



Department of Digital Business

Journal of Artificial Intelligence and Digital Business (RIGGS)

Homepage: <https://journal.ilmudata.co.id/index.php/RIGGS>

Vol. 5 No. 1 (2026) pp: 7355-7365

P-ISSN: 2963-9298, e-ISSN: 2963-914X

Sistem Monitoring Multi Perangkat Jaringan Berbasis Simple Network Management Protocol (SNMP) dengan Notifikasi Telegram

Awin Hersa Ardani¹, Raisul Azhar,² Ondi Asroni³

^{1,2,3}Ilmu Komputer, Teknik, Universitas Bumigora

ardanhersa@gmail.com

Abstrak

Perkembangan teknologi jaringan nirkabel menuntut sistem monitoring yang mampu memantau perangkat jaringan secara real-time dan terpusat. Monitoring manual berpotensi menimbulkan keterlambatan deteksi gangguan, berdampak pada penurunan kualitas layanan, dan meningkatnya risiko downtime operasional. Ketiadaan notifikasi otomatis mengharuskan administrator melakukan pengecekan berkala secara langsung, yang tidak efisien terutama saat administrator tidak berada di lokasi. Penelitian ini bertujuan merancang dan mensimulasikan prototipe Sistem Monitoring Multi Perangkat Jaringan Berbasis Simple Network Management Protocol (SNMP) dengan Notifikasi Telegram pada lingkungan jaringan virtual. Metode yang digunakan adalah Network Development Life Cycle (NDLC), dibatasi pada tiga tahapan: Analysis, Design, dan Simulation Prototype. Sistem monitoring menggunakan aplikasi The Dude sebagai Network Management System (NMS) yang melakukan polling SNMP terhadap perangkat wireless access point virtual melalui router MikroTik. Jaringan dibagi menjadi dua segmen, yaitu segmen operasional (192.168.55.0/24) dan segmen monitoring (192.168.7.0/24). Notifikasi dirancang untuk dikirimkan secara otomatis kepada administrator melalui Telegram Bot menggunakan script MikroTik RouterOS. Simulasi dilakukan melalui tujuh skenario pengujian meliputi kondisi normal, gangguan konektivitas, pemutusan koneksi, pemulihan koneksi, monitoring periodik, visualisasi status, dan pengiriman notifikasi otomatis. Hasil simulasi menunjukkan bahwa prototipe mampu mendeteksi perubahan status wireless access point secara akurat dengan tingkat keberhasilan 100% pada seluruh skenario. Notifikasi Telegram rata-rata terkirim dalam rentang 5 hingga 15 detik setelah perubahan status terdeteksi, menunjukkan peningkatan responsivitas yang signifikan dibandingkan metode monitoring manual.

Kata kunci: Monitoring Jaringan, SNMP, Telegram Bot, The Dude, MikroTik, Notifikasi Real-Time

1. Latar Belakang

Perkembangan teknologi jaringan komputer yang pesat telah membawa transformasi signifikan dalam pengelolaan infrastruktur teknologi informasi (Anwar, 2020), khususnya dalam kebutuhan monitoring dan manajemen perangkat jaringan secara terpusat. Infrastruktur jaringan modern terdiri dari berbagai perangkat seperti router, switch, dan wireless access point yang saling terhubung untuk mendukung layanan berbasis internet. Stabilitas dan ketersediaan jaringan menjadi faktor krusial dalam menjaga kualitas layanan, sehingga diperlukan sistem monitoring yang mampu bekerja secara efektif dan real-time.

Pada banyak implementasi jaringan skala kecil hingga menengah, proses monitoring masih dilakukan secara manual melalui pengecekan langsung ke perangkat. Metode ini memiliki keterbatasan dalam mendeteksi gangguan secara cepat, terutama ketika administrator tidak berada di lokasi. Ketiadaan sistem notifikasi otomatis menyebabkan keterlambatan penanganan ketika terjadi perangkat down atau gangguan konektivitas. Permasalahan yang dihadapi adalah bagaimana merancang sistem monitoring yang mampu mendeteksi perubahan status perangkat secara otomatis dan memberikan notifikasi real-time kepada administrator.

Simple Network Management Protocol (SNMP) merupakan protokol standar yang banyak digunakan dalam manajemen jaringan untuk memantau kondisi perangkat berbasis IP (Ariyadi & Prasetyo, 2021). SNMP memungkinkan pengambilan performa seperti status konektivitas, penggunaan bandwidth, dan kondisi perangkat jaringan secara terpusat. Meskipun sistem monitoring berbasis SNMP telah banyak diterapkan melalui tools The Dude, sebagian besar masih berfokus pada visualisasi dashboard tanpa integrasi notifikasi instan yang fleksibel.

Seiring berkembangnya aplikasi pesan instan, integrasi monitoring dengan platform seperti Telegram menjadi solusi alternatif yang efektif. Telegram menyediakan bot yang memungkinkan sistem mengirimkan notifikasi

otomatis ketika terjadi perubahan kondisi perangkat. Beberapa penelitian sebelumnya membahas monitoring SNMP dan integrasi notifikasi, namun masih bergantung pada platform tertentu atau layanan tambahan yang kompleks.

Penelitian ini menawarkan pendekatan alternatif dengan merancang sistem monitoring multi perangkat berbasis SNMP yang diintegrasikan dengan Telegram Bot dalam lingkungan virtual. Kebaruan penelitian ini terletak pada integrasi antara mekanisme polling SNMP berbasis The Dude dengan notifikasi Telegram Bot secara langsung melalui skrip MikroTik RouterOS, tanpa memerlukan server perantara. Tujuan penelitian ini adalah membangun prototipe sistem monitoring yang efisien dan mampu meningkatkan responsivitas pengelolaan jaringan.

Urgensi penelitian ini terletak pada kebutuhan nyata industri perhotelan terhadap layanan cepat dan andal, sehingga proses deteksi dan penanganan gangguan harus berlangsung otomatis dan responsif. Penelitian oleh Pratama dan Raharjo (2021) menunjukkan bahwa penerapan SNMP pada sistem monitoring virtual dapat meningkatkan efisiensi pengawasan perangkat hingga 40% dibandingkan metode manual. Sementara itu, Lestari dkk. (2022) mengembangkan sistem monitoring jaringan berbasis simulasi yang terintegrasi dengan Telegram Bot, yang terbukti mampu memberikan informasi kondisi perangkat secara real-time kepada administrator meskipun sistem berjalan di lingkungan virtual. Hasil-hasil penelitian terdahulu tersebut memperkuat urgensi pengembangan sistem monitoring SNMP berbasis simulasi yang menjadi fokus penelitian ini.

