

BAB II LANDASAN TEORI

2.1 Tinjauan Pustaka

Untuk mendukung penelitian ini, penulis menggunakan sejumlah *Literature* yang berkaitan dengan judul dan topik penelitian. *Literature* yang digunakan dapat dilihat pada Tabel 2.1.

Tabel 2. 1 Tinjauan Pustaka

No. <i>Literature</i>	Penulis, Tahun	Judul
<i>Literature 1</i>	(Pangestu & Dasmen, n.d., 2018)	Monitoring dan analisis traffic jaringan distribusi pada PT. Mora Telematika Indonesia Regional Palembang dengan PRTG
<i>Literature 2</i>	(Alip et al., 2018)	Network Monitoring System Data Radar Penerbangan berbasis PRTG dan ADSB
<i>Literature 3</i>	(Hakim & Nugroho, 2020)	Implementasi Telegram Bot untuk Monitoring Mikrotik Router
<i>Literature 4</i>	(Efrando et al., 2019)	Monitoring pada Server STMIK Amik Riau dengan menggunakan Suricata melalui Notifikasi Bot Telegram
<i>Literature 5</i>	(Agung, 2020)	Monitoring sarana pendukung pada <i>Point of Presence</i> (POP) di PT XYZ menggunakan external alarm SIMON2000
<i>Literature 6</i>	(Muhammad Irsyad Firdaus, 2020)	Analisa Volume Trafik Jaringan dan Service Level Agreement (SLA)

2.1.1 Tinjauan Terhadap *Literature 1*

Pada penelitian yang dilakukan oleh (Aidil et al., 2018). (Aidil et al., 2018) dengan judul “Monitoring Dan Analisis Traffic Jaringan Distribusi Pada PT. Mora Telematika Indonesia Regional Palembang Dengan PRTG”. Penulis mengangkat

permasalahan ketika jaringan putus ke pelanggan maka pelanggan tersebut harus menelpon ke nomor *customer service* pusat (Jakarta) baru di sampaikan ke pihak bagian NOC/FOC regional di kota Palembang, maka dari itu penulis melakukan analisis untuk memudahkan *monitoring* jaringan ke pelanggan di perlukannya aplikasi yang dapat memantau jaringan mana yang mati (*down*), sehingga mendapatkan hasil aplikasi yang dapat di gunakan untuk melakukan monitoring jaringan salah satunya yaitu menggunakan aplikasi PRTG.

Setelah penulis menyelesaikan penelitiannya dapat di ambil kesimpulan bahwa aplikasi PRTG dapat memonitoring jaringan, melihat *traffic* jaringan, serta mengetahui apabila terjadinya *downtime* dan juga dapat mempermudah seorang administrator IT dalam memonitoring suatu jaringan baik ke pelanggan atau ke client, serta untuk mengetahui adanya *troubleshoot*.

2.1.2 Tinjauan Terhadap *Literature* 2

Berdasarkan penelitian yang dilakukan oleh (Alip et al., 2018) dengan judul “*Network Monitoring System (NMS) Data Radar Penerbangan Berbasis PRTG Dan ADSB*”. Penelitian ini bertujuan untuk menunjang transportasi penerbangan dengan mengirimkan data radar supaya ADSB dapat dikonfigurasi dengan baik dan juga dapat diintegrasikan menggunakan server PRTG, setelah dilakukan implementasi, hasil dari pengujian yaitu semua perangkat *router* yang menerima aliran data radar dan ADSB dapat termonitoring dengan memasang SNMP disetiap *router*.

Setelah penulis menyelesaikan penelitiannya dapat di ambil kesimpulan dengan adanya server PRTG, pengelola dapat langsung melakukan perbaikan jika terdapat alarm tanpa perlu menunggu *complain* dari pihak pemakai. Dengan

adanya server PRTG, pengelola akan menerima notifikasi *email* dengan cepat jika terjadi gangguan pada jaringan yang dimonitor.

