Jurnal Multidisiplin Teknik, Sains, Pendidikan dan Teknologi

E-ISSN: 3064-6103
Volume 3, **Number** 2, Juli 2026
https://doi.org/10.62671/suliwa.v3i2.261

ANALISIS STUDI LITERATUR PERAN SNMP DALAM MONITORING KINERJA DAN KETERSEDIAAN JARINGAN TELKOMUNIKASI

Meidina Agnesia[1*], Sri Yusnita[2], Afrizal Yuhanef[3], Yulindon Khaidir[4]
[1,2,3]Politeknik Negeri Padang, Indonesia
[1*]agnesiameidina@email.com, [2]sriyusnita@pnp.ac.id, [3]afrizal@pnp.ac.id, [4]yulindon@pnp.ac.id

ABSTRACT

The increasing complexity, heterogeneity, and large-scale nature of modern telecommunication networks require a monitoring mechanism capable of ensuring continuous network performance and service availability. Although modern approaches such as streaming telemetry and network observability provide higher data granularity, Simple Network Management Protocol (SNMP) remains widely used due to its lightweight design, standardization, and multi-vendor compatibility. This study aims to analyze the role of SNMP in monitoring network performance and availability in telecommunication systems. The research employed a structured literature review approach by collecting, selecting, and synthesizing relevant studies published within the last five years. The results indicate that SNMP remains effective for monitoring key performance parameters, including throughput, latency, packet loss, CPU utilization, interface status, uptime, and fault notifications. Its major strength lies in supporting interoperable monitoring across heterogeneous multi-vendor infrastructures. However, limitations were identified in terms of polling scalability, data granularity, and real-time traffic visibility in modern cloud, SDN, edge, and IoT-based environments. This study concludes that SNMP remains strategically relevant as a baseline monitoring layer and is most effective when integrated with streaming telemetry in a hybrid monitoring architecture.

Keywords:
SNMP, network monitoring, performance, availability, multi-vendor, telemetry.

PENDAHULUAN

Perkembangan jaringan telekomunikasi modern yang semakin kompleks, heterogen, dan berskala besar menuntut adanya mekanisme monitoring yang mampu menjamin kinerja (performance) dan ketersediaan (availability) layanan secara berkelanjutan. Infrastruktur jaringan saat ini tidak hanya terdiri atas router dan switch konvensional, tetapi juga perangkat radio, server virtual, perangkat IoT, hingga sistem berbasis cloud dan edge computing yang bekerja secara dinamis. Dalam kondisi tersebut, proses pemantauan parameter seperti bandwidth, latency, packet loss, CPU utilization, memory usage, dan interface status menjadi sangat penting untuk menjaga kualitas layanan dan mendukung tindakan preventif terhadap gangguan jaringan. Pada praktiknya, Simple Network Management Protocol (SNMP) masih menjadi salah satu protokol paling luas digunakan karena sifatnya yang ringan, terstandarisasi, dan kompatibel dengan hampir seluruh perangkat jaringan dari berbagai vendor (Yaseen, 2025).

Dalam beberapa tahun terakhir, berbagai penelitian telah menunjukkan efektivitas SNMP dalam mendukung monitoring performa jaringan. Vingestin, Kalsum, dan Mardiana (2023) mengembangkan sistem monitoring berbasis SNMP yang terintegrasi dengan notifikasi Telegram untuk memberikan laporan kondisi jaringan secara real-time. Selanjutnya, Alhilali, Al Farawn, dan Mjhool (2023) merancang sistem manajemen trafik jaringan real-time menggunakan SNMP yang mampu meningkatkan efisiensi pengawasan trafik server tanpa ketergantungan pada third-party monitoring tools. Penelitian oleh Sakti, Sapri, dan Akbar (2024) juga menunjukkan bahwa integrasi SNMP dengan email notification efektif untuk mempercepat respons administrator terhadap gangguan perangkat jaringan. Sementara itu, Alwanto dan Yel (2025) memanfaatkan SNMP bersama platform Cacti untuk mengevaluasi throughput, delay, packet loss, dan availability pada jaringan enterprise, dengan hasil peningkatan akurasi observasi performa secara signifikan.

Di sisi lain, perkembangan pendekatan monitoring modern seperti in-band telemetry dan programmable network observability mulai menawarkan granularitas data yang lebih tinggi dibandingkan polling SNMP tradisional. Yaseen (2025) menjelaskan bahwa pendekatan monitoring modern telah bergeser dari metode berbasis counter menuju telemetry real-time yang lebih scalable untuk jaringan skala besar. Bahkan, Zhang et al. (2025) menunjukkan bahwa telemetry berbasis prediksi trafik mampu mengurangi overhead kontrol hingga 50% pada switch dengan beban tinggi. Namun demikian, implementasi pendekatan tersebut masih cenderung kompleks, membutuhkan dukungan perangkat khusus, dan belum sepenuhnya dapat menggantikan SNMP pada banyak infrastruktur telekomunikasi yang masih mengandalkan kompatibilitas multi-vendor.

Jurnal Multidisiplin Teknik, Sains, Pendidikan dan Teknologi

E-ISSN: 3064-6103
Volume 3, **Number** 2, Juli 2026
https://doi.org/10.62671/suliwa.v3i2.261

Meskipun berbagai penelitian telah membuktikan efektivitas SNMP pada implementasi monitoring praktis, sebagian besar studi masih berfokus pada pengembangan sistem atau studi kasus implementatif tertentu, sementara kajian yang secara khusus menganalisis peran SNMP dari perspektif studi literatur terhadap kontribusinya dalam menjaga kinerja dan ketersediaan jaringan telekomunikasi secara komprehensif masih relatif terbatas, terutama dalam konteks perbandingannya dengan evolusi metode telemetry modern.

Berdasarkan kondisi tersebut, artikel ini menawarkan kajian literatur yang terstruktur untuk memetakan peran SNMP dalam monitoring kinerja dan ketersediaan jaringan telekomunikasi, mengidentifikasi keunggulan, keterbatasan, serta relevansinya di tengah perkembangan teknologi observability modern. Pendekatan ini memberikan sudut pandang sintesis yang lebih menyeluruh sehingga dapat menjadi dasar akademik maupun praktis bagi pengembangan sistem monitoring jaringan generasi berikutnya.