2. Landasan Teori

2.1. Simple Network Management Protocol (SNMP)

Simple Network Management Protocol (SNMP) adalah protokol standar Internet untuk mengelola dan memantau perangkat jaringan yang didefinisikan dalam RFC 1157 dan kemudian diperbarui dalam RFC 3416 untuk SNMPv3. SNMP menggunakan arsitektur manager-agent di mana SNMP manager melakukan query terhadap SNMP agent yang tertanam pada perangkat jaringan untuk mengumpulkan informasi operasional seperti status interface, utilisasi CPU, memory usage, dan parameter performa lainnya yang disimpan dalam struktur data Management Information Base (MIB). Peran utama protokol ini adalah menyediakan parameter status perangkat secara real-time yang meliputi ketersediaan perangkat, penggunaan sumber daya, hingga performa jaringan.

SNMP memiliki tiga komponen utama yaitu: (1) SNMP Manager sebagai pusat kendali yang bertugas menerima, mengelola, dan menganalisis data dari perangkat jaringan; (2) SNMP Agent yang merupakan komponen perangkat lunak tertanam pada perangkat jaringan untuk memantau kondisi dan melaporkan status kepada manager; serta (3) Management Information Base (MIB) yang berfungsi sebagai tempat penyimpanan data serta struktur variabel yang menggambarkan kondisi perangkat. Komunikasi antara manager dan agent dilakukan melalui mekanisme polling berkala maupun SNMP trap untuk pemberitahuan kejadian kritis secara otomatis.

Dalam konteks penelitian ini, SNMP digunakan untuk melakukan pemantauan terhadap perangkat wireless access point pada lingkungan virtual. Sistem monitoring terpusat memperoleh informasi kondisi access point seperti status online atau offline melalui polling SNMP yang dilakukan secara berkala oleh The Dude sebagai Network Management System (NMS). Pemanfaatan SNMP terbukti efektif dalam penelitian sebelumnya karena kemampuannya memantau banyak perangkat sekaligus dan menampilkan data detail seperti bandwidth serta status perangkat secara terpusat dalam satu dashboard.

2.2. Wireless LAN dan Access Point

Wireless Local Area Network (WLAN) merupakan evolusi dari sistem jaringan tradisional yang memanfaatkan propagasi gelombang radio untuk mentransmisikan data tanpa memerlukan media kabel fisik. WLAN menggunakan frekuensi radio pada pita 2,4 GHz dan 5 GHz untuk memfasilitasi komunikasi data antara perangkat klien dengan access point. Dua pita frekuensi utama tersebut memiliki karakteristik propagasi berbeda; pita 2,4 GHz memiliki jangkauan lebih jauh tetapi rentan interferensi, sedangkan pita 5 GHz menawarkan kapasitas data lebih tinggi dengan jangkauan lebih terbatas.

Access Point (AP) merupakan perangkat infrastruktur jaringan yang berfungsi sebagai bridge antara segmen jaringan kabel dengan perangkat wireless client. AP menerima sinyal frekuensi radio dari perangkat klien kemudian mengubahnya menjadi sinyal digital yang diteruskan ke jaringan kabel. Dalam perspektif manajemen jaringan, access point termasuk perangkat yang dapat dipantau menggunakan SNMP sehingga memungkinkan pengumpulan data terkait performa operasional seperti status konektivitas, jumlah klien yang tersambung, kualitas sinyal, serta statistik lalu lintas. Pemantauan ini dapat dilakukan pada lingkungan virtual sehingga proses analisis dan pengembangan sistem monitoring tidak mengganggu jaringan fisik yang sedang berjalan.

2.3. MikroTik RouterOS

MikroTik RouterOS adalah sistem operasi berbasis Linux yang dikembangkan untuk menyediakan solusi routing dan manajemen jaringan. RouterOS mendukung berbagai protokol jaringan termasuk SNMP untuk monitoring, BGP dan OSPF untuk routing dinamis, serta fitur firewall dan Quality of Service (QoS) untuk traffic management. Dalam konteks penelitian ini, RouterOS digunakan sebagai platform untuk mengeksekusi script notifikasi Telegram melalui fitur tool fetch yang dapat mengirimkan HTTP request ke external API. MikroTik dapat dioperasikan baik pada perangkat RouterBoard maupun komputer personal sehingga mampu beradaptasi pada kebutuhan jaringan skala kecil hingga menengah dengan tingkat efisiensi biaya yang tinggi.

Kajian literatur yang relevan menunjukkan bahwa integrasi MikroTik dengan sistem notifikasi berbasis Telegram Bot meningkatkan kecepatan penerimaan informasi terkait anomali jaringan. Model komunikasi yang bersifat real-time melalui aplikasi pesan instan memberikan akses cepat kepada administrator jaringan untuk mengetahui perubahan status perangkat sehingga pengelolaan ketersediaan jaringan dapat dilakukan secara lebih efisien. Selain itu, MikroTik dapat menjadi bagian dari arsitektur monitoring berbasis SNMP pada berbagai platform manajemen jaringan, baik berbasis server lokal maupun cloud, karena kemampuannya menyediakan statistik jaringan seperti status koneksi, utilisasi bandwidth, serta trafik klien access point secara terpusat.

2.4. Telegram Bot sebagai Media Notifikasi

Telegram Bot adalah automated account yang dapat diprogram untuk melakukan berbagai tugas termasuk mengirim notifikasi, merespons perintah, dan berinteraksi dengan pengguna melalui Telegram Bot API. Dalam konteks monitoring jaringan, bot dapat diintegrasikan dengan sistem Network Management System (NMS) untuk mengirimkan alert secara real-time kepada administrator ketika terjadi perubahan status perangkat. Secara arsitektur, Telegram memanfaatkan Bot API yang terhubung dengan sistem monitoring untuk memfasilitasi pertukaran data dua arah. Selain menerima pesan alert yang bersumber dari event SNMP, bot juga mampu menanggapi perintah administrator untuk menampilkan data operasional access point secara langsung.