2.1.3 Tinjauan Terhadap *Literature* 3

Pada penelitian yang dilakukan oleh (Dimara et al., 2019.) dengan judul “Implementasi Telegram Bot Untuk Monitoring Mikrotik Router”. Penulis mengangkat permasalahan pada CV. Infomedia mengenai pengawasan seperti koneksi terputus, user login kedalam mikrotik yang akan berakibat fatal apabila tidak diawasi secara rutin dan admin atau teknisi yang terkadang memiliki jadwal diluar, maka dari itu CV. Infomedia membutuhkan sebuah *Telegram Bot* untuk *monitoring Mikrotik router* yang dapat memberikan layanan informasi ketika koneksi terputus secara mendadak, *user hotspot login* kedalam jaringan dan kondisi fisik *mikrotik* untuk admin maupun teknisi yang rata-rata mempunyai smartphone.

Setelah penulis menyelesaikan penelitiannya dapat di ambil kesimpulan dengan menggunakan bot telegram dapat mempermudah admin atau teknisi dalam mendapatkan informasi konektivitas jaringan secara *real time*, dalam mendapatkan informasi *user* yang *login* dan *logout* kedalam jaringan dan dalam mendapatkan informasi kondisi fisik *Mikrotik router*.

2.1.4 Tinjauan Terhadap *Literature* 4

Pada penelitian yang dilakukan oleh (Efrando et al., 2019) dengan judul “Monitoring pada Server STMIK Amik Riau Dengan Menggunakan Suricata Melalui Notifikasi Bot Telegram”. Penulis mengidentifikasi adanya *issue* permasalahan pencurian/perusakan informasi dan penghapusan data, sehingga

apabila hal ini tidak dapat diidentifikasi sejak dini akan menimbulkan kerusakan yang merugikan pihak yang menyediakan sumber layanan tersebut dalam hal ini kampus STMIK Amik Riau.

Pada penelitian ini penulis melakukan *brute force* attack untuk service *ssh* menggunakan *tool hydra*, sebuah metode keamanan jaringan yang dapat melakukan pendeteksian, *monitoring*, dan mengidentifikasi aktifitas pada suatu *host* atau *network* salah satunya menggunakan Suricata. Berdasarkan hasil pengujian dan analisa dengan adanya *Monitoring Server* berbasis *Suricata* akan meminimalisir serangan dan ancaman dari *attacker* yang berpotensi merusak dan mengganggu sistem dari *server*, pengujian *Monitoring Server* berbasis *Suricata* menggunakan *tool pentest* seperti *Nmap*, *nikto* dan *hydra* telah berhasil dalam pengujian dengan mengirimkan notifikasi ke telegram sehingga administrator jaringan dapat mengambil tindakan pencegahan dini ketika mendapatkan laporan dari notifikasi telegram.

2.1.5 Tinjauan Terhadap Literature 5

Pada penelitian yang dilakukan oleh (Agung, 2020) yang berjudul “*Monitoring sarana pendukung pada Point of Presence (POP) di PT XYZ menggunakan external alarm SIMON2000*”. Penelitian ini bertujuan dalam membantu pekerjaan PT XYZ dalam menangani segala tiket gangguan dan meminimalisir kesalahan-kesalahan yang mungkin atau sedang terjadi di dalam POP baik dari segi kelistrikan dan keadaan di dalam POP seperti temperatur suhu dan sebagainya. Oleh karena itu diperlukan aplikasi *monitoring* yang diintegrasikan dengan alarm dalam menangani segala tiket gangguan.

Setelah penulis menyelesaikan penelitiannya dapat di ambil kesimpulan bahwa penggunaan sistem *external alarm* SIMON2000 di PT XYZ sebagai langkah pengawasan terhadap perangkat aktif dan juga kondisi lokasi di POP sangat penting untuk diterapkan karena dengan adanya perangkat yang dapat termonitor secara *realtime*. tim dapat melakukan pencegahan sebelum terjadinya gangguan dan dapat melakukan tindakan cepat ketika terjadi gangguan atau kerusakan yang diakibatkan bencana, pemadaman listrik, kerusakan peralatan, atau ancaman keamanan lainnya.