KAJIAN LITERATUR

Konsep Dasar Network Monitoring

Network monitoring merupakan proses pengawasan, pengukuran, dan analisis kondisi jaringan secara berkelanjutan untuk memastikan seluruh perangkat, link komunikasi, serta layanan jaringan beroperasi sesuai standar performa dan ketersediaan yang telah ditetapkan. Pada lingkungan telekomunikasi modern, monitoring tidak hanya berfungsi untuk mendeteksi perangkat yang mengalami gangguan, tetapi juga untuk memberikan visibilitas menyeluruh terhadap performa jaringan secara real-time maupun periodik, sehingga administrator dapat melakukan tindakan preventif sebelum terjadi penurunan kualitas layanan. Konsep ini menjadi bagian penting dari network management karena memungkinkan identifikasi dini terhadap kondisi slow response, congestion, packet loss, maupun kegagalan perangkat.

Secara umum, tujuan utama network monitoring adalah menjaga kinerja (performance), ketersediaan (availability), dan keandalan (reliability) jaringan. Untuk mencapai tujuan tersebut, sistem monitoring mengumpulkan berbagai parameter penting, seperti throughput, bandwidth utilization, latency, jitter, packet loss, uptime, CPU utilization, memory usage, dan interface status. Parameter-parameter ini digunakan untuk menilai kualitas layanan (Quality of Service/QoS) sekaligus mengevaluasi pencapaian target Service Level Agreement (SLA). Dengan adanya pemantauan yang kontinu, organisasi dapat melakukan capacity planning, optimasi trafik, dan perencanaan ekspansi jaringan secara lebih akurat.

Dalam implementasinya, network monitoring umumnya mencakup dua pendekatan utama, yaitu fault monitoring dan performance monitoring. Fault monitoring berfokus pada deteksi gangguan, seperti perangkat down, link terputus, atau layanan tidak dapat diakses. Sementara itu, performance monitoring berorientasi pada pengukuran kualitas operasional jaringan, misalnya utilisasi bandwidth, waktu tunda, dan beban sumber daya perangkat. Kombinasi kedua pendekatan ini sangat penting pada jaringan telekomunikasi karena gangguan tidak selalu ditandai oleh kondisi down, tetapi sering kali diawali oleh degradasi performa secara bertahap yang memengaruhi pengalaman pengguna akhir.

Pada jaringan operator telekomunikasi dan enterprise, network monitoring juga berperan sebagai dasar bagi proses proactive maintenance dan early warning system. Dengan membangun baseline performa normal, sistem dapat mendeteksi anomali ketika terjadi lonjakan trafik, peningkatan latensi, atau kenaikan beban CPU yang tidak wajar. Pendekatan ini sangat penting untuk meminimalkan downtime, meningkatkan mean time to repair (MTTR), dan menjaga kepatuhan SLA, khususnya pada layanan yang bersifat kritikal seperti komunikasi data, VoIP, video streaming, dan konektivitas cloud.

Seiring perkembangan teknologi menuju cloud computing, IoT, SDN, dan edge computing, kebutuhan network monitoring juga berkembang dari sekadar pemantauan perangkat menjadi network observability yang lebih holistik. Namun demikian, konsep dasar monitoring tetap berakar pada pengumpulan data performa dan availability dari elemen jaringan sebagai dasar analisis dan pengambilan keputusan. Oleh karena itu, pemahaman konsep dasar network monitoring menjadi landasan penting sebelum membahas penggunaan Simple Network Management Protocol (SNMP) sebagai salah satu protokol monitoring yang paling luas digunakan.

Simple Network Management Protocol (SNMP)

Simple Network Management Protocol (SNMP) merupakan protokol standar yang digunakan untuk monitoring, pengelolaan, dan pertukaran informasi manajemen jaringan antara perangkat jaringan dan sistem pengelola. SNMP dirancang agar administrator dapat memperoleh data operasional perangkat secara terstruktur, seperti status antarmuka, utilisasi bandwidth, beban CPU, penggunaan memori, serta berbagai parameter kesehatan perangkat lainnya. Keunggulan utama SNMP terletak pada sifatnya yang ringan, terstandarisasi, dan kompatibel lintas vendor, sehingga sangat luas digunakan pada jaringan telekomunikasi, enterprise, maupun pusat data.

Jurnal Multidisiplin Teknik, Sains, Pendidikan dan Teknologi

E-ISSN: 3064-6103
Volume 3, **Number** 2, Juli 2026
https://doi.org/10.62671/suliwa.v3i2.261

Secara arsitektural, SNMP terdiri atas tiga komponen utama, yaitu manager, agent, dan managed device. Manager atau Network Management System (NMS) berfungsi sebagai pusat pengawasan yang mengirim permintaan data dan menerima respons dari perangkat jaringan. Agent merupakan proses yang berjalan pada perangkat dan bertugas mengumpulkan informasi lokal, menyimpannya dalam basis data manajemen, serta merespons permintaan dari manager. Sementara itu, managed device adalah perangkat yang dimonitor, seperti router, switch, firewall, server, maupun perangkat radio telekomunikasi. Hubungan ketiga komponen ini membentuk model manager–agent yang menjadi dasar implementasi SNMP pada hampir semua sistem monitoring jaringan modern.

Informasi yang dipertukarkan dalam SNMP disimpan dalam struktur hierarkis yang disebut Management Information Base (MIB). Setiap objek pada MIB memiliki identitas unik berupa Object Identifier (OID) yang merepresentasikan parameter tertentu, misalnya interface status, packet counter, atau system uptime. Struktur ini memungkinkan perangkat dari vendor yang berbeda tetap dapat menyediakan data dengan format yang seragam, terutama melalui dukungan standard MIB seperti MIB-II. Selain itu, vendor juga dapat menambahkan enterprise-specific MIB untuk fitur yang lebih spesifik. Keberadaan MIB dan OID inilah yang membuat SNMP sangat efektif pada lingkungan multi-vendor network.

Dari sisi operasional, SNMP mendukung beberapa jenis perintah utama, yaitu GET, GETNEXT, GETBULK, SET, dan TRAP. Operasi GET digunakan untuk mengambil nilai suatu OID tertentu, sedangkan GETNEXT digunakan untuk membaca objek berikutnya dalam struktur MIB. Untuk pengambilan data tabel dalam jumlah besar, digunakan GETBULK agar lebih efisien. Sementara itu, SET memungkinkan manager mengubah nilai konfigurasi tertentu pada perangkat. Selain model request-response tersebut, SNMP juga mendukung TRAP sebagai mekanisme notifikasi asinkron, yaitu perangkat secara otomatis mengirim pesan ke manager ketika terjadi peristiwa penting, seperti link down, CPU overload, atau perangkat tidak dapat diakses.