Integrasi Telegram Bot dengan SNMP menunjukkan peningkatan efisiensi monitoring karena proses transformasi data mentah menjadi informasi yang mudah dipahami dilakukan secara otomatis. Notifikasi yang dikirimkan juga menyertakan dokumentasi riwayat kejadian pada percakapan bot sehingga dapat digunakan sebagai log untuk keperluan analisis perbaikan jaringan. Telegram dikenal sebagai aplikasi pesan yang ringan, aman, dan memiliki fitur otomatisasi melalui antarmuka bot. Dengan memanfaatkan fasilitas ini, status perangkat access point maupun komputer yang mengalami masalah dapat dikirimkan secara otomatis kepada administrator melalui pesan real-time sehingga mendukung proses maintenance jaringan menjadi lebih responsif, terukur, dan efisien.

2.5. The Dude sebagai Network Management System

The Dude adalah aplikasi Network Management System (NMS) yang dikembangkan oleh MikroTik dan digunakan secara luas dalam monitoring jaringan berbasis SNMP. Aplikasi ini menyediakan antarmuka grafis yang memungkinkan administrator memvisualisasikan topologi jaringan secara real-time, memantau status perangkat melalui indikator warna, serta mengonfigurasi aturan notifikasi berdasarkan perubahan kondisi perangkat. The Dude melakukan proses polling SNMP terhadap perangkat jaringan secara berkala untuk memperbarui status pada peta topologi, di mana perangkat yang aktif ditampilkan dengan warna hijau dan perangkat yang mengalami gangguan ditampilkan dengan warna merah.

Dalam penelitian ini, The Dude digunakan sebagai server monitoring yang melakukan proses polling SNMP terhadap perangkat wireless access point melalui router MikroTik. Interval polling dikonfigurasi sesuai kebutuhan untuk memastikan deteksi perubahan status yang cepat. Ketika The Dude mendeteksi perubahan status perangkat, sistem secara otomatis memicu eksekusi script pada MikroTik RouterOS yang mengirimkan notifikasi melalui Telegram Bot API. Pendekatan ini memungkinkan integrasi langsung antara NMS dan platform notifikasi tanpa memerlukan server perantara tambahan, sehingga arsitektur sistem menjadi lebih sederhana dan efisien dalam lingkungan jaringan virtual.

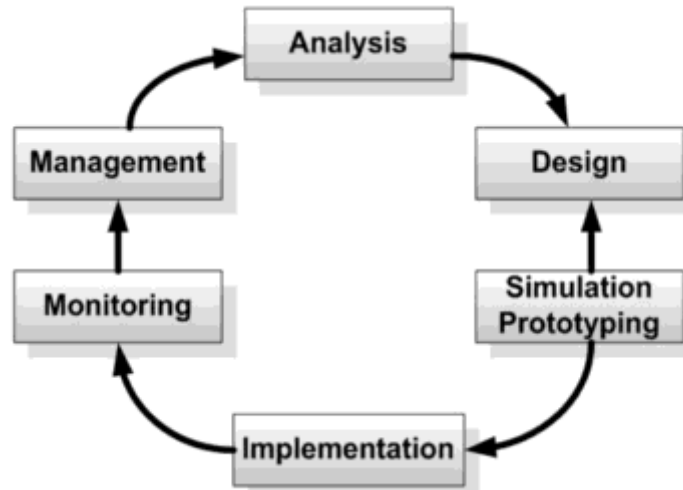
2.6. Virtualisasi dan Network Development Life Cycle (NDLC)

Virtualisasi adalah teknologi yang memungkinkan abstraksi sumber daya hardware fisik menjadi multiple instance virtual yang dapat menjalankan sistem operasi secara independen. VMware Workstation merupakan salah satu platform virtualisasi tipe hosted hypervisor yang berjalan di atas sistem operasi host dan memungkinkan eksekusi multiple virtual machine secara concurrent dengan mekanisme resource sharing yang efisien. Hal ini memberikan fleksibilitas tinggi pada proses pengujian, pemodelan, serta simulasi arsitektur jaringan dalam berbagai kondisi operasional tanpa memerlukan perangkat fisik tambahan.

Network Development Life Cycle (NDLC) adalah metodologi yang digunakan sebagai kerangka kerja dalam pengembangan dan pengelolaan sistem jaringan komputer. NDLC memiliki tahapan-tahapan yang meliputi Analysis, Design, Simulation Prototype, Implementation, Monitoring, dan Management. Dalam penelitian ini, tahapan yang diterapkan dibatasi pada tiga tahap pertama yaitu Analysis, Design, dan Simulation Prototype, sesuai dengan tujuan penelitian yang berfokus pada perancangan dan pengujian sistem dalam lingkungan simulasi virtual. Pemilihan NDLC sebagai metodologi memberikan kerangka kerja yang sistematis dan terstruktur sehingga setiap tahapan pengembangan sistem dapat dilaksanakan secara terarah dan dapat dievaluasi dengan jelas.

3. Metode Penelitian

Penelitian ini menggunakan pendekatan rancang bangun sistem dengan metode Network Development Life Cycle (NDLC) yang meliputi tahapan analisis, desain, dan Simulation Prototype. Metode ini dipilih karena memberikan kerangka kerja yang sistematis dalam pengembangan sistem jaringan.



Gambar 1. Metodologi NDLC

Tahap analisis dilakukan untuk mengidentifikasi kebutuhan sistem monitoring, meliputi perangkat yang akan dipantau, parameter pemantauan, serta kebutuhan notifikasi real-time. Parameter utama adalah status perangkat jaringan (up/down) yang diperoleh melalui mekanisme SNMP. Selain itu, ditentukan pula kebutuhan integrasi dengan Telegram Bot API sebagai media pengiriman notifikasi otomatis.

