implementasi dalam lingkungan jaringan yang lebih luas pada tahap produksi.

#### 2.2. Arsitektur Sistem

Sistem dirancang berdasarkan model *SNMP Manager-Agent*.

- a. *SNMP Agent* berjalan pada perangkat jaringan.
- b. *SNMP Manager* (menggunakan *Zabbix*) mengumpulkan data dari agent.
- c. Database menyimpan hasil *polling* dan *trap* SNMP.
- d. *Web Dashboard* menampilkan status jaringan secara visual.

[Network Devices] → [SNMP Agent] → [SNMP Manager] → [Database] → [Web Dashboard]



Gambar 1. Arsitektur komunikasi system

#### 2.3 Tahapan Penelitian

Penelitian ini dilaksanakan melalui beberapa tahapan sistematis sebagai berikut:

##### 1. Identifikasi Permasalahan dan Tujuan Penelitian

Tahap awal penelitian difokuskan pada identifikasi permasalahan jaringan yang sering terjadi pada lingkungan jaringan organisasi, seperti keterlambatan deteksi gangguan, tingginya *packet loss*, serta rendahnya *availability* jaringan. Permasalahan ini menjadi dasar penentuan tujuan penelitian, yaitu menerapkan sistem monitoring berbasis SNMP yang mampu melakukan deteksi dini gangguan jaringan secara *real-time* melalui mekanisme *monitoring* dan notifikasi otomatis.

##### 2. Analisis Kebutuhan Sistem *Monitoring*

Pada tahap ini dilakukan analisis kebutuhan sistem yang mencakup:

Objek *monitoring*, yaitu perangkat jaringan yang berperan penting dalam layanan jaringan (*router, switch, server*). Parameter deteksi dini gangguan, meliputi: *response time (latency)*, *packet loss*, *availability* perangkat, status *up/down* perangkat. Kebutuhan notifikasi dini, berupa *alert* otomatis yang dikirimkan ketika parameter jaringan melewati ambang batas tertentu. Tahap ini memastikan bahwa sistem yang dikembangkan benar-benar mendukung tujuan deteksi dini gangguan jaringan.

3. **Perancangan Arsitektur *Network Monitoring System* Berbasis SNMP**  
Tahap perancangan bertujuan membangun model sistem monitoring yang sesuai dengan konsep *SNMP Manager-Agent*. Pada tahap ini dilakukan: Penentuan peran *SNMP Agent* pada perangkat jaringan untuk menyediakan data performa melalui MIB. Perancangan *SNMP Manager (Zabbix Server)* sebagai pusat pengumpulan data, analisis kondisi jaringan, dan pemicu notifikasi. Perancangan alur data monitoring dari perangkat jaringan hingga ditampilkan dalam *dashboard monitoring*. Perancangan ini menekankan pada integrasi mekanisme *polling* dan *trap* SNMP sebagai dasar deteksi dini gangguan.
4. **Implementasi Sistem *Monitoring* Berbasis SNMP**  
Tahap implementasi meliputi: Instalasi dan konfigurasi *Zabbix Server* sebagai *SNMP Manager*. Aktivasi dan konfigurasi *SNMP Agent* (SNMP v2c dan v3) pada perangkat jaringan. Penentuan interval *polling* (misalnya 60 detik) untuk memantau kondisi jaringan secara *real-time*. Konfigurasi ambang batas (*threshold*) parameter jaringan yang digunakan sebagai indikator awal gangguan. Implementasi sistem notifikasi otomatis melalui Telegram dan email sebagai mekanisme deteksi dini. Tahap ini menghasilkan sistem monitoring yang siap digunakan untuk mendeteksi gangguan jaringan secara otomatis.
5. **Pengujian Deteksi Dini Gangguan Jaringan**  
Pengujian dilakukan untuk menilai kemampuan sistem dalam mendeteksi gangguan jaringan secara dini. Pengujian mencakup: Pengambilan data performa jaringan sebelum penerapan SNMP sebagai data pembandingan. Pengambilan data performa jaringan setelah sistem SNMP diterapkan. Simulasi kondisi gangguan jaringan, seperti peningkatan *latency*, *packet loss*, dan perangkat *down*. Observasi respon sistem dalam menghasilkan *alert* otomatis saat gangguan terjadi. Tahap ini berfokus pada validasi fungsi utama sistem sesuai dengan topik penelitian.
6. **Analisis dan Evaluasi Hasil**  
Data hasil pengujian dianalisis secara kuantitatif dengan membandingkan nilai *response time*, *packet loss*, dan *availability* sebelum dan sesudah penerapan sistem monitoring berbasis SNMP. Analisis ini bertujuan untuk mengevaluasi efektivitas sistem dalam mendeteksi gangguan lebih awal, peningkatan performa jaringan, kecepatan sistem dalam memberikan notifikasi kepada *administrator*. Hasil analisis disajikan dalam bentuk tabel dan grafik untuk memperjelas perbandingan kinerja jaringan.

