

BAB II

TINJAUAN PUSTAKA

2.1 Landasan Teori

Banyak penelitian tentang manajemen dan pemantauan jaringan yang telah dilakukan. Penelitian membahas tentang kegunaan dari SNMP yang tidak hanya bisa digunakan dalam memantau kondisi perangkat hardware maupun software dari suatu jaringan namun juga bisa digunakan untuk memantau keamanan dari informasi yang terdapat dalam server. Pada penelitian dikembangkan sebuah system yang dapat memantau dan mengontrol server tanpa mempengaruhi beban server dan kinerja layanan.

Dalam penelitian ini, penulis membangun sebuah sistem monitoring jaringan menggunakan LibreNMS untuk memantau kondisi perangkat jaringan yang ada di Kampus Universitas Pembangunan Jaya. Tujuan dari penelitian ini adalah untuk dapat mengetahui kinerja dari setiap perangkat jaringan yang dipantau apakah sudah berjalan dengan baik dan dapat memonitor trafik jaringan yang masuk dan keluar serta penggunaan resource pada tiap perangkat jaringan yang berjalan pada jaringan Kampus Universitas Pembangunan Jaya.

2.1.1 Network Monitoring Server (NMS)

Menurut Ali (2018), NMS merupakan tool untuk melakukan monitoring pada elemen-elemen dalam jaringan komputer seperti router, switch maupun server. NMS umumnya menggunakan protokol SNMP yang dirancang untuk mengumpulkan data manajemen perangkat jaringan dan konfigurasi perangkat secara jarak jauh. Hasil dari pemantauan tersebut menjadi bahan pertimbangan dalam pengambilan keputusan oleh pihak manajemen maupun sebagai bahan analisa apakah terdapat kejanggalan dalam operasional jaringan.

Berikut merupakan beberapa alasan mengapa perlu menggunakan aplikasi pemantauan jaringan.

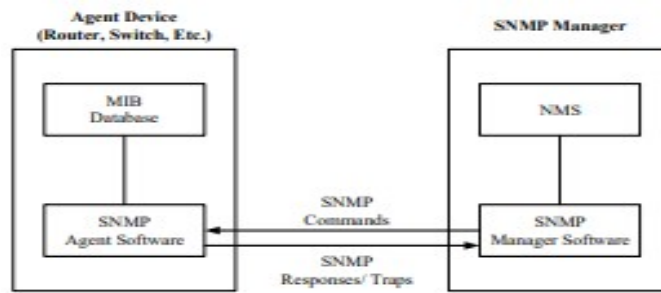
1. Mengetahui kondisi perangkat yang terhubung dalam suatu jaringan.
2. Mengetahui informasi status jaringan secara remote.
3. Bahan informasi untuk perencanaan pengembangan jaringan dan perubahan peralatan jaringan.
4. Bahan informasi untuk mendiagnosa masalah-masalah dalam jaringan.
5. Memastikan keamanan sistem jaringan beroperasi dengan baik.
6. Menghemat pengeluaran dengan menekan jumlah waktu jaringan down dan memangkas waktu untuk menganalisa masalah.

2.1.2 Simple Network Management Protocol (SNMP)

Menurut Fakhruddin (2019) Simple Network Management Protocol atau biasanya dikenal dengan nama SNMP adalah protokol standar yang telah muncul sebagai teknologi andal yang dapat diimplementasikan dalam manajemen jaringan. SNMP menyediakan cara untuk mengumpulkan informasi, mengontrol, memanipulasi, mengkonfigurasi maupun saling bertukar informasi antar perangkat yang berada di dalam suatu jaringan. Hal ini akan membantu untuk memantau, mengaudit, mendeteksi kesalahan dalam jaringan dan mengkonfigurasi perangkat jauh secara real-time.