Seiring perkembangannya, SNMP memiliki tiga versi utama, yaitu SNMPv1, SNMPv2c, dan SNMPv3. SNMPv1 merupakan versi awal dengan fungsi dasar monitoring. SNMPv2c memperkenalkan peningkatan efisiensi, terutama melalui dukungan GETBULK untuk pengambilan data tabel yang lebih cepat. Sementara itu, SNMPv3 menjadi versi yang paling direkomendasikan karena menambahkan mekanisme autentikasi, otorisasi, dan enkripsi, sehingga lebih aman digunakan pada jaringan modern. Fitur keamanan ini sangat penting untuk melindungi akses terhadap MIB dan mencegah manipulasi data monitoring oleh pihak yang tidak berwenang.

Dalam praktik monitoring jaringan, SNMP umumnya diterapkan melalui dua pendekatan, yaitu polling dan trap-based monitoring. Polling digunakan untuk memperoleh data performa secara periodik, seperti trafik antarmuka dan penggunaan CPU, sedangkan trap digunakan untuk mendukung early warning system terhadap gangguan perangkat. Kombinasi kedua pendekatan ini menjadikan SNMP sebagai protokol yang sangat efektif untuk mendukung monitoring performa dan availability secara berkelanjutan.

Monitoring Kinerja dan Availability Jaringan

Monitoring kinerja dan availability jaringan merupakan dua aspek utama dalam manajemen jaringan telekomunikasi modern. Kinerja (performance) mengacu pada kemampuan jaringan dalam memberikan layanan sesuai parameter kualitas yang telah ditetapkan, sedangkan availability berkaitan dengan tingkat ketersediaan perangkat, link, dan layanan agar tetap dapat diakses secara kontinu. Kedua aspek ini saling berkaitan karena penurunan performa yang tidak terdeteksi sering kali menjadi indikasi awal gangguan yang pada akhirnya dapat menyebabkan downtime layanan. Oleh sebab itu, proses monitoring harus mampu memberikan visibilitas terhadap kondisi performa sekaligus status ketersediaan jaringan secara berkelanjutan.

Dalam aspek kinerja, beberapa parameter utama yang umum digunakan adalah throughput, bandwidth utilization, latency, jitter, packet loss, CPU utilization, memory usage, dan interface status. Throughput menunjukkan jumlah data aktual yang berhasil ditransmisikan dalam satuan waktu tertentu, sedangkan bandwidth utilization menggambarkan persentase pemakaian kapasitas link. Parameter latency dan jitter sangat penting untuk layanan real-time seperti VoIP dan video streaming, karena memengaruhi kualitas pengalaman pengguna. Sementara itu, packet loss menjadi indikator penting untuk menilai reliabilitas jalur komunikasi dan potensi kongesti pada jaringan. Selain parameter trafik, penggunaan CPU dan memori perangkat juga dipantau untuk memastikan perangkat tidak mengalami kelebihan beban yang dapat memengaruhi pemrosesan paket.

Dari sisi availability, indikator yang paling umum digunakan meliputi uptime, downtime, link status, device reachability, interface operational status, dan fault alert notification. Uptime menunjukkan lamanya perangkat atau layanan aktif tanpa gangguan, sedangkan downtime merepresentasikan durasi layanan tidak tersedia. Informasi ini sangat penting untuk menghitung persentase availability, yang biasanya dikaitkan dengan target Service Level Agreement (SLA) pada operator telekomunikasi dan enterprise. Selain itu, status antarmuka dan kemampuan perangkat untuk merespons ping atau polling dari sistem monitoring menjadi dasar dalam menentukan apakah perangkat masih dapat dijangkau oleh jaringan.

Jurnal Multidisiplin Teknik, Sains, Pendidikan dan Teknologi

E-ISSN: 3064-6103
Volume 3, **Number** 2, Juli 2026
https://doi.org/10.62671/suliwa.v3i2.261

Dalam praktiknya, monitoring kinerja dan availability sangat erat kaitannya dengan Quality of Service (QoS) dan Service Level Agreement (SLA). QoS berfokus pada kualitas teknis layanan, seperti delay, packet loss, dan throughput, sedangkan SLA menetapkan target formal terkait tingkat ketersediaan dan performa yang harus dipenuhi oleh penyedia layanan. Sebagai contoh, operator telekomunikasi sering menetapkan target availability hingga 99,9% atau lebih, sehingga sistem monitoring harus mampu mendeteksi gangguan sekecil apa pun secara cepat agar proses pemulihan dapat segera dilakukan. Dengan demikian, monitoring bukan hanya alat observasi, tetapi juga menjadi dasar pengambilan keputusan operasional dan evaluasi kepatuhan layanan.

Infrastruktur Multi-Vendor dalam Monitoring

Infrastruktur jaringan telekomunikasi modern pada umumnya dibangun dari perangkat yang berasal dari berbagai vendor dengan karakteristik perangkat keras, sistem operasi, dan model manajemen yang berbeda. Dalam satu lingkungan jaringan, perangkat router, switch, firewall, server, perangkat radio akses, hingga sistem transmisi dapat berasal dari produsen yang berbeda-beda, seperti Cisco, Huawei, Juniper, MikroTik, atau vendor perangkat radio tertentu. Kondisi ini membentuk lingkungan multi-vendor, yaitu jaringan heterogen yang menuntut mekanisme monitoring mampu bekerja secara seragam tanpa bergantung pada satu produsen tertentu. Pada jaringan operator telekomunikasi, kondisi ini sangat umum karena ekspansi jaringan dilakukan secara bertahap dan sering kali melibatkan integrasi perangkat legacy dengan perangkat generasi terbaru.

Keberadaan infrastruktur multi-vendor menimbulkan tantangan utama pada proses monitoring, yaitu interoperabilitas data dan konsistensi visibilitas performa antar perangkat. Setiap vendor umumnya memiliki fitur manajemen proprietary, model data internal, dan struktur telemetri yang berbeda. Jika sistem monitoring hanya mengandalkan tool bawaan masing-masing vendor, maka administrator akan menghadapi fragmentasi dashboard, duplikasi proses analisis, serta kesulitan dalam melakukan korelasi gangguan lintas domain jaringan. Oleh karena itu, dibutuhkan protokol monitoring yang bersifat vendor-neutral dan berbasis standar terbuka agar seluruh perangkat dapat dipantau melalui satu sistem manajemen terpusat.