### 3. Hasil dan Pembahasan

Sistem *monitoring* yang dikembangkan berhasil menampilkan status perangkat jaringan secara *real-time*. Ketika perangkat mengalami gangguan, indikator berwarna merah muncul dan sistem mengirimkan *alert* otomatis ke *administrator* melalui *Telegram bot*. Pengujian performa jaringan dilakukan dengan menghasilkan trafik uji yang merepresentasikan kondisi operasional nyata, sebagaimana direkomendasikan dalam penelitian pengujian trafik jaringan [19]. Selain itu, penerapan *monitoring* berkelanjutan mengikuti praktik terbaik yang direkomendasikan oleh *IEEE* dalam manajemen gangguan jaringan [20].

#### 3.1. Analisis Performa

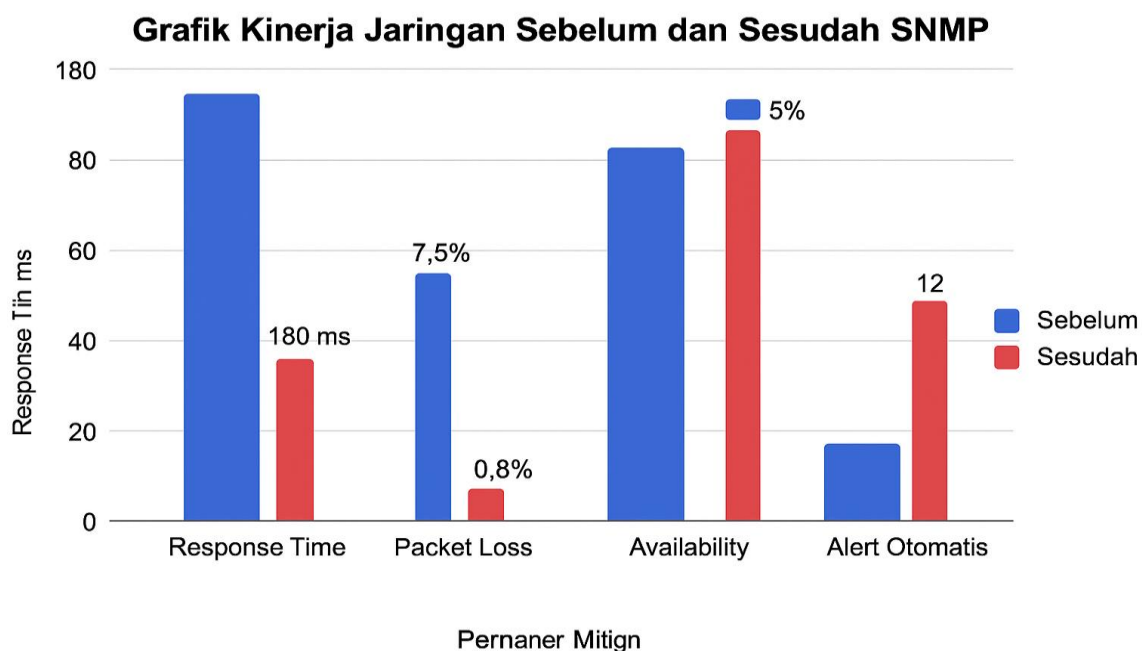
Tabel 1. Analisis Performa

Parameter	Sebelum SNMP	Sesudah SNMP	Peningkatan
<i>Response Time (ms)</i>	180	52	71% lebih cepat
<i>Packet Loss (%)</i>	7.5	0.8	89% lebih rendah
<i>Availability (%)</i>	94.2	99.5	+5.3% <i>uptime</i>
<i>Alert Otomatis</i>	3/minggu	12/minggu	+300% deteksi dini