A. Komponen Utama SNMP

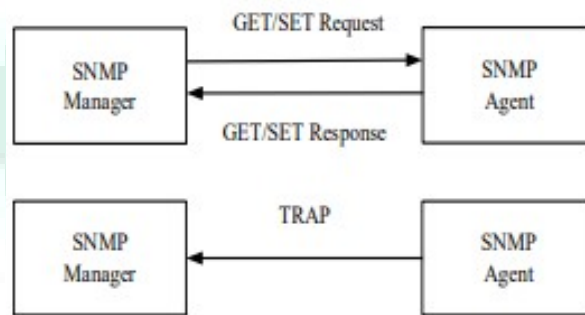
Terdapat tiga komponen utama dari SNMP, yaitu SNMP Manager, SNMP Agent, dan MIB (Management Information Base). Manager merupakan software yang berjalan di sebuah host yang bertugas berkomunikasi dengan agent untuk meminta informasi ke dalam jaringan. Agent merupakan perangkat lunak yang dijalankan di setiap elemen jaringan, seperti workstation, repeater, router, switch, dan personal computer yang bertugas untuk merespon dan memberikan informasi sesuai permintaan manager. MIB merupakan struktur basis data variabel dari sebuah elemen jaringan yang dimonitor. Pendefinisian MIB dalam SNMP menggunakan diagram pohon, dan menempatkan setiap Object Identifier (OID) pada suatu lokasi unik pada pohon. Berikut ini adalah struktur pada SNMP.



Gambar 2.1 Struktur SNMP

Sumber: <http://edocs.ilkom.unsri.ac.id/>

B. Fungsi SNMP



Gambar 2.2 SNMP Query dan Trap

Sumber: <http://edocs.ilkom.unsri.ac.id/>

Gambar 2 merupakan interaksi yang terjadi antara manager dan agent. Untuk mendapatkan informasi yang terdapat pada MIB, manager akan mengirimkan permintaan berupa query pada agent. Agent akan berinteraksi dengan MIB dan memproses query. Setelah query diproses, agent akan memberikan respon sesuai permintaan yang dikirimkan oleh manager. Trap merupakan pesan yang dikirimkan oleh agent ke manager sebagai laporan dari suatu event.

2.1.3 Internet Protocol (IP)

Menurut Alvin (2017) Internet Protocol (IP) berada pada layer Internetwork atau Internet. IP merupakan kunci dari jaringan TCP/IP, agar dapat berjalan dengan baik maka semua aplikasi jaringan TCP/IP pasti bertumpu kepada internet protocol. IP

adalah protokol yang mengatur bagaimana suatu data dapat dikenal dan dikirim dari satu komputer ke komputer lain. IP bersifat connectionless protocols. Protokol IP memiliki lima fungsi utama, yaitu :

1. Mendefinisikan paket yang menjadi unit satuan terkecil pada transmisi data di internet.
2. Memindahkan data antara Transport Layer dan Network Interface Layer.
3. Mendefinisikan skema pengalamatan internet atau IP address.
4. Menentukan routing paket, Dan melakukan fragmentasi dan penyusunan ulang paket.

TCP/IP adalah protocol komunikasi yang bersifat bebas kesalahan connection-oriented (mengabaikan media reuter) yang terdiri dari dua protocol yaitu TCP dan IP. Protocol IP melaksanakan hubungan antara dua peralatan dalam sebuah jaringan komputer berdasarkan pengalamatan 4 byte (32-bit). Untuk pengalamatan seperti ini menyebabkan protocol TCP/IP memiliki reuter bebas. Metode pengiriman paket pada TCP/IP dimana setiap kali terjadi koneksi yang dilakukan oleh dua mesin dalam jaringan yang telah dispesifikasi oleh 13 alamat OP dan subnet mask, TCP menciptakan paket tunggal IP dari data yang akan ditransfer. Setiap paket memiliki header yang menyimpan informasi sebagai berikut:

- a. PortId, mengidentifikasi aplikasi yang akan dijalankan pada mesin yang datanya sedang ditransfer.
- b. CheckSum, digunakan untuk memeriksa apakah paket yang ditransfer terdapat kesalahan atau tidak. Jika ada kesalahan maka akan dilakukan pengiriman data kembali (resend),
- c. Informasi control lainnya yang berhubungan dengan tipe data dan aplikasinya. Sebelum keseluruhan data dikirim, TCP akan memecah terlebih dahulu data tersebut menjadi datagram (kelompok data) kemudian satu persatu datagram ini ditransmisikan menuju alamat IP yang dituju.

Proses transmisi ini dilakukan dalam route bebas, yang berarti bahwa tiap-tiap datagram dalam satu sistem data dapat ditransmisikan dalam route yang berbeda.

Apabila salah satu dari datagram tersebut mengalami kesalahan dalam hal pengiriman data, maka TCP pada mesin yang dituju meminta kembali datagram tersebut. Jika semua datagram dapat diterima dengan benar, selanjutnya TCP akan mengurutkannya kembali menjadi satu kempok data seperti yang berasal dari sumbernya.