2.1.6 Tinjauan Terhadap *Literature* 6

Pada penelitian yang dilakukan (Muhammad Irsyad Firdaus, 2020) dengan judul “Analisa Volume Trafik Jaringan dan *Service Level Agreement (SLA)*”. Penelitian ini bertujuan untuk menganalisa volume dan intensitas trafik yang dapat membantu dalam penjadwalan *maintenance* dan kebutuhan untuk meningkatkan *Service level Agreement (SLA)*, Adapun data penggunaan *bandwith* hasil monitoring PRTG selama 2 bulan diambil dengan cara analisis trafik harian dan mingguan. Analisis Perhitungan *uptime* per bulan terhadap SLA ISP dengan total menit *downtime* per bulan sama dengan 6 menit. hasil dari perhitungan SLA, didapat hasil persentase *uptime* selama dua bulan pengamatan sebesar 99,98611%. Hasil *uptime* tersebut melebihi SLA ISP dengan nilai 99,5 %. Hasil *uptime* tersebut masuk dalam ketegori baik menurut PT XYZ.

2.2 Keaslian Penelitian

Adapun beberapa hal yang menjadi pembeda antara penelitian yang dilakukan penulis dengan penelitian yang sudah dilakukan sebelumnya sebagaimana terlampir di tabel tinjauan pustaka, antara lain ialah:

- 1) Pada penelitian ini PRTG memonitoring router yang ada di setiap POP dengan total jumlah 10 router.
- 2) Aplikasi PRTG di integrasikan dengan bot telegram sebagai pesan notifikasi untuk mengetahui kondisi status router POP yang di *monitoring*.
- 3) Penelitian ini di lakukan pada kantor PT. Indonesia Trans Network di Jl. Kimaja Kota Bandar Lampung.
- 4) Pada penelitian ini menggunakan *Operating System Windows 10* sebagai *server* PRTG.

2.3 Monitoring Jaringan

Monitoring adalah suatu proses mengukur, mencatat, mengumpulkan, memproses, dan mengkomunikasikan informasi untuk membantu pengambilan keputusan manajemen program/proyek (Duskarnaen & Rie Pratama, 2017).

Monitoring jaringan ini merupakan bagian dari manajemen jaringan. Monitoring jaringan memiliki peranan yang penting dalam upaya pencegahan insiden. Monitoring jaringan juga dapat memantau kondisi jaringan setiap saat, memperoleh laporan statistik, dan memperkirakan apakah ada perangkat yang perlu diganti, ditambah, atau ditiadakan. *Network monitoring* tidak dapat digunakan untuk menyelesaikan masalah ketika terjadi insiden, namun berbagai informasi yang sangat berharga dapat disajikan oleh sebuah aplikasi *network monitoring* (Duskarnaen & Rie Pratama, 2017).

2.4 Wide Area Network (WAN)

Menurut (Idrus, 2016) mengatakan WAN (Wide Area Network) adalah kumpulan dari LAN dan/atau *Workgroup* yang dihubungkan dengan menggunakan alat komunikasi modem dan jaringan internet, dari/ke kantor pusat dan kantor cabang, maupun antar kantor cabang. Dengan sistem jaringan ini, pertukaran data antar kantor dapat dilakukan dengan cepat serta dengan biaya yang relatif murah. Sistem jaringan ini dapat menggunakan jaringan Internet yang sudah ada, untuk menghubungkan antara kantor pusat dan kantor cabang atau dengan *PC Stand Alone/Notebook* yang berada di lain kota ataupun negara. Contoh dari WAN adalah internet.

2.5 Point of Presence (POP)

Point of Presence (POP) adalah sebuah *local access point* menuju internet yang berfungsi menghubungkan beberapa perangkat yang berada di dalam satu jaringan dalam satu atau beberapa POP yang saling terhubung satu dan yang lainnya. Jalur akses lokal inilah yang memungkinkan perangkat terhubung ke penyedia layanan internet atau *Internet Service Provider (ISP)*. POP ini biasanya menampung banyak *server*, *router*, dan semua peralatan antarmuka lainnya (Agung, 2020).