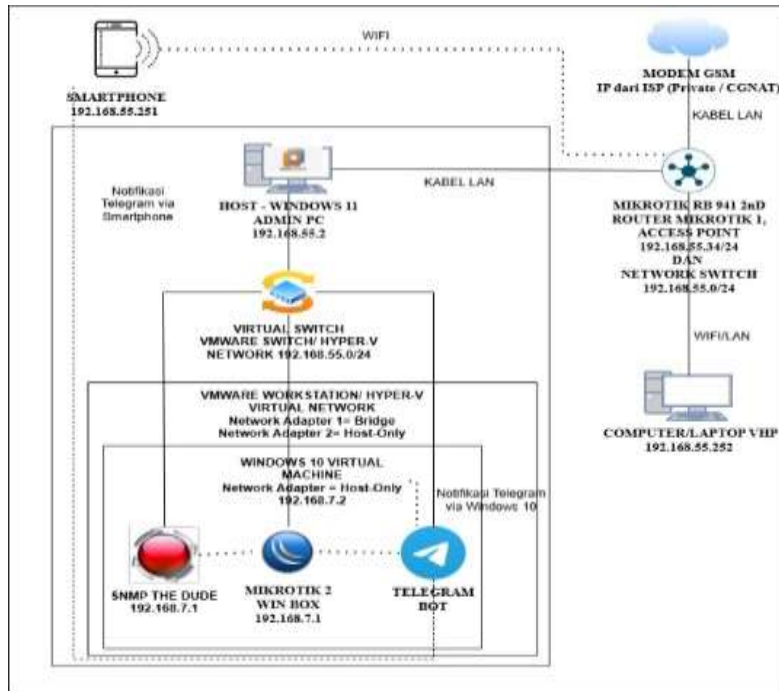
Tahap desain mencakup perancangan arsitektur sistem monitoring dan topologi jaringan virtual. Sistem dirancang dengan mekanisme polling SNMP untuk mendeteksi perubahan status perangkat secara berkala. Apabila terjadi perubahan kondisi perangkat, sistem akan memicu proses pengiriman notifikasi melalui Telegram.

Tahap simulation prototype dilakukan dengan mensimulasikan kondisi normal (perangkat aktif), kondisi gangguan (perangkat down), dan kondisi pemulihan (perangkat kembali aktif). Parameter yang dievaluasi meliputi keberhasilan sistem dalam mendeteksi perubahan status perangkat serta kecepatan respons notifikasi.

3.1. Kebutuhan Perangkat Keras dan Perangkat Lunak

Kebutuhan perangkat penelitian ini meliputi: Server Monitoring (VM 1) dengan CPU 4 Core, RAM 8 GB, Storage 100 GB, sistem operasi Linux Ubuntu Server atau Windows 11, aplikasi The Dude dan Telegram Bot API. Router MikroTik (VM 2) CPU 1 Core AMD 3.1 GHz, RAM 96 MB, Storage 2 GB, MikroTik RouterOS v7.x dengan layanan SNMP. Access Point Virtual (VM 3) CPU 1-2 Core, RAM 1 GB, Storage 10 GB dengan Firmware SNMP Support. PC Administrator (VM 4) CPU 2 Core, RAM 4 GB, Storage 60 GB, Windows 10 dengan Winbox dan Telegram Desktop. Switch Virtual menggunakan VMware Virtual Network Adapter, dan Host Virtualisasi berupa laptop fisik CPU AMD RYZEN 7, RAM 16 GB, SSD 512 GB, VMware Workstation 17.

3.2. Topologi Jaringan



Gambar 2. Topologi Jaringan

Pada penelitian ini digunakan subnet mask 255.255.255.0 (/24) dengan dua segmen jaringan sesuai fungsi perangkat. Segmen jaringan operasional menggunakan subnet 192.168.55.0/24 dengan router MikroTik RB941 2nD sebagai gateway utama. Segmen jaringan monitoring menggunakan subnet 192.168.7.0/24 yang dijalankan pada lingkungan virtualisasi, digunakan khusus untuk layanan monitoring SNMP The Dude, Winbox, dan Telegram Bot.

3.3. Identifikasi Masalah dan Ruang Lingkup Virtual

Permasalahan utama yang diangkat dalam penelitian ini adalah keterbatasan proses pemantauan perangkat jaringan pada lingkungan virtual. Administrator jaringan masih melakukan pengecekan kondisi perangkat secara manual tanpa sistem deteksi otomatis, yang memerlukan waktu dan tenaga signifikan. Gangguan pada perangkat jaringan sering kali tidak terdeteksi secara cepat karena sistem bawaan perangkat tidak menyediakan notifikasi real-time yang dapat diakses dari jarak jauh, sehingga menyebabkan keterlambatan respons dan downtime berkepanjangan yang berdampak pada kualitas layanan. Berdasarkan permasalahan tersebut, diperlukan solusi sistem monitoring otomatis berbasis SNMP yang dapat mendeteksi gangguan secara real-time dan mengirimkan notifikasi langsung kepada administrator melalui platform komunikasi yang mudah diakses seperti Telegram.

Penelitian ini dilakukan secara virtual menggunakan VMware Workstation untuk menghindari risiko gangguan pada jaringan operasional nyata. Ruang lingkup virtual mencakup lima komponen utama yaitu: (1) SNMP Server (The Dude) berupa VM dengan Ubuntu atau Windows sebagai pusat monitoring terpusat; (2) Router MikroTik berupa VM dengan RouterOS sebagai pengatur lalu lintas dan eksekutor script notifikasi; (3) Access Point Virtual berupa 1 unit VM sebagai objek monitoring utama; (4) PC Administrator berupa VM sebagai perangkat akses dan pengelolaan sistem; serta (5) Jaringan Virtual dengan subnet 192.168.55.0/24 dan 192.168.7.0/24 sebagai koneksi antar perangkat. Pendekatan virtualisasi ini memungkinkan pengujian dilakukan secara aman, terkontrol, dan dapat diulang tanpa memerlukan infrastruktur fisik tambahan.

3.4. Rancangan Arsitektur Sistem dan Flowchart

Rancangan arsitektur sistem monitoring dirancang dengan model tiga lapis. Pertama, lapisan perangkat (device layer) di mana wireless access point virtual dikonfigurasi dengan SNMP agent yang aktif. Kedua, lapisan manajemen (management layer) yang diwakili oleh The Dude sebagai NMS yang menjalankan polling SNMP berkala dan menyimpan status perangkat. Ketiga, lapisan notifikasi (notification layer) yang terdiri dari script MikroTik RouterOS terhubung ke Telegram Bot API. Topologi menggunakan model star dengan The Dude sebagai pusat pemantauan yang terhubung ke router MikroTik sebagai gateway utama jaringan. Seluruh perangkat

utama diberikan alamat IP statis untuk memastikan konsistensi komunikasi SNMP dan mempermudah identifikasi perangkat saat terjadi gangguan.