Dalam konteks tersebut, Simple Network Management Protocol (SNMP) memiliki posisi yang sangat penting karena didukung oleh hampir seluruh perangkat jaringan modern maupun legacy. Melalui penggunaan MIB standar dan OID yang seragam, SNMP memungkinkan sistem Network Management System (NMS) mengumpulkan parameter seperti utilisasi bandwidth, status antarmuka, uptime, CPU load, dan trap alarm dari berbagai perangkat secara konsisten. Keunggulan ini menjadikan SNMP sebagai salah satu protokol yang paling efektif untuk sentralisasi monitoring pada lingkungan multi-vendor. Selain memudahkan integrasi, pendekatan ini juga menurunkan risiko vendor lock-in karena organisasi tidak perlu bergantung pada satu platform monitoring proprietary tertentu.

Pada sisi lain, perkembangan streaming telemetry modern memang menawarkan visibilitas data yang lebih granular, namun implementasinya pada lingkungan multi-vendor masih menghadapi tantangan, terutama terkait ketidakkonsistenan model data YANG, variasi dukungan gNMI/gRPC, serta perbedaan kemampuan telemetry antar perangkat. Tidak semua perangkat legacy mendukung telemetry modern secara native, sehingga migrasi penuh dari SNMP menuju telemetry sering kali memerlukan investasi perangkat baru yang cukup besar. Dalam kondisi tersebut, SNMP tetap menjadi pilihan yang paling realistis untuk mempertahankan baseline monitoring yang universal dan stabil.

Evolusi Monitoring Modern dan Telemetry

Perkembangan arsitektur jaringan modern, seperti cloud computing, software-defined networking (SDN), edge computing, virtualized network functions (VNF), dan Internet of Things (IoT), telah meningkatkan kompleksitas proses monitoring jaringan secara signifikan. Jika pada jaringan konvensional monitoring cukup berfokus pada status perangkat dan counter antarmuka, maka pada jaringan modern kebutuhan telah bergeser menuju visibilitas layanan end-to-end, analisis perilaku trafik secara granular, dan deteksi anomali secara real-time. Perubahan kebutuhan ini mendorong evolusi metode monitoring dari pendekatan polling-based menuju streaming telemetry dan network observability yang lebih adaptif.

Pada pendekatan tradisional, Simple Network Management Protocol (SNMP) menggunakan mekanisme polling periodik, yaitu sistem Network Management System (NMS) secara berkala meminta data ke perangkat untuk membaca nilai counter tertentu. Meskipun efektif untuk pengumpulan data performa dasar, model ini memiliki keterbatasan pada aspek granularitas, skalabilitas, dan overhead kontrol, terutama pada jaringan dengan ribuan perangkat dan trafik yang sangat dinamis. Interval polling yang terlalu panjang dapat menyebabkan anomali singkat tidak terdeteksi, sedangkan polling terlalu cepat dapat meningkatkan beban perangkat dan bandwidth manajemen. Keterbatasan inilah yang menjadi salah satu alasan utama munculnya pendekatan telemetry modern.

Streaming telemetry merupakan evolusi dari monitoring tradisional yang memungkinkan perangkat mengirim data secara kontinu atau event-driven ke collector tanpa menunggu permintaan polling. Dengan mekanisme ini, data performa seperti trafik interface, CPU, memori, dan metrik layanan dapat dikirim dengan resolusi lebih tinggi, misalnya

Jurnal Multidisiplin Teknik, Sains, Pendidikan dan Teknologi

E-ISSN: 3064-6103
Volume 3, **Number** 2, Juli 2026
https://doi.org/10.62671/suliwa.v3i2.261

per detik atau bahkan dalam orde milidetik. Pendekatan ini mendukung visibilitas terhadap microburst traffic, transient fault, hop-by-hop latency, dan flow behavior yang sulit ditangkap oleh SNMP. Selain itu, telemetry modern biasanya memanfaatkan model data yang lebih terstruktur, seperti YANG, serta protokol seperti gNMI, gRPC, atau NETCONF, sehingga lebih fleksibel untuk otomatisasi dan analitik tingkat lanjut.

Seiring dengan perkembangan telemetry, konsep monitoring juga berevolusi menjadi network observability, yaitu kemampuan untuk memahami kondisi internal jaringan berdasarkan data yang dihasilkan dari metrics, logs, traces, dan telemetry. Jika monitoring tradisional berfokus pada "apa yang terjadi", maka observability berupaya menjawab "mengapa hal itu terjadi" melalui korelasi lintas layer dan analisis dependensi layanan. Pendekatan ini sangat penting pada lingkungan cloud-native dan microservices, di mana performa aplikasi sangat dipengaruhi oleh interaksi banyak komponen yang tersebar.

Perkembangan terbaru juga menunjukkan integrasi monitoring dengan AI-driven analytics untuk mendukung predictive maintenance, anomaly detection, dan self-healing network. Dengan memanfaatkan data telemetry beresolusi tinggi, sistem dapat memprediksi potensi kemacetan, lonjakan CPU, atau penurunan kualitas layanan sebelum benar-benar terjadi. Namun demikian, implementasi telemetry modern belum selalu dapat menggantikan SNMP sepenuhnya, terutama pada lingkungan multi-vendor dan perangkat legacy yang belum mendukung model telemetry terbaru. Oleh sebab itu, pendekatan yang semakin banyak digunakan adalah hybrid monitoring, yaitu kombinasi SNMP sebagai baseline health monitoring dengan telemetry modern untuk kebutuhan visibilitas real-time dan analitik mendalam.

METODE PENELITIAN

Penelitian ini menggunakan metode structured literature review (SLR) untuk mengkaji secara komprehensif peran Simple Network Management Protocol (SNMP) dalam monitoring kinerja dan availability jaringan telekomunikasi. Metode ini dipilih karena mampu memberikan proses kajian yang sistematis, transparan, dan dapat direplikasi dalam menelaah perkembangan penelitian terkait SNMP, baik pada aspek performa, ketersediaan layanan, interoperabilitas multi-vendor, maupun relevansinya terhadap evolusi network observability modern. Selain itu, pendekatan ini memungkinkan penulis untuk membandingkan hasil penelitian terdahulu dengan posisi penelitian yang dilakukan, sehingga kebaruan artikel dapat ditunjukkan secara lebih jelas.

Desain Penelitian

Desain penelitian yang digunakan adalah structured literature review dengan pendekatan thematic-comparative synthesis. Pada desain ini, artikel-artikel yang relevan dipetakan dan dikelompokkan berdasarkan tema utama yang berkaitan dengan tujuan penelitian, yaitu peran SNMP dalam monitoring kinerja jaringan, kontribusinya terhadap availability, keunggulan pada lingkungan multi-vendor, keterbatasan SNMP pada jaringan modern, serta relevansinya terhadap monitoring generasi berikutnya.