2.6 Paessler Router Traffic Grapher (PRTG)

Paessler Router Traffic Grapher (PRTG) Network Monitor merupakan sebuah perangkat lunak monitoring jaringan yang dibuat oleh perusahaan *Paessler* yang berpusat di Jerman. *PRTG Network Monitor* telah digunakan oleh lebih dari 500.000 administrator jaringan untuk memantau LAN, WAN, *server*, *website*,

peralatan, URL, dan banyak lagi (Paessler AG, 2022). PRTG *network* monitor tersedia dalam tiga pilihan lisensi, yaitu *Freeware Edition*, *Trial Edition*, dan *Commercial Editions*. PRTG Network Monitor berjalan pada mesin *Windows* dalam jaringan, PRTG mengumpulkan berbagai statistik dari mesin, perangkat lunak, dan perangkat lain yang ditentukan. PRTG juga menyimpan data statistik yang telah dikumpulkan sehingga penggunaanya dapat melihat riwayat kerja perangkat yang dimonitor sehingga dapat merespon perubahan yang terjadi. PRTG mendukung beberapa protokol untuk mengumpulkan data berikut (Paessler AG, 2022):

- a. Ping, SNMP; web queries via HTTP and HTTPS; email via Post Office Protocol version 3 (POP3), Internet Message Access Protocol (IMAP), Simple Mail Transfer Protocol (SMTP).
- b. Hardware parameters via SNMP, Secure Shell (SSH), Simple Object Access Protocol (SOAP).
- c. Bandwidth usage via Flow (NetFlow, jFlow, sFlow, IPFIX), packet sniffing, SNMP.
- d. Windows systems via Windows Management Instrumentation (WMI).
- e. Other interfaces via SSH and scripts (for example, PowerShell and Python).

Secara garis besar, PRTG dapat digunakan untuk melakukan hal-hal berikut (Paessler AG, 2022) :

- a. Pengawasan terhadap koneksi sumber daya pada jaringan
- b. Mengawasi dan mengukur penggunaan bandwidth pada perangkat jaringan
- c. Mencari dan menemukan serta mengakses perangkat yang ada pada jaringan

- d. Mendeteksi aktivitas yang tidak seharusnya (*suspicious and malicious*) baik dari user maupun dari device yang ada dalam jaringan.
- e. Pengawasan terhadap penggunaan sumber daya sistem, seperti traffic, CPU load, Temperature, Disk Space, dan memory Usage.
- f. Mengelompokkan paket-paket yang lewat pada lalu lintas jaringan berdasarkan sumber dan tujuannya.

2.6.1 Kebutuhan PRTG

Untuk menginstall dan bekerja dengan PRTG Network Monitor, diperlukan persyaratan sebagai berikut (Paessler AG, 2022):

a. *Hardware*

PRTG menyarankan menggunakan perangkat keras server x64 atau yang dikonfigurasi *virtual environment*.

b. *Operating system*

PRTG menyarankan Anda menggunakan Microsoft Windows Server 2019, Microsoft Windows Server 2016, atau Microsoft Windows Server 2012 R2.

c. *Microsoft .NET Framework*

Microsoft .NET Framework 4.7.2 atau yang lebih baru harus diinstal pada Sistem server core PRTG atau remote probe system. kami sarankan .NET Framework 4.8

d. *Web browser*

Peramban web (web browser) berikut secara resmi didukung oleh PRTG Web Interface (berdasarkan kinerja dan keandalan):

- Google Chrome 72 or later (direkomendasikan)
- Mozilla Firefox 65 or later

- Microsoft Internet Explorer 11

2.7 Mikrotik

Mikrotik merupakan sebuah perusahaan yang bergerak dibidang produksi perangkat keras (*Hardware*) dan perangkat lunak (*Software*) yang berhubungan dengan sistem jaringan komputer yang berkantor pusat di Latvia, bersebelahan di Rusia. Mikrotik didirikan pada tahun 1995 untuk mengembangkan *router* dan sistem ISP (Internet Service Provider) *nirkabel* (Husna & Rosyani, 2021).