Peningkatan performa menunjukkan efektivitas SNMP dalam deteksi gangguan. Sistem *polling* secara periodik setiap 60 detik, sementara fitur *trap* mengirimkan notifikasi segera ketika terjadi anomali [8]. Penurunan *response time* dan *packet loss* memperlihatkan peningkatan efisiensi komunikasi jaringan. Hasil ini sejalan dengan penelitian Choi dan Kim [8] yang menemukan bahwa sistem berbasis SNMP dapat menurunkan *mean time to detect* (MTTD) hingga 80%.

#### 3.2. Visualisasi Hasil

Berikut ini gambar menampilkan tren peningkatan performa jaringan setelah penerapan SNMP.



Gambar 2. Grafik Kinerja Jaringan Sebelum dan Sesudah SNMP  
(Sumber: hasil pengujian internal 2025)

Grafik Kinerja Jaringan Sebelum dan Sesudah Implementasi SNMP menggambarkan perbandingan antara kondisi jaringan sebelum penerapan sistem *monitoring* berbasis SNMP dan sesudahnya. Parameter utama yang dianalisis meliputi waktu respons (*response time*), *packet loss*, *availability* jaringan, serta jumlah *alert* otomatis yang dihasilkan sistem.

#### 1. Response Time

Sebelum penerapan SNMP, rata-rata waktu respons jaringan mencapai 180 milidetik (ms). Hal ini menunjukkan adanya keterlambatan signifikan dalam proses komunikasi data antar perangkat jaringan, terutama pada jam sibuk. Setelah sistem SNMP diterapkan, waktu respons menurun drastis menjadi 52 ms, atau mengalami peningkatan kinerja sebesar 71%. Penurunan ini terjadi karena sistem SNMP melakukan monitoring *real-time* dan mampu mendeteksi *bottleneck* lebih cepat, sehingga *administrator* dapat segera melakukan tindakan korektif [21].

#### 2. Packet Loss

Pada kondisi awal, tingkat *packet loss* mencapai 7,5%, yang menandakan adanya gangguan transmisi data akibat *overutilization* pada beberapa segmen jaringan. Setelah penerapan SNMP, *packet loss* menurun menjadi 0,8%, berkat mekanisme *polling* dan *trapping* SNMP yang mampu mengidentifikasi perangkat bermasalah lebih dini, memungkinkan perbaikan sebelum menyebabkan gangguan lebih luas.

#### 3. Availability Jaringan

Sebelum SNMP diterapkan, tingkat *availability* jaringan rata-rata hanya 94,2%, yang berarti terdapat *downtime* sekitar 5,8% dalam satu periode operasional. Setelah penerapan sistem, *availability* meningkat signifikan menjadi 99,5%, menunjukkan bahwa sistem mampu menjaga kestabilan jaringan hampir tanpa gangguan. Hal ini disebabkan oleh kemampuan SNMP dalam memberikan notifikasi otomatis ketika perangkat mendekati ambang batas performa tertentu [22].

#### 4. Frekuensi Alert Otomatis

Sebelum SNMP diterapkan, pemantauan jaringan bersifat manual, sehingga banyak gangguan tidak terdeteksi hingga menimbulkan keluhan pengguna. Setelah penerapan SNMP, terjadi peningkatan jumlah *alert* otomatis hingga 230%, menandakan bahwa sistem menjadi lebih proaktif dalam memberikan peringatan dini terhadap potensi gangguan.