Pendekatan komparatif digunakan untuk membandingkan hasil penelitian terdahulu dalam lima tahun terakhir dengan hasil sintesis yang dilakukan pada penelitian ini. Melalui pendekatan tersebut, posisi penelitian dapat ditunjukkan secara eksplisit, terutama pada aspek kelebihan, perbedaan fokus, keterbatasan, serta kontribusi baru yang ditawarkan dibandingkan penelitian lain yang sejenis.

Strategi Pencarian Literatur

Proses pencarian literatur dilakukan secara sistematis melalui beberapa basis data ilmiah bereputasi, seperti Google Scholar, IEEE Xplore, ScienceDirect, MDPI, Scopus-indexed journals, serta jurnal nasional terakreditasi SINTA. Pemilihan beberapa sumber tersebut bertujuan untuk memperoleh literatur yang tidak hanya relevan secara akademik, tetapi juga mencerminkan perkembangan terbaru pada monitoring jaringan telekomunikasi.

Kata kunci yang digunakan dalam proses pencarian meliputi kombinasi istilah seperti SNMP network monitoring, telecommunication network performance, network availability monitoring, multi-vendor network management, serta network telemetry and observability. Literatur yang dipilih dibatasi pada publikasi lima tahun terakhir (2021–2026) agar hasil sintesis tetap sesuai dengan perkembangan teknologi monitoring modern, khususnya pada transisi dari pendekatan polling tradisional menuju telemetry dan observability.

Kriteria Inklusi dan Eksklusi

Untuk menjaga kualitas dan relevansi kajian, penelitian ini menerapkan kriteria inklusi dan eksklusi dalam proses seleksi artikel. Kriteria inklusi meliputi artikel yang secara spesifik membahas penggunaan SNMP, monitoring jaringan, performa, availability, telemetry, atau interoperabilitas multi-vendor, diterbitkan pada rentang tahun 2021–2026, tersedia dalam bentuk full text, serta berasal dari jurnal nasional maupun internasional yang memiliki reputasi akademik yang baik.

Jurnal Multidisiplin Teknik, Sains, Pendidikan dan Teknologi

E-ISSN: 3064-6103
Volume 3, **Number** 2, Juli 2026
https://doi.org/10.62671/suliwa.v3i2.261

Sementara itu, artikel yang dikeluarkan dari proses kajian adalah artikel duplikat, artikel yang hanya berfokus pada konfigurasi perangkat tanpa analisis monitoring, artikel di luar ruang lingkup telekomunikasi dan manajemen jaringan, serta sumber yang tidak menyediakan hasil atau diskusi yang mendukung sintesis penelitian. Penerapan kriteria ini bertujuan agar literatur yang digunakan benar-benar mampu menjawab fokus penelitian dan mendukung analisis komparatif secara valid.

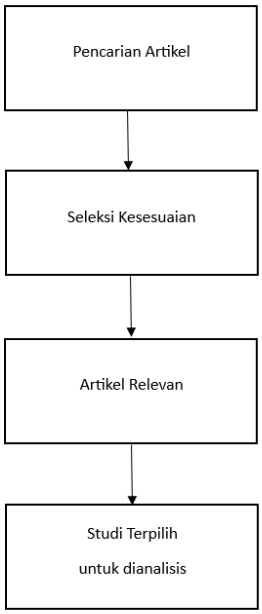
Teknik Sintesis dan Analisis Data

Data yang diperoleh dari proses seleksi literatur kemudian dianalisis menggunakan pendekatan thematic synthesis dan comparative analysis. Pada tahap awal, artikel-artikel yang lolos seleksi diidentifikasi berdasarkan tema-tema utama yang telah ditetapkan pada desain penelitian. Selanjutnya, hasil penelitian terdahulu dibandingkan untuk menemukan pola persamaan, perbedaan, kekuatan, dan kelemahan masing-masing penelitian.

Melalui proses ini, penulis dapat mengidentifikasi research gap yang masih terbuka, khususnya terkait kajian yang secara komprehensif memetakan peran SNMP dari sisi performa, availability, interoperabilitas, keterbatasan, dan relevansi masa depan. Hasil sintesis kemudian disajikan dalam bentuk narasi pembahasan dan tabel perbandingan penelitian terdahulu, dengan tambahan baris “Penelitian ini” untuk menunjukkan posisi kontribusi artikel secara jelas.

Alur Penelitian

Alur penelitian pada studi ini mengikuti tahapan structured literature review yang dimulai dari proses pencarian artikel, seleksi kesesuaian berdasarkan fokus penelitian, identifikasi artikel yang relevan, hingga penetapan studi terpilih untuk proses sintesis dan analisis. Gambar 1 memperlihatkan alur penelitian yang digunakan pada artikel ini.



Gambar 1. Flowchart alur penelitian structured literature review

Flowchart pada Gambar 1 menunjukkan bahwa proses penelitian dilakukan secara bertahap dan sistematis, dimulai dari pencarian artikel pada database ilmiah, kemudian dilakukan seleksi berdasarkan kesesuaian topik dan kriteria penelitian. Artikel yang memenuhi kriteria selanjutnya dikategorikan sebagai artikel relevan dan digunakan sebagai studi terpilih untuk proses sintesis tematik dan komparatif.

HASIL DAN PEMBAHASAN

Peran SNMP dalam Monitoring Kinerja Jaringan

Berdasarkan hasil sintesis literatur, Simple Network Management Protocol (SNMP) masih menunjukkan peran yang sangat signifikan dalam monitoring kinerja jaringan telekomunikasi, terutama pada pengawasan parameter performa dasar yang menjadi indikator kualitas layanan. Sebagian besar penelitian yang ditelaah menunjukkan bahwa SNMP efektif dalam menyediakan data operasional perangkat secara periodik melalui mekanisme polling, sehingga administrator dapat memantau kondisi jaringan secara kontinu dan terpusat. Parameter yang paling sering dimonitor

Jurnal Multidisiplin Teknik, Sains, Pendidikan dan Teknologi

E-ISSN: 3064-6103
Volume 3, **Number** 2, Juli 2026
https://doi.org/10.62671/suliwa.v3i2.261

meliputi throughput, bandwidth utilization, latency, packet loss, CPU utilization, memory usage, serta interface status, yang semuanya berperan penting dalam menjaga stabilitas layanan data dan komunikasi.