2.8 Telegram

Saat ini telah banyak aplikasi pesan instan / *instant messaging* (IM) seperti Whatsapp, Line, Snapchat, Facebook Messenger dan Telegram. Telegram merupakan satu-satunya aplikasi pesan singkat yang menyediakan *Application Programming Interface* (API) bagi pengguna untuk dapat membuat bot yang bisa dimanfaatkan untuk sistem informasi (Mulyanto, 2020). Notifikasi melalui Telegram menjadi alternatif yang efektif dalam menginformasikan permasalahan jaringan kepada administrator yang bertanggung jawab. Telegram merupakan aplikasi komunikasi yang populer dengan fitur notifikasi yang dapat dikonfigurasi secara fleksibel. Dengan mengintegrasikan PRTG dengan Telegram, administrator dapat menerima notifikasi langsung melalui aplikasi Telegram saat terjadi permasalahan jaringan. Hal ini memungkinkan administrator untuk merespons dengan cepat dan mengambil tindakan yang diperlukan guna meminimalkan dampak negatif terhadap SLA.

2.9 Bot Telegram

Bot merupakan aplikasi pihak ketiga yang dapat dijalankan di dalam Telegram. Pengguna dapat mengirim pesan, perintah, dan *inline request*. Kita dapat mengontrol bot menggunakan HTTPS ke API telegram. Banyak sekali kegunaan bot telegram diantaranya:

- a. Bot dapat digunakan sebagai koran pintar (*smart newspaper*) yang akan memberikan berita kepada pelanggan bot tersebut.
- b. Bot juga dapat digunakan sebagai jembatan layanan lain seperti Gmail, Gambar, GIF, IMDB, Wiki, Musik, Youtube, GitHub.
- c. Bot dapat juga digunakan untuk menerima pembayaran dari pengguna telegram. Bot dapat menawarkan layanan berbayar atau bekerja sebagai etalase virtual. Terkait hal ini dapat dipelajari lebih lanjut di <https://t.me/shopbot>.
- d. Bot juga dapat digunakan sebagai alat khusus misalnya memberikan peringatan, ramalan cuaca, terjemahan, pemformatan, atau layanan lainnya.
- e. Bot dapat juga digunakan sebagai *game* baik *singleplayer* ataupun *multi-player*.
- f. Bot dapat digunakan sebagai layanan sosial yang menghubungkan orang yang mencari mitra percakapan berdasarkan minat atau kedekatan yang sama

Bot atau robot biasa digunakan untuk kegiatan otomatisasi terhadap sebuah kegiatan yang berulang, serta dapat digunakan sebagai alat pengawasan/*monitoring* yang dilakukan oleh pihak admin (Mulyanto, 2020).

2.10 Latency

Latency adalah jeda waktu yang dibutuhkan dalam pengantaran paket data dari pengirim ke penerima. Semakin tinggi jeda waktu atau *latency* tersebut maka akan semakin tinggi resiko kegagalan akses. *Latency* juga sering diartikan sebagai tingkat keterlambatan pengantaran pada jaringan komunikasi data dan juga suara (Saputri et al., 2020).

Delay merupakan lamanya waktu yang dibutuhkan oleh data atau informasi untuk sampai ke tempat tujuan data atau informasi tersebut dikirim. Delay pada suatu jaringan akan menentukan langkah apa yang akan di ambil ketika di manajemen suatu jaringan. Ketika delay besar, dapat diketahui jaringan tersebut sedang sibuk atau kemungkinan yang lain adalah kapasitas jaringan tersebut yang kecil sehingga bisa melakukan tindakan pencegahan agar tidak terjadi overload. Misalkan dengan memindahkan sebagian aliran data ke jalur lain atau memperbesar kapasitas jaringan di (Bhakti et al., 2017). Menurut versi TIPHON standarisasi nilai delay dari *latency* dapat dilihat pada Tabel 2.2.