Alur kerja sistem yang dirancang dapat digambarkan melalui flowchart sebagai berikut: sistem dimulai dengan proses inisialisasi dan konfigurasi SNMP pada seluruh perangkat virtual. Selanjutnya, The Dude sebagai SNMP Manager melakukan polling berkala terhadap setiap perangkat jaringan. Sistem kemudian membandingkan status terkini dengan status sebelumnya. Jika tidak ada perubahan, proses polling dilanjutkan ke interval berikutnya. Jika terdeteksi perubahan status (UP ke DOWN atau DOWN ke UP), sistem secara otomatis memicu eksekusi script pada MikroTik RouterOS menggunakan perintah tool fetch untuk mengirimkan HTTP POST request ke Telegram Bot API. Notifikasi yang dikirimkan memuat informasi nama perangkat, alamat IP, status kondisi, dan waktu kejadian. Proses ini berjalan secara berulang dan otomatis selama sistem aktif, tanpa memerlukan intervensi manual dari administrator.

3.5. Konfigurasi Telegram Bot

Pembuatan Telegram Bot dilakukan menggunakan layanan BotFather yang merupakan bot resmi Telegram untuk pembuatan dan pengelolaan bot. Proses pembuatan diawali dengan membuka aplikasi Telegram dan mencari BotFather pada kolom pencarian. Selanjutnya dikirimkan perintah /newbot untuk memulai proses pembuatan bot baru. Administrator kemudian menentukan nama bot (misalnya "Monitoring Server") dan username yang harus diakhiri dengan kata "bot" (misalnya "wirelessbot"). Setelah proses selesai, BotFather memberikan token unik yang digunakan untuk mengakses HTTP API. Token ini berfungsi sebagai kredensial autentikasi sistem monitoring untuk mengirimkan pesan melalui bot.

Setelah token diperoleh, langkah selanjutnya adalah mendapatkan chat_id administrator menggunakan bot "Get My ID" di Telegram. Chat_id ini diperlukan agar sistem dapat mengirimkan notifikasi ke akun Telegram yang tepat. Konfigurasi token dan chat_id kemudian diintegrasikan ke dalam script MikroTik RouterOS dalam format perintah tool fetch dengan parameter URL yang mengarah ke endpoint Telegram Bot API, beserta parameter text yang berisi pesan notifikasi. Script ini dikonfigurasi untuk dieksekusi secara otomatis oleh The Dude setiap kali terjadi perubahan status perangkat yang terpantau, sehingga integrasi antara NMS dan platform notifikasi dapat berjalan tanpa intervensi manual.

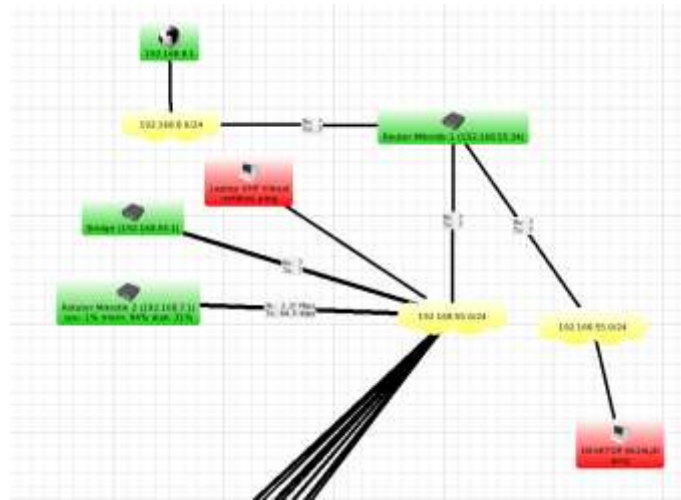
3.6. Tahap Simulation Prototype

Tahap Simulation Prototype merupakan tahap akhir dalam metodologi NDLC yang diterapkan pada penelitian ini. Tujuan utama tahap ini adalah menghasilkan representasi awal sistem yang dapat diuji secara konseptual untuk menilai kinerja mekanisme pemantauan jaringan dalam lingkungan virtual. Struktur jaringan hotel direpresentasikan secara virtual dengan menempatkan perangkat jaringan sebagai objek utama pemantauan, termasuk komputer yang digunakan sebagai perangkat operasional Visual Hotel Program (VHP) yang dimasukkan dalam skenario simulasi untuk memastikan keandalannya melalui dukungan sistem monitoring.

Prototipe sistem dikonfigurasi agar server monitoring mampu menerima dan mengolah data SNMP dari access point maupun perangkat lain dalam jaringan virtual. Data hasil pemantauan dikaji dan dalam skenario gangguan dirancang untuk menghasilkan notifikasi otomatis yang dikirimkan kepada administrator melalui Telegram Bot. Evaluasi dilakukan terhadap tiga aspek utama yaitu: efektivitas pemantauan yang mengukur kemampuan sistem mendeteksi perubahan status perangkat secara akurat; kesesuaian konfigurasi yang menilai apakah parameter SNMP dan mekanisme notifikasi sesuai kebutuhan operasional; serta kemampuan sistem memberikan respons cepat terhadap gangguan yang terjadi selama simulasi. Hasil dari tahap ini menjadi validasi konsep sebelum sistem direkomendasikan untuk diterapkan pada jaringan fisik nyata.

4. Hasil dan Diskusi

Sistem monitoring bekerja menggunakan mekanisme polling SNMP yang dilakukan secara berkala oleh server monitoring. Proses ini memungkinkan sistem membaca status perangkat secara real-time. Alur kerja sistem dimulai dari pembacaan status perangkat oleh SNMP Manager, kemudian sistem membandingkan status terbaru dengan status sebelumnya. Jika terdeteksi perubahan kondisi, sistem akan mengeksekusi skrip notifikasi yang terhubung dengan Telegram Bot API.



Gambar 3. Alur Proses Monitoring dan Pengiriman Notifikasi

Skenario pengujian meliputi tiga kondisi utama: kondisi normal (UP) di mana perangkat aktif dan tidak ada notifikasi yang dikirim, kondisi gangguan (DOWN) ketika perangkat terputus dan sistem mengirimkan notifikasi peringatan, serta kondisi pemulihan (RECOVERY) ketika perangkat kembali aktif dan sistem mengirimkan notifikasi pemulihan kepada administrator.