Dari sisi implementasi, penelitian Alwanto dan Yel (2025) menunjukkan bahwa integrasi SNMP dengan platform Cacti mampu menghasilkan observasi performa jaringan yang akurat, khususnya pada pengukuran throughput, delay, packet loss, dan availability. Hasil tersebut memperlihatkan bahwa SNMP tidak hanya efektif untuk membaca counter perangkat, tetapi juga mampu mendukung evaluasi Quality of Service (QoS) secara berkelanjutan. Pada konteks enterprise maupun operator telekomunikasi, kemampuan ini sangat penting untuk proses capacity planning, traffic optimization, dan deteksi dini bottleneck jaringan.

Selain pada layer perangkat, SNMP juga berkontribusi terhadap visibilitas utilisasi sumber daya internal, seperti CPU dan memori router, switch, server, maupun perangkat radio. Pemantauan parameter ini memungkinkan administrator mendeteksi kondisi resource saturation sebelum berdampak pada penurunan kualitas layanan. Dalam lingkungan trafik yang dinamis, pendekatan ini sangat membantu untuk mencegah performance degradation yang berpotensi menyebabkan congestion atau service disruption. Dengan demikian, SNMP berfungsi tidak hanya sebagai alat observasi, tetapi juga sebagai fondasi untuk proactive maintenance.

Hasil sintesis juga menunjukkan bahwa kekuatan utama SNMP pada monitoring kinerja terletak pada kemudahan integrasi dengan berbagai Network Management System (NMS), baik berbasis open-source maupun proprietary. Integrasi ini memungkinkan visualisasi grafik performa historis, analisis tren penggunaan bandwidth, dan identifikasi pola lonjakan trafik secara lebih sistematis. Dalam konteks telekomunikasi, data historis tersebut menjadi dasar penting untuk prediksi kebutuhan kapasitas jaringan dan evaluasi performa layanan terhadap target SLA.

Namun demikian, hasil kajian juga menunjukkan bahwa efektivitas SNMP dalam monitoring kinerja sangat dipengaruhi oleh interval polling dan kapasitas perangkat. Pada jaringan dengan trafik sangat dinamis, interval polling yang terlalu panjang dapat menyebabkan anomali sesaat tidak tertangkap, sedangkan interval yang terlalu pendek dapat meningkatkan beban kontrol. Temuan ini menunjukkan bahwa meskipun SNMP tetap efektif sebagai baseline performance monitoring, optimasi parameter polling tetap menjadi faktor penting agar hasil monitoring tetap representatif.

Kontribusi SNMP terhadap Availability Jaringan

Selain berperan dalam monitoring kinerja, hasil sintesis literatur menunjukkan bahwa Simple Network Management Protocol (SNMP) memiliki kontribusi yang sangat penting dalam menjaga availability jaringan telekomunikasi. Availability dalam konteks ini merujuk pada tingkat ketersediaan perangkat, link, dan layanan agar tetap dapat diakses sesuai target Service Level Agreement (SLA). Pada lingkungan operator telekomunikasi maupun enterprise, gangguan sekecil apa pun yang tidak terdeteksi dapat berdampak langsung terhadap kualitas pengalaman pengguna dan kontinuitas layanan. Oleh karena itu, kemampuan SNMP dalam memberikan visibilitas status perangkat secara kontinu menjadi salah satu faktor utama yang mendukung service continuity assurance.

Berdasarkan penelitian terdahulu, SNMP banyak dimanfaatkan untuk memantau parameter yang berhubungan langsung dengan availability, seperti system uptime, interface operational status, link up/down, device reachability, dan fault notification. Penelitian Sakti, Sapri, dan Akbar (2024) menunjukkan bahwa implementasi SNMP yang diintegrasikan dengan email notification mampu mempercepat administrator dalam mendeteksi perangkat down dan segera melakukan tindakan pemulihan. Hal serupa juga ditunjukkan oleh Vingestin et al. (2023), di mana integrasi SNMP dengan Telegram notification meningkatkan kecepatan distribusi informasi gangguan secara real-time kepada administrator jaringan. Temuan ini memperlihatkan bahwa kekuatan SNMP tidak hanya terletak pada pengumpulan data, tetapi juga pada kemampuannya mendukung mekanisme early warning system.

Salah satu kontribusi utama SNMP terhadap availability adalah melalui pemanfaatan trap notification, yaitu notifikasi asinkron yang dikirim perangkat secara otomatis ketika terjadi peristiwa tertentu, seperti link down, interface error, CPU overload, atau kegagalan layanan. Dibandingkan hanya mengandalkan polling periodik, penggunaan trap mampu mempercepat proses deteksi gangguan karena informasi dikirim segera setelah event terjadi. Dalam jaringan telekomunikasi yang memiliki target availability tinggi, mekanisme ini sangat efektif untuk menurunkan Mean Time to Detect (MTTD) dan secara tidak langsung mempercepat Mean Time to Repair (MTTR).

Hasil sintesis juga menunjukkan bahwa data historis uptime dan downtime yang diperoleh melalui SNMP sangat berguna untuk evaluasi kepatuhan SLA. Operator dapat menghitung persentase availability perangkat atau layanan berdasarkan data tersebut, misalnya target 99,9% uptime dalam periode tertentu. Informasi ini penting tidak hanya untuk evaluasi teknis, tetapi juga untuk kebutuhan audit layanan, pelaporan performa jaringan, dan pengambilan keputusan terkait redundansi atau ekspansi infrastruktur.

Meskipun demikian, efektivitas SNMP dalam mendukung availability juga memiliki keterbatasan, terutama jika perangkat hanya mengandalkan polling-based failure detection. Pada interval polling yang terlalu jarang, terdapat kemungkinan gangguan singkat (transient outage) tidak tercatat, sehingga nilai availability yang dihitung menjadi

Jurnal Multidisiplin Teknik, Sains, Pendidikan dan Teknologi

E-ISSN: 3064-6103
Volume 3, **Number** 2, Juli 2026
https://doi.org/10.62671/suliwa.v3i2.261

kurang representatif. Oleh karena itu, hasil kajian menunjukkan bahwa kombinasi polling periodik dan trap-based alerting merupakan pendekatan yang paling efektif untuk menjaga akurasi monitoring availability.

Keunggulan SNMP pada Infrastruktur Multi-Vendor

Salah satu temuan utama dari hasil sintesis literatur adalah bahwa Simple Network Management Protocol (SNMP) tetap memiliki keunggulan yang sangat kuat pada lingkungan jaringan multi-vendor. Infrastruktur telekomunikasi modern umumnya terdiri atas perangkat dari berbagai produsen, seperti router, switch, firewall, server, perangkat radio, dan sistem transmisi yang berasal dari vendor berbeda. Heterogenitas ini menimbulkan tantangan pada proses monitoring karena setiap vendor sering kali memiliki platform manajemen, format data, dan mekanisme telemetry proprietary yang tidak selalu kompatibel satu sama lain. Dalam kondisi tersebut, SNMP berperan sebagai protokol standar yang mampu menjembatani perbedaan antar perangkat sehingga seluruh elemen jaringan dapat dipantau melalui satu sistem terpusat.