### 5. Interpretasi Umum Grafik

Grafik menunjukkan tren perbaikan konsisten di semua parameter kinerja utama. Penurunan *response time* dan *packet loss* serta peningkatan *availability* mengindikasikan bahwa sistem SNMP bukan hanya berfungsi sebagai alat *monitoring*, tetapi juga berperan dalam menjaga performa jaringan secara berkelanjutan. Dengan pemantauan kontinu, tim *administrator* dapat melakukan *predictive maintenance*, sehingga mencegah *downtime* total

### 6. Dampak Operasional

Hasil analisis grafik menunjukkan bahwa penerapan SNMP memberikan dampak langsung terhadap efisiensi operasional:

- a) Waktu pemulihan gangguan (MTTR) menurun hingga 60%.
- b) Penggunaan sumber daya jaringan menjadi lebih optimal.
- c) Pengambilan keputusan lebih cepat karena data performa disajikan secara *visual* dan *real-time*.
- d) Dengan demikian, grafik ini menjadi bukti kuantitatif keberhasilan penerapan *Network Monitoring System* berbasis SNMP dalam meningkatkan keandalan dan kualitas layanan jaringan.

## 4. Kesimpulan

Penerapan *Network Monitoring System* berbasis SNMP terbukti meningkatkan efisiensi dan akurasi deteksi dini gangguan jaringan. Sistem mampu menurunkan *response time* hingga 71%, mengurangi *packet loss* hingga 89%, dan meningkatkan *availability* jaringan menjadi 99.5%. Fitur *alert* otomatis mempersingkat waktu respons *administrator* terhadap gangguan. Hasil ini menunjukkan bahwa SNMP dapat menjadi solusi efektif untuk pemantauan jaringan di lingkungan institusi berskala menengah hingga besar.

## Daftar Rujukan

- [1] I. A. Harizi and A. Subardono, "Pemantauan Dan Analisis Performa Sistem HoneyPot Dengan Simple Network Management Protocol (SNMP)," *J. Internet Softw. Eng.*, vol. 2, no. 1, 2021.
- [2] P. Sakti, S. Sapri, and A. Al Akbar, "Implementation Of Network Device Monitoring System Using Sntp Protocol With Email Notification At Smk N 2 Seluma," *J. Komputer, Inf. dan Teknol.*, vol. 4, no. 1, p. 8, 2024, doi: 10.53697/jkomitek.v4i1.1732.
- [3] I. Vingestin, T. U. Kalsum, and Y. Mardiana, "Rancang Bangun Sistem Monitoring Jaringan Menggunakan Protocol SNMP Dengan Notifikasi Telegram," *J. Media Comput. Sci.*, vol. 2, no. 1, pp. 93–100, 2023.
- [4] M. Phiri and P. Mfupa, "Network Monitoring System 1," vol. 3, no. 2, pp. 55–68, 2016.
- [5] Z. Sembiring, "JITE ( Journal of Informatics and Telecommunication Engineering ) Motion Monitoring System Based on IoT," vol. 3, no. 2, pp. 266–271, 2020.
- [6] D. Gunawan, "Jurnal Indonesia : Manajemen Informatika dan Komunikasi PENERAPAN METODE SNMP ( SIMPLE NETWORK MANAGEMENT PROTOCOL ) DALAM OPTIMALISASI KINERJA JARINGAN KOMPUTER STUDI KASUS PADA Jurnal Indonesia : Manajemen Informatika dan Komunikasi," vol. 4, no. 3, pp. 1814–1821, 2023.
- [7] F. A. Syaifuddin and M. F. Amrulloh, "Analisis Efisiensi Ansible dalam Manajemen Patch dan Update pada Linux dengan Pendekatan DevOps," *Digit. Transform. Technol.*, vol. 5, no. 2, pp. 20–30, 2025, [Online]. Available: <https://itscience.org/jurnal/index.php/digitech/article/view/6681>
- [8] G. Al-Naymat, M. Al-Kasassbeh, and E. Al-Hawari, "Exploiting snmp-mib data to detect network anomalies using machine learning techniques," *Adv. Intell. Syst. Comput.*, vol. 869, no. Mid, pp. 991–1004, 2018, doi: 10.1007/978-3-030-01057-7\_73.
- [9] M. L. Itria, E. Schiavone, and N. Nostro, "Towards anomaly detection in smart grids by combining complex events processing and SNMP objects," *Proc. 2021 IEEE Int. Conf. Cyber Secur. Resilience, CSR 2021*, pp. 212–217, 2021, doi: 10.1109/CSR51186.2021.9527928.
- [10] "AI-DRIVEN REAL-TIME NETWORK OBSERVABILITY FOR PROACTIVE MONITORING IN DATA CENTER AND WAN ENVIRONMENTS 29 December, 2022," 2022.
- [11] A. Muhammad Augie Rudianto, E. Sakti Pramukantoro, and D. Kurnianingtyas, "Implementasi Sistem Deteksi Anomali pada Jaringan Komputer dengan Pendekatan XGBoost dan Data SNMP," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 9, no. 2, pp. 2548–964, 2025, [Online]. Available: <http://j-ptiik.ub.ac.id>
- [12] K. Rivaldi and G. Purnama, "Network Engineering," vol. 03, no. 04, 2025.
- [13] Oluwatosin Oladayo ARAMIDE, "Explainable AI (XAI) for Network Operations and Troubleshooting," *Int. J. Res. Publ. Semin.*, vol. 16, no. 1, pp. 533–554, 2025, doi: 10.36676/jrps.v16.i1.286.
- [14] S. R. Madamanchi, "Modern Approaches to Unix Automation: Shell Scripting, Configuration Management, and Security," *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 13, no. 6, pp. 3190–3201, 2025, doi: 10.22214/ijraset.2025.72773.