Tabel 2. 2 Parameter Delay (TIPHON)

Kategori <i>Latency</i>	Besar <i>Delay Latency</i>
Sangat Bagus	<150 ms
Bagus	150 s/d 300 ms
Sedang	300 s/d 450 ms
Jelek	>450 ms

Untuk mencari nilai rata-rata delay, dapat menggunakan persamaan berikut:

$$Delay\ rata - rata = \frac{Total\ delay}{Total\ paket\ yang\ diterima}$$

2.11 Traffic

Data *traffic* merupakan *port ethernet* pada perangkat router yang telah aktif atau sudah digunakan untuk melayani pelanggan ITN di setiap POP. Data ini sangat penting untuk memberikan informasi terkait total *traffic* perangkat dan berapa besar *occupancy traffic* yang ada di dalam *port ethernet* tersebut. *port traffic* adalah kapasitas atau daya tampung kabel *port ethernet* agar dapat dilewati *traffic* paket data dalam jumlah tertentu. Selain itu, *traffic* dikatakan data yang keluar masuk (*upload-download*). *Traffic* dapat dipakai untuk mengukur baik aliran data analog maupun data digital (Santoso & Suryapradana, 2019). Menurut ITN standarisasi *traffic* dari kapasitas dapat dilihat pada Tabel 2.3.

Tabel 2. 3 Traffic

Kategori Traffic	Kapasitas Port Ethernet
Baik	< 80%
Buruk	≥ 80%

2.12 CPU Load

CPU load digunakan untuk mengetahui seberapa berat kinerja dari CPU pada perangkat router tersebut. Hal ini dilakukan untuk menjaga kinerja CPU agar tidak *overload* atau melebihi persyaratan dari ITN yaitu tidak boleh lebih dari 80% *CPU load*. Hal ini juga menjaga agar kondisi dari perangkat router di POP selalu dalam keadaan prima. Apabila kinerja dari CPU unit di perangkat router sudah melebihi ambang batas yang dipersyaratkan maka ITN akan melakukan penyesuaian atau upgrade terhadap perangkat router tersebut. Menurut (Khadafi et al., 2017) standarisasi *CPU load* dapat dilihat pada Tabel 2.4.

Tabel 2. 4 Standarisasi *CPU load*

Kategori CPU load	Besar CPU load
Normal	<80%
Peringatan	>80%

2.13 *Temperature*

Temperature atau yang biasa diketahui juga sebagai suhu menunjukkan derajat panas benda. Mudahnya, semakin tinggi temperatur suatu benda, semakin panas benda tersebut. Secara *mikroskopis*, *temperature* menunjukkan energi yang dimiliki oleh suatu benda. Setiap atom dalam suatu benda masing - masing bergerak, baik itu dalam bentuk perpindahan maupun gerakan di tempat getaran. Makin tingginya energi atom-atom penyusun benda, makin tinggi suhu benda tersebut. Hal ini dilakukan untuk menjaga suhu agar tidak *overhead* atau melebihi persyaratan dari ITN yaitu tidak boleh lebih dari 70°C. Hal ini juga menjaga agar kondisi dari perangkat router di POP selalu dalam keadaan prima. Menurut (Santoso & Suryapradana, 2019) standarisasi *temperature* dapat dilihat pada Tabel 2.5.

Tabel 2. 5 Standarisasi *Temperature*

Kategori <i>Temperature</i>	Besar <i>Temperature</i>
Normal	20°C - 60°C
Siaga	60°C - 70°C
Bahaya	>75°C

2.14 *Service Level Agreement (SLA)*

Service Level Agreement (SLA) merupakan kesepakatan kontrak antara penyedia layanan dan pelanggan yang menetapkan standar dan persyaratan kinerja yang harus dipenuhi oleh penyedia layanan. SLA mencakup parameter seperti kecepatan akses, ketersediaan, waktu henti yang diizinkan, dan waktu respons terhadap permasalahan. Monitoring jaringan yang efektif membantu dalam menentukan apakah SLA telah terpenuhi atau tidak. Dengan menggunakan data monitoring jaringan, perusahaan dapat mengidentifikasi pelanggaran SLA dan mengambil langkah-langkah perbaikan yang diperlukan.