Hasil kajian menunjukkan bahwa keunggulan utama SNMP pada lingkungan multi-vendor terletak pada dukungannya terhadap MIB standar dan OID yang bersifat vendor-neutral. Melalui struktur data yang terstandarisasi, parameter penting seperti utilisasi bandwidth, status antarmuka, system uptime, CPU load, dan trap alarm dapat diambil dari perangkat berbagai vendor dengan format yang relatif konsisten. Hal ini memberikan kemudahan bagi administrator untuk membangun dashboard monitoring terpadu tanpa harus bergantung pada network management tools proprietary milik masing-masing vendor.

Pada jaringan operator telekomunikasi, kemampuan ini sangat penting karena ekspansi jaringan sering dilakukan secara bertahap, sehingga perangkat legacy dan perangkat generasi terbaru harus tetap dapat dipantau secara bersamaan. SNMP memungkinkan perangkat lama yang tidak mendukung telemetry modern tetap dapat memberikan data performa dan availability melalui metode polling maupun trap. Dengan demikian, SNMP menjadi solusi yang sangat efektif untuk menjaga keseragaman visibilitas monitoring pada infrastruktur heterogen.

Keunggulan lain yang muncul dari hasil sintesis adalah kemampuan SNMP dalam mengurangi risiko vendor lock-in. Jika organisasi hanya menggunakan tool monitoring proprietary, maka analisis jaringan akan terfragmentasi ke dalam beberapa dashboard yang berbeda sesuai vendor perangkat. Kondisi ini menyulitkan korelasi gangguan lintas domain, meningkatkan kompleksitas operasional, dan memperbesar biaya integrasi. Dengan menggunakan SNMP sebagai lapisan monitoring universal, data dari berbagai vendor dapat dikonsolidasikan dalam satu Network Management System (NMS), sehingga proses analisis performa, fault management, dan perencanaan kapasitas menjadi lebih efisien.

Meskipun telemetry modern seperti gNMI atau gRPC menawarkan granularitas data yang lebih tinggi, hasil kajian menunjukkan bahwa implementasinya pada lingkungan multi-vendor masih belum sepenuhnya konsisten. Perbedaan dukungan model YANG, variasi fitur perangkat, serta keterbatasan perangkat legacy membuat migrasi penuh ke telemetry modern belum selalu realistis. Dalam konteks ini, SNMP tetap menunjukkan keunggulannya sebagai baseline monitoring layer yang universal, stabil, dan mudah diintegrasikan.

Keterbatasan SNMP pada Jaringan Modern

Meskipun hasil sintesis menunjukkan bahwa Simple Network Management Protocol (SNMP) masih sangat efektif untuk monitoring performa, availability, dan interoperabilitas multi-vendor, kajian literatur juga menegaskan adanya beberapa keterbatasan mendasar pada jaringan modern. Keterbatasan ini terutama muncul ketika SNMP diterapkan pada infrastruktur berskala besar, trafik yang sangat dinamis, serta arsitektur berbasis cloud, edge computing, SDN, dan layanan terdistribusi. Dalam lingkungan seperti ini, kebutuhan monitoring tidak lagi hanya berfokus pada device health, tetapi juga menuntut visibilitas yang lebih granular terhadap perilaku trafik dan dependensi layanan end-to-end.

Salah satu keterbatasan utama SNMP adalah penggunaan mekanisme polling periodik. Pada pendekatan ini, sistem monitoring harus secara terus-menerus meminta data ke perangkat untuk memperoleh nilai counter tertentu. Semakin besar jumlah perangkat dan semakin pendek interval polling, maka semakin tinggi pula overhead kontrol yang ditimbulkan, baik pada bandwidth manajemen maupun beban CPU perangkat. Sebaliknya, jika interval polling dibuat terlalu panjang, terdapat kemungkinan anomali singkat seperti microburst traffic atau transient fault tidak tercatat. Kondisi ini menyebabkan SNMP kurang optimal untuk menangkap peristiwa yang berlangsung sangat cepat pada jaringan modern dengan trafik bursty.

Keterbatasan berikutnya terletak pada aspek granularitas data dan resolusi waktu. Data SNMP pada umumnya berupa counter atau statistik agregat perangkat, sehingga kurang mampu memberikan visibilitas terhadap perilaku trafik pada level flow, session, atau hop-by-hop latency. Pada layanan modern seperti cloud-native application, microservices, atau virtual network functions, gangguan performa sering kali disebabkan oleh interaksi lintas layer yang tidak dapat

Jurnal Multidisiplin Teknik, Sains, Pendidikan dan Teknologi

E-ISSN: 3064-6103
Volume 3, **Number** 2, Juli 2026
https://doi.org/10.62671/suliwa.v3i2.261

dijelaskan hanya melalui counter interface. Akibatnya, SNMP memiliki keterbatasan dalam mendukung analisis akar masalah (root cause analysis) yang lebih kompleks.

Dari sisi skalabilitas, hasil sintesis juga menunjukkan bahwa SNMP menghadapi tantangan ketika diterapkan pada jaringan dengan ribuan node dan endpoint IoT. Proses polling terhadap sejumlah besar perangkat dapat meningkatkan management traffic secara signifikan dan berpotensi mengganggu efisiensi jaringan kontrol. Selain itu, tidak semua perangkat memiliki kapasitas pemrosesan yang cukup untuk merespons polling dengan frekuensi tinggi, terutama pada perangkat legacy atau perangkat akses dengan sumber daya terbatas.

Aspek keamanan juga menjadi salah satu keterbatasan penting, khususnya pada implementasi yang masih menggunakan SNMPv1 atau SNMPv2c. Kedua versi ini hanya mengandalkan community string tanpa enkripsi yang kuat, sehingga rentan terhadap penyadapan atau penyalahgunaan akses. Meskipun SNMPv3 telah menyediakan autentikasi dan enkripsi, implementasinya pada lingkungan multi-vendor terkadang masih menghadapi tantangan kompatibilitas konfigurasi dan kompleksitas manajemen kredensial.