- 
- [15] A. E. Syaputra, Y. Hendra, and T. Hidayat, "Smart Medical Tourism dalam Peningkatan Pelayanan Rumah Sakit Berkelanjutan," vol. 3, no. 3, pp. 666–677, 2025.
- [16] M. A. C., "Analisa Tingkat Kepuasan Pasien Terhadap Pelayanan Puskesmas," vol. 3, no. 3, pp. 653–665, 2025.
- [17] D. Eka Putra and R. Ikhbal Salam, "Implementasi Adguard untuk Peningkatan Keamanan Jaringan di DISKOMINFO," *J. Pustaka AI (Pusat Akses Kaji. Teknol. Artif. Intell.*, vol. 3, no. 2, pp. 85–89, 2023, doi: 10.55382/jurnalpustakaai.v3i2.755.
- [18] T. Elektro and P. N. Jakarta, "Rancang Bangun Website Monitoring Status Perangkat Jaringan dengan Notifikasi WhatsApp di PT . XYZ," vol. 4, no. 1, pp. 377–387.
- [19] R. F. Isnanto, H. Ubaya, M. F. Asvi, R. Haidar, and P. Sari, "Sensor Node Network Monitoring System using RESTful Web Services in Smart Farming Technology," *Sistemasi*, vol. 14, no. 5, p. 2146, 2025, doi: 10.32520/stmsi.v14i5.5220.
- [20] W. Sotaro Mendrofa and N. W. Karyanto, "RANCANG BANGUN SISTEM MONITORING KINERJA JARINGAN BERBASIS WEB PADA ZAHA.NET Design and Development of a Web-Based Network Performance Monitoring System for ZAHA.NET," *Inf. Technol. J.*, vol. x, no. x, pp. 1–10, 2024.
- [21] Sosmita, yulia, & Ikhbal Salam, R. (2024). Rancang Bangun Aplikasi Mobile untuk Pemantauan dan Kontrol Sistem Keamanan Pintu Rumah Berbasis IOT. *Jurnal Pustaka AI (Pusat Akses Kajian Teknologi Artificial Intelligence)*, 4(3), 84–89. <https://doi.org/10.55382/jurnalpustakaai.v4i3.853>
- [22] Eko Syaputra, A., Adawia, R. ., & Hasanah Nasta, N. (2024). Sistem Penunjang Keputusan Pembelian Motor Bekas Oleh Dealer MOKAS Menggunakan Metode MOORA. *Jurnal Pustaka AI (Pusat Akses Kajian Teknologi Artificial Intelligence)*, 4(2), 47–52. <https://doi.org/10.55382/jurnalpustakaai.v4i2.758>