Perhitungan SLA (*Service Level Agreement*) dapat dilihat dari hasil persentase *uptime*. Berikut rumus perhitungan SLA.

$$1 - \frac{\text{Total Menit downtime}}{\text{Jumlah hari} \times 24 \text{ jam} \times 60 \text{ menit}} \times 100\%$$

Berdasarkan rumus diatas total menit *downtime* didapat dari jumlah menit *downtime* selama pengujian, dan hasil dari perhitungan di dapat nilai *uptime* bentuk persen (%). Pada ITN telah menentukan standar SLA seperti pada tabel 2.6

Tabel 2. 6 Kategori SLA menurut ITN

SLA	Kategori
≥ 99.50%	Baik
< 99.50%	Buruk

2.15 *Simple Network Management Protocol (SNMP)*

Simple Network Management Protocol (SNMP) adalah sebuah protokol aplikasi pada jaringan TCP/IP yang menangani manajemen jaringan. Protokol ini didesain sehingga pengguna dapat dengan mudah memantau kondisi jaringan

komputer. Pemantauan kondisi jaringan dapat dilakukan dengan cara pengumpulan nilai-nilai informasi dari kondisi jaringan secara jarak jauh atau mengagunkan satu pusat pengamatan. SNMP menjadi protokol yang terus dikembangkan karena banyak perangkat jaringan yang mendukung dan tersedia layanan SNMP seperti *router*, *switch*, *server*, *workstation*, dan *printer*. Protokol SNMP pada jaringan TCP/IP menggunakan transport UDP oleh karena itu dalam penggunaannya tidak akan membebani trafik jaringan. Pada sistem pemantauan jaringan dengan menggunakan layanan SNMP, terdapat tiga komponen dasar antara lain (Tantular, 2021):

- a. Manajer SNMP adalah perangkat yang menjalankan dan dapat menangani tugas-tugas manajemen jaringan.
- b. Agen SNMP adalah perangkat pada jaringan yang akan diamati dan dikelola. Setiap agen akan merespon dan menjawab permintaan manajer SNMP.

2.16 Metode *Experiment*

Metode Eksperimen adalah pemberian kesempatan kepada perorangan maupun kelompok untuk melakukan percobaan yang sengaja dirancang dan terencana untuk membuktikan kebenaran suatu teori dengan menempuh atau menggunakan cara yang teratur dan sistematis (Dewi, 2006). Penelitian eksperimen dilakukan untuk mengetahui pengaruh pemberian suatu *treatment* atau perlakuan terhadap subjek penelitian (Cahya, 2013). Selain itu, metode eksperimen dilakukan untuk menghasilkan suatu data yang diperlukan dengan parameter yang sudah ditentukan. Metode eksperimen dilakukan dengan cara melakukan pengesanan langsung pada media (Hasim dan Riadi, 2013).

Karakteristik dari metode eksperimen menurut (Rismawati, Ratman dan Dewi, 2006) sebagai berikut :

1. Metode untuk melakukan percobaan, pengamatan dan penarikan kesimpulan terhadap sesuatu yang sedang diuji.
2. Metode yang dirancang untuk mengembangkan pengetahuan.
3. Metode yang membantu dalam pemrosesan informasi yang aktif.
4. Metode yang mengarahkan untuk mempelajari lingkungan belajar sebagai suatu teknologi.
5. Metode yang digunakan untuk memecahkan masalah yang bersifat ilmiah.

2.17 Metode Pengujian

Pada tahap ini, pengujian yang dilakukan untuk dapat memantau *sensor* di PRTG dengan parameter yaitu *Traffic*, *Latency*, *CPU load*, dan *Temperature*. Pada penelitian ini PRTG juga memberikan analisis kategori dari SLA yang ditetapkan ITN yaitu 99.5% dari *uptime* dan juga *downtime* dari *latency*, selain itu memberikan notifikasi secara *realtime* mengenai status kondisi router *Point of Presence* (POP) jika terjadi masalah pada router POP melalui notifikasi terintegrasi dengan PRTG dikirim melalui telegram supaya masalah tersebut dapat segera ditangani (Husna & Rosyani, 2021).