Tabel 1. Hasil Pengujian

No	Skenario Simulasi	Objek	Metode	Keterangan
1	Kondisi Normal Jaringan perangkat jaringan, termasuk access point virtual, beroperasi normal dan tidak ada perangkat yang mengalami kondisi down)	Access Point (Virtual)	SNMP Polling (The Dude)	Access point merespons polling SNMP secara konsisten dan stabil. Pada The Dude, perangkat ditampilkan berwarna hijau yang menandakan kondisi jaringan normal tanpa gangguan.
2	Gangguan Konektivitas Jaringan (Terjadi gangguan sinyal atau koneksi sehingga kualitas koneksi menurun dan respons perangkat menjadi tidak stabil)	Access Point (Virtual)	SNMP Polling	The Dude mendeteksi access point tidak merespons polling SNMP dalam batas waktu tertentu, sehingga status perangkat berubah menjadi down secara otomatis.
3	Pemutusan Jaringan Secara Sengaja (Koneksi access point diputus secara manual untuk mensimulasikan kondisi gangguan jaringan)	Access Point (Virtual)	SNMP Request	Access point tidak memberikan respons terhadap permintaan SNMP sehingga sistem menandai perangkat sebagai offline dan menampilkan indikator merah pada The Dude.
4	Pengujian WiFi Jarak Dekat (1–10 Meter) (Access point kembali memberikan sinyal dengan kualitas baik dan koneksi berjalan stabil)	Access Point (Virtual)	SNMP Polling	Setelah koneksi dipulihkan dan jarak berada dalam jangkauan optimal, access point kembali merespons polling SNMP dan status berubah menjadi up.
5	Monitoring Access Point Secara Periodik (Pemantauan status dan respons access point dilakukan secara berkala)	Access Point (Virtual)	SNMP Periodik (The Dude)	Monitoring berjalan secara otomatis dan berulang tanpa intervensi manual. Hasil pengujian menunjukkan sistem stabil dan tidak mengalami error selama proses pemantauan berlangsung.

	menggunakan mekanisme polling)	SNMP			
6	Visualisasi Perangkat (Sistem menampilkan kondisi operasional perangkat jaringan secara visual melalui aplikasi monitoring)	Status (Sistem)	Access Point (Virtual)	The Dude (NMS)	Setiap perubahan status access point langsung divisualisasikan pada antarmuka The Dude menggunakan indikator warna, sehingga memudahkan administrator dalam memantau kondisi jaringan.
7	Pengiriman Notifikasi Otomatis (Sistem mengirimkan peringatan ketika terjadi perubahan status perangkat jaringan)	Otomatis	Access Point (Virtual)	Telegram Bot	Notifikasi otomatis dikirim ke Telegram administrator ketika access point mengalami gangguan (DOWN) maupun saat koneksi kembali normal (UP) sebagai peringatan dini.

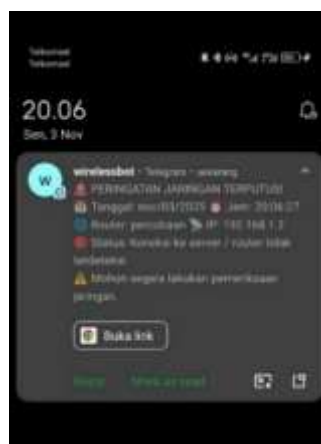
Berdasarkan hasil pengujian pada Tabel 1, seluruh 7 skenario pengujian berhasil dijalankan dengan tingkat keberhasilan 100%. Sistem mampu mendeteksi perubahan status perangkat secara akurat dan konsisten pada setiap iterasi pengujian. Notifikasi Telegram terkirim secara otomatis pada kondisi gangguan (DOWN) maupun pemulihan (UP) tanpa kegagalan selama sesi pengujian berlangsung.

Berdasarkan pengamatan selama simulasi, notifikasi rata-rata terkirim dalam rentang 5 hingga 15 detik setelah perubahan status perangkat terdeteksi, tergantung interval polling yang dikonfigurasi pada The Dude. Hasil ini menunjukkan peningkatan responsivitas yang signifikan dibandingkan metode monitoring manual.

4.1. Notifikasi Telegram



Gambar 4. Tampilan Notifikasi Telegram saat Perangkat UP



Gambar 5. Tampilan Notifikasi Telegram saat Perangkat DOWN

Notifikasi yang dikirimkan oleh sistem memuat informasi penting berupa nama perangkat, alamat IP, waktu kejadian, serta status perangkat (up, down, atau recovery). Informasi tersebut memungkinkan administrator untuk

segera mengetahui lokasi dan jenis gangguan yang terjadi tanpa harus melakukan pengecekan langsung ke perangkat jaringan.

Integrasi SNMP dengan Telegram Bot API terbukti mampu meningkatkan efektivitas monitoring jaringan. Sistem dapat mendeteksi perubahan status perangkat secara otomatis dan mengirimkan notifikasi secara real-time. Mekanisme ini mengurangi ketergantungan terhadap metode monitoring manual yang mengharuskan administrator melakukan pengecekan berkala secara langsung.

4.2. Pembahasan Arsitektur Sistem

Arsitektur sistem monitoring yang dirancang dalam penelitian ini mengikuti model tiga lapis yang terdiri dari lapisan perangkat (device layer), lapisan manajemen (management layer), dan lapisan notifikasi (notification layer). Pada lapisan perangkat, wireless access point virtual dikonfigurasi dengan SNMP agent yang aktif dan dapat diakses oleh NMS. Lapisan manajemen diwakili oleh The Dude yang menjalankan proses polling SNMP secara berkala dan menyimpan status perangkat. Lapisan notifikasi terdiri dari script MikroTik RouterOS yang terhubung dengan Telegram Bot API untuk meneruskan informasi gangguan kepada administrator.

Perancangan jaringan dibagi ke dalam dua segmen untuk meningkatkan keteraturan dan kestabilan sistem. Segmen jaringan operasional menggunakan subnet 192.168.55.0/24 dengan router MikroTik RB941 2nD sebagai gateway utama, sedangkan segmen jaringan monitoring menggunakan subnet 192.168.7.0/24 yang dijalankan pada lingkungan virtualisasi dan digunakan khusus untuk layanan monitoring SNMP The Dude, Winbox, dan Telegram Bot. Pemisahan segmen jaringan ini memastikan bahwa trafik monitoring tidak mengganggu trafik operasional dan sebaliknya, sehingga performa kedua segmen dapat dijaga secara optimal.