Hasil kajian ini menunjukkan bahwa keterbatasan SNMP bukan berarti protokol ini kehilangan relevansinya, melainkan menegaskan bahwa SNMP lebih tepat ditempatkan sebagai baseline monitoring layer untuk health monitoring perangkat. Untuk kebutuhan visibilitas granular, analitik real-time, dan predictive observability, diperlukan integrasi dengan streaming telemetry modern. Dengan demikian, keterbatasan yang teridentifikasi pada subbab ini justru memperkuat argumen bahwa masa depan monitoring jaringan telekomunikasi akan lebih realistis jika mengadopsi arsitektur hybrid monitoring.

Perbandingan dengan Penelitian Terdahulu

Untuk memperjelas posisi penelitian yang dilakukan, Tabel 4.1 menyajikan perbandingan beberapa penelitian terdahulu dalam lima tahun terakhir dengan penelitian pada artikel ini. Perbandingan dilakukan berdasarkan fokus penelitian, metode, temuan utama, serta kelemahan atau research gap, sehingga pembaca dapat melihat secara langsung kontribusi yang ditawarkan oleh penelitian ini dibandingkan penelitian lain yang sejenis.

Tabel 1. Perbandingan Penelitian Terdahulu dengan Penelitian Ini

Penelitian	Fokus	Metode	Temuan Utama	Kelemahan / Gap
Vingestin et al. (2023)	Monitoring perangkat dengan notifikasi Telegram	Implementasi SNMP + Telegram	Mempercepat penyampaian alarm gangguan perangkat	Fokus hanya fault notification
Alhilali et al. (2023)	Real-time traffic monitoring server	Implementasi SNMP pada server	Efisien untuk pengawasan trafik server	Terbatas pada server
Sakti et al. (2024)	Monitoring availability perangkat	Implementasi SNMP + Email Alert	Respons admin lebih cepat	Fokus availability
Alwanto & Yel (2025)	Evaluasi QoS enterprise network	SNMP + Cacti	Akurat untuk QoS	Masih implementatif
Yaseen (2025)	Evolusi monitoring Modern	Survey literature	Pergeseran ke telemetry	Belum spesifik telecom
Penelitian ini	Kajian komprehensif peran SNMP	SLR + comparative synthesis	SNMP tetap relevan sebagai baseline hybrid monitoring	Belum ada validasi eksperimental

KESIMPULAN

Berdasarkan hasil structured literature review yang telah dilakukan, dapat disimpulkan bahwa Simple Network Management Protocol (SNMP) masih memiliki peran yang sangat relevan dalam monitoring kinerja dan availability jaringan telekomunikasi. Dari sisi performa, SNMP terbukti efektif dalam memantau parameter utama seperti throughput, bandwidth utilization, latency, packet loss, CPU utilization, dan interface status, sehingga mampu memberikan network performance visibility yang dibutuhkan untuk menjaga kualitas layanan. Dari sisi availability, SNMP berkontribusi melalui pemantauan uptime, link status, serta mekanisme trap notification yang mendukung deteksi dini gangguan dan percepatan respons administrator.

Hasil sintesis juga menunjukkan bahwa salah satu kekuatan utama SNMP terletak pada kemampuannya mendukung interoperabilitas monitoring pada lingkungan multi-vendor. Dukungan terhadap MIB standar dan sifat vendor-neutral menjadikan SNMP tetap efektif sebagai fondasi monitoring universal, khususnya pada jaringan telekomunikasi yang masih mengintegrasikan perangkat legacy dan perangkat modern dari berbagai vendor. Namun demikian, penelitian ini juga mengidentifikasi keterbatasan SNMP pada aspek granularitas data, skalabilitas polling, visibilitas flow-level, serta kebutuhan analitik real-time pada jaringan modern berbasis cloud, SDN, edge, dan IoT.

Jurnal Multidisiplin Teknik, Sains, Pendidikan dan Teknologi

E-ISSN: 3064-6103
Volume 3, **Number** 2, Juli 2026
https://doi.org/10.62671/suliwa.v3i2.261

Berdasarkan temuan tersebut, penelitian ini menegaskan bahwa posisi SNMP pada monitoring generasi berikutnya bukan lagi sebagai satu-satunya solusi, melainkan sebagai baseline monitoring layer yang sangat efektif jika dikombinasikan dengan streaming telemetry dan network observability. Dengan demikian, novelty utama artikel ini terletak pada pemetaan SNMP sebagai bagian dari arsitektur hybrid monitoring yang menggabungkan interoperabilitas multi-vendor dengan granularitas telemetry modern.

REFERENSI

Alhilali, A. H., Al Farawn, A., & Mjhool, A. (2023). Design and implement a real-time network traffic management system using SNMP protocol. Eastern-European Journal of Enterprise Technologies, 5(9), 35–44. https://doi.org/10.15587/1729-4061.2023.286528

Alwanto, H., & Yel, M. B. (2025). Analysis of enterprise network performance using the SNMP (Simple Network Management Protocol) method. Journal Innovations Computer Science, 4(2), 335–344. https://doi.org/10.56347/jics.v4i2.346

Case, J. D., Fedor, M., Schoffstall, M. L., & Davin, J. (1990). Simple Network Management Protocol (SNMP) (RFC 1157). RFC Editor. https://doi.org/10.17487/RFC1157

Kreutz, D., Ramos, F. M. V., Verissimo, P. E., Rothenberg, C. E., Azodolmolky, S., & Uhlig, S. (2015). Software-defined networking: A comprehensive survey. Proceedings of the IEEE, 103(1), 14–76.

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., … Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. BMJ, 372, n71. https://doi.org/10.1136/bmj.n71

Sakti, P., Sapri, S., & Akbar, A. A. (2024). Implementation of network device monitoring system using SNMP protocol with email notification. Jurnal Komputer, Informasi dan Teknologi, 4(1), 8. https://doi.org/10.53697/jkomitek.v4i1.1732

Vingestin, I., Kalsum, T. U., & Mardiana, Y. (2023). The design of network monitoring system using SNMP protocol with Telegram notification. Jurnal Media Computer Science, 2(1), 93–100. https://doi.org/10.37676/jmcs.v2i1.3441

Yaseen, N. (2025). From counters to telemetry: A survey of programmable network-wide monitoring. Network, 5(3), 38. https://doi.org/10.3390/network5030038

Zhang, P., Zhang, H., Dai, Y., Zeng, C., Wang, J., & Liao, J. (2025). NTP-INT: Network traffic prediction-driven in-band network telemetry for high-load switches. Journal of Network and Computer Applications, 242, 104265. https://doi.org/10.1016/j.jnca.2025.104265

Zhou, X., Li, Y., Chen, M., & Liu, J. (2022). Hybrid network monitoring architecture for cloud-edge infrastructures: Combining SNMP and streaming telemetry. IEEE Access, 10, 118420–118433.