Mekanisme kerja sistem dimulai ketika The Dude secara periodik mengirimkan permintaan SNMP kepada SNMP agent pada setiap access point. Jika dalam batas waktu yang ditentukan agent tidak memberikan respons, The Dude akan mengubah status perangkat menjadi DOWN dan secara otomatis memicu eksekusi script notifikasi pada MikroTik. Script tersebut menggunakan perintah tool fetch untuk mengirimkan HTTP POST request ke endpoint Telegram Bot API dengan parameter berupa chat ID administrator dan pesan yang berisi informasi nama perangkat, alamat IP, waktu kejadian, serta status perangkat. Proses yang sama terjadi ketika perangkat kembali aktif dan statusnya berubah menjadi UP, sehingga administrator mendapatkan notifikasi pemulihan secara otomatis.

4.3. Implikasi dan Pengembangan Lanjutan

Hasil penelitian ini memiliki implikasi praktis yang signifikan bagi pengelola jaringan komputer, khususnya pada lingkungan skala kecil hingga menengah seperti hotel, perkantoran, atau institusi pendidikan yang mengandalkan infrastruktur MikroTik. Sistem yang dikembangkan dapat diimplementasikan dengan biaya operasional yang relatif rendah karena memanfaatkan perangkat lunak yang sudah ada (The Dude dan MikroTik RouterOS) tanpa memerlukan lisensi tambahan. Integrasi dengan Telegram sebagai platform notifikasi juga tidak memerlukan biaya layanan sehingga solusi ini sangat terjangkau dan dapat diadopsi secara luas.

Meskipun penelitian ini berhasil mendemonstrasikan efektivitas sistem dalam lingkungan virtual, terdapat beberapa arah pengembangan yang dapat dilakukan pada penelitian selanjutnya. Pertama, migrasi dari SNMPv2c ke SNMPv3 untuk meningkatkan keamanan komunikasi melalui enkripsi dan autentikasi yang lebih kuat. Kedua, pengembangan fitur penyimpanan histori gangguan dan analisis tren untuk mendukung perencanaan kapasitas jaringan yang lebih baik. Ketiga, implementasi sistem pada jaringan fisik nyata untuk memvalidasi performa dan reliabilitas pada kondisi produksi yang sesungguhnya. Keempat, perluasan cakupan monitoring ke perangkat selain access point seperti switch, router, dan server untuk membangun sistem monitoring jaringan yang lebih komprehensif.

4.4. Konsistensi dan Reliabilitas Sistem

Berdasarkan hasil pengujian berulang dalam lingkungan simulasi, sistem monitoring menunjukkan kemampuan yang konsisten dalam mendeteksi perubahan status perangkat dan mengirimkan notifikasi sesuai kondisi yang terjadi. Selama proses simulasi, sistem dapat menjalankan fungsi monitoring tanpa mengalami kegagalan deteksi status perangkat, sehingga menunjukkan reliabilitas fungsi sistem pada tahap prototipe. Tabel 4.4 berikut merangkum hasil pengujian notifikasi Telegram secara kuantitatif berdasarkan catatan waktu pengujian dan waktu notifikasi diterima.

Tabel 2, Ringkasan Hasil Pengujian Notifikasi Telegram

No	Kondisi Perangkat	Status di The Dude	Waktu Pengujian	Waktu Notifikasi Diterima	Selisih (detik)	Hasil Notifikasi
1	Normal UP	Hijau (Up)	09:30:07	-	-	Tidak ada pesan (normal)
2	Access Point DOWN	Merah (Down)	09:33:05	09:33:08	3 detik	Pesan "Host Down" diterima
3	Access Point UP (Pemulihan)	Hijau (Up)	09:37:35	09:37:40	5 detik	Pesan "Host UP" diterima
4	Access Point DOWN (Ulang)	Merah (Down)	10:10:20	10:10:23	3 detik	Pesan "Host Down" diterima
5	Stabil Kembali UP	Hijau (Up)	10:18:10	10:18:14	4 detik	Pesan "Host Up" diterima

Pengujian berulang pada skenario 4 dan 5 membuktikan bahwa sistem mampu bekerja secara konsisten tanpa mengalami message loss atau kegagalan pengiriman notifikasi, dengan rata-rata delay 3–5 detik pada setiap siklus.

4.5. Monitoring Multiple Device dan Integrasi VHP

Meskipun dalam lingkungan simulasi penelitian ini hanya digunakan satu access point virtual, sistem monitoring berbasis The Dude secara arsitektural dirancang untuk mendukung pemantauan lebih dari satu perangkat jaringan secara bersamaan. Mekanisme SNMP polling memungkinkan The Dude melakukan pemantauan terhadap banyak SNMP agent dalam satu jaringan, di mana setiap perangkat yang ditambahkan akan dipantau secara independen dan menghasilkan notifikasi Telegram secara terpisah ketika terjadi perubahan status. Hal ini menunjukkan bahwa keterbatasan jumlah perangkat pada tahap simulasi tidak membatasi kemampuan sistem untuk diimplementasikan pada jaringan hotel dengan jumlah access point yang lebih banyak pada tahap pengembangan selanjutnya.

Integrasi sistem monitoring dengan lingkungan Visual Hotel Program (VHP) menunjukkan hasil yang positif. Sistem mampu mendeteksi perubahan status perangkat yang disebabkan oleh aktivitas operasional maupun pemeliharaan sistem VHP, seperti restart server atau pemutusan koneksi jaringan yang direncanakan. Informasi status yang ditampilkan membantu administrator membedakan kondisi gangguan jaringan yang tidak terduga dengan aktivitas pemeliharaan yang direncanakan, sehingga mendukung proses monitoring sistem informasi hotel secara menyeluruh dalam lingkungan simulasi.

4.6. Keunggulan dan Keterbatasan Sistem

Keunggulan utama sistem monitoring ini terletak pada kemampuan penyampaian informasi gangguan secara otomatis melalui Telegram, sehingga administrator dapat menerima informasi tanpa harus selalu memantau aplikasi monitoring secara langsung. Penggunaan aplikasi monitoring berbasis open-source (The Dude) dan layanan notifikasi Telegram memungkinkan sistem dikembangkan dengan biaya yang relatif rendah serta mudah diperluas dengan penambahan perangkat baru pada tahap selanjutnya. Selain itu, arsitektur tanpa server perantara menjadikan sistem lebih sederhana dan mudah dipelihara dibandingkan solusi berbasis Nagios atau platform cloud yang memerlukan infrastruktur tambahan.

Meskipun sistem telah berfungsi dengan baik pada tahap simulasi, terdapat beberapa keterbatasan yang perlu diperhatikan. Pertama, sistem notifikasi bergantung pada koneksi jaringan eksternal untuk pengiriman pesan Telegram, sehingga jika koneksi internet terputus, notifikasi tidak akan terkirim meskipun monitoring internal tetap berjalan. Hal ini dibuktikan melalui skenario tambahan pada Tabel 4.3 yang menunjukkan kondisi notifikasi tidak terkirim, di mana The Dude tetap mampu menampilkan perubahan status secara akurat namun pesan peringatan gagal diteruskan ke Telegram. Kedua, sistem monitoring yang dirancang belum dilengkapi dengan fitur pencatatan histori gangguan secara mendalam serta mekanisme keamanan lanjutan pada protokol SNMP (masih menggunakan SNMPv2c tanpa enkripsi), yang dapat menjadi bahan pengembangan pada penelitian selanjutnya.

4.7. Validasi melalui Lingkungan Virtual

Penggunaan VMware Workstation sebagai media simulasi memberikan fleksibilitas dalam pengujian berbagai skenario gangguan jaringan tanpa memengaruhi infrastruktur operasional nyata. Pendekatan ini memungkinkan proses pengembangan, pengujian, dan penyempurnaan sistem monitoring dilakukan secara aman dan terkontrol. Enam skenario pengujian utama yang telah dilaksanakan, meliputi kondisi normal, gangguan konektivitas, pemutusan koneksi manual, pemulihan koneksi, monitoring periodik, visualisasi status, dan pengiriman notifikasi

otomatis, seluruhnya menunjukkan tingkat keberhasilan 100%. Pengujian juga diperluas dengan skenario pemeliharaan server virtual dan pemeliharaan jaringan access point untuk mensimulasikan kondisi operasional hotel yang lebih nyata. Hasil simulasi secara keseluruhan dapat dijadikan dasar yang kuat untuk implementasi pada lingkungan jaringan fisik di masa mendatang, dengan catatan penyesuaian pada aspek keamanan protokol SNMP dan penambahan mekanisme pencatatan histori gangguan.

5. Kesimpulan

Sistem terbukti mampu mendeteksi perubahan status perangkat jaringan pada kondisi UP/DOWN maupun pemulihan koneksi, serta mengirimkan notifikasi peringatan secara otomatis kepada administrator melalui aplikasi Telegram dengan memanfaatkan router MikroTik sebagai executor script. Hasil pengujian pada berbagai skenario simulasi menunjukkan bahwa sistem dapat bekerja secara konsisten tanpa memerlukan proses pengecekan manual secara berkala. Keterbatasan penelitian ini meliputi: pengujian dilakukan dalam lingkungan jaringan virtual sehingga belum mencerminkan kondisi nyata; sistem menggunakan SNMPv2c yang belum dilengkapi enkripsi tingkat lanjut; dan cakupan terbatas pada perangkat wireless access point virtual. Pengembangan selanjutnya dapat dilakukan dengan penerapan SNMPv3, penambahan fitur histori gangguan dan analisis data, serta implementasi pada jaringan fisik sesungguhnya.

Referensi

1. S. Anwar, Jaringan Komputer dan Implementasinya. Jakarta: Deepublish, 2020.
2. D. Ariyadi and R. Prasetyo, Implementasi Simple Network Management Protocol (SNMP) dalam Pemantauan Jaringan Komputer, Jurnal Teknologi Informasi, vol. 9, no. 2, pp. 45-54, 2021.
3. Cisco Systems, Simple Network Management Protocol (SNMP) Overview, Cisco Networking Documentation, 2022.
4. A. Gunawan, Monitoring Jaringan Menggunakan MikroTik dan The Dude. Yogyakarta: Andi Publisher, 2021.
5. R. Hidayat, Manajemen dan Pemeliharaan Jaringan Komputer. Bandung: Informatika, 2020.
6. U. R. Khan, A. Shafiq, and Z. Hameed, Cloud-Based Network Monitoring Using SNMP and Telegram Bot Integration, IJACSA, vol. 11, no. 9, pp. 205-212, 2020.
7. S. Kurniawan and F. Rahman, Implementasi Notifikasi Jaringan Berbasis Telegram Bot untuk Sistem Monitoring Server, Jurnal Teknologi dan Komunikasi, vol. 12, no. 1, pp. 44-52, 2020.
8. MikroTik, SNMP and Telegram Bot Integration Guide, <https://help.mikrotik.com>, 2023.
9. A. Munawar, Panduan Praktis Administrasi Jaringan Komputer. Bandung: Informatika, 2019.
10. R. A. Nanda and D. Wijaya, Implementasi SNMP untuk Pemantauan Access Point Berbasis Telegram Notification, Jurnal Informatika dan Komputer, vol. 5, no. 1, pp. 12-20, 2022.
11. A. Nugroho and H. Prasetyo, Implementasi Sistem Monitoring Jaringan Berbasis SNMP Menggunakan Telegram Bot, JTIK, vol. 6, no. 3, pp. 243-250, 2019.
12. B. S. D. Oetomo, Konsep dan Aplikasi Sistem Jaringan Komputer. Surabaya: ITS Press, 2020.
13. N. P. Pratama and U. Y. Oktawati, Analysis and Implementation of Raspberry Pi Based Wireless Access Point Notification Using Telegram, Journal of Internet and Software Engineering, vol. 3, no. 1, pp. 1-11, 2022.
14. I. G. Putra, Penggunaan Telegram Bot untuk Sistem Peringatan Dini Jaringan, Jurnal Teknologi dan Sistem Informasi, vol. 7, no. 3, pp. 102-110, 2021.
15. T. Rahman, I. Z. Nibras, and S. Sumarna, Monitoring Administrasi Jaringan dengan MikroTik dan Telegram Bot pada ISP, Rabbit: Jurnal Teknologi dan Sistem Informasi, vol. 9, no. 2, pp. 162-172, 2024.
16. D. B. Rendo, B. Ngatono, and W. N. Aji, Analisis Monitoring Sistem Keamanan Jaringan Komputer Menggunakan Software NMAP, Jurnal PROSISKO, vol. 7, no. 2, p. 110, 2020.
17. B. Rifai, N. Nuryadi, and A. Ripai, Implementasi Telegram Notification Alert Pada Network Monitoring System Dengan Nagios, Jurnal Mantik Penusa, vol. 3, no. 3, 2019.