2.1.4 IPV4 Address

Menurut Stevan (2015) IP address adalah sekumpulan bilangan biner sepanjang 32 bit, yang dibagi atas 4 segmen dan setiap segmen terdiri dari atas 8 bit. IP address merupakan identifikasi setiap host pada jaringan Internet. Secara teori, tidak boleh ada dua host atau lebih yang tergabung ke internet menggunakan IP address yang sama.

Untuk memudahkan pembacaan dan penulisan, IP address telah direpresentasikan dalam bilangan desimal yang dipisahkan oleh titik atau disebut dotted-decimal format. Nilai desimal dari IP address inilah yang dikenal dalam pemakaian sehari-hari. Apabila setiap segmen dikonversikan ke bilangan desimal berarti nilai yang mungkin antara 0 hingga 255. Contoh IP address sebagai berikut: 01000100 10000001 11111111 00000001. Jika dikonversikan ke bilangan desimal menjadi 68.129.255.1. Jangkauan alamat (range address) yang bisa digunakan adalah dari 00000000 00000000 00000000 00000000 atau 0.0.0.0 Sampai dengan 11111111 11111111 11111111 11111111 atau 255.255.255.255. Dengan demikian, secara teori ada sebanyak 232 kombinasi IP address yang bisa dipakai di seluruh dunia. Jadi, jaringan TCP/IP dengan 32 bit address mampu menampung sebanyak lebih dari 4 milyar host.

Dalam IPV4 terbagi menjadi beberapa kelas yaitu:

1. Kelas A

Rentang angka IP : 0.0.0.0 – 127.255.255.255

Jumlah alamat IP (maksimal) : 16.777.216

Jumlah jaringan (maksimal) : 128

Cocok di gunakan untuk jaringan yang memiliki skala sangat besar karena kapasitasnya pun sangat memadai. Namun, jika di bandingkan dengan kelas lainnya, seperti B dan C, kelas A mempunyai jumlah pembentukan jaringan cenderung minim, akan tetapi dari segi kapasitasnya, kelas A memegang posisi utama.

2. Kelas B

Rentang angka IP : 128.0.0.0 – 191.255.255.255

Jumlah alamat IP (maksimal) : 1.048.576

Jumlah jaringan (maksimal): 16.384

Kelas B di peruntukan bagi jaringan dengan skala menengah ke atas dan mampu menciptakan jaringan hingga mencapai 16.384 buah, serta masing-masing jaringan bisa menampung host dengan jumlah 65.534.

3. Kelas C

Rentang angka IP: 192.0.0.0 – 223.255.255.255

Jumlah alamat IP (maksimal) : 65.536

Jumlah jaringan (maksimal) : 2.097.152

Kelas ini di gunakan untuk skala jaringan yang jauh lebih kecil, karena setiap jaringan hanya mampu menampung host hingga mencapai 254 host saja. Nah, biasanya, kelas C lebih di gunakan pada rangkaian internet protokol secara private, misalnya saja seperti sekolah, universitas, hingga kost-kostan.

Sebuah alamat IP terdiri dari 4 set dari 8-bit (oktet) dengan total 32-bit, masing-masing dipisahkan oleh sebuah titik (.). Untuk masing-masing dari 4 set oktet dalam sebuah alamat IP, nilai yang paling maksimum adalah 255 (mewakili oktet yang berisi semua). Oleh karena itu, nilai-nilai alamat IP berkisar dari 0.0.0.0 ke 255.255.255.255, yang diterjemahkan ke 3720314628 alamat IP yang berbeda.

Total keseluruhan ada 4 klasifikasi IP address, yaitu klasifikasi A, B, C, D, dan E. Hanya saja pada realita di dunia pekerjaan yang sering digunakan yaitu hanya 3 segment yaitu A,B,dan C. Dari beberapa kelas ip memiliki kekurangan dan kelebihan karena antar komputer dengan komputer lain di butuhkan suatu bahasa yang sama

dimana tidak bergantung dengan aplikasi yang dipakai dan hardware yang di pasang. Oleh karena itu dibutuhkan protokol. Untuk penanda untuk setiap komputer digunakan sebuah alamat yaitu dengan IP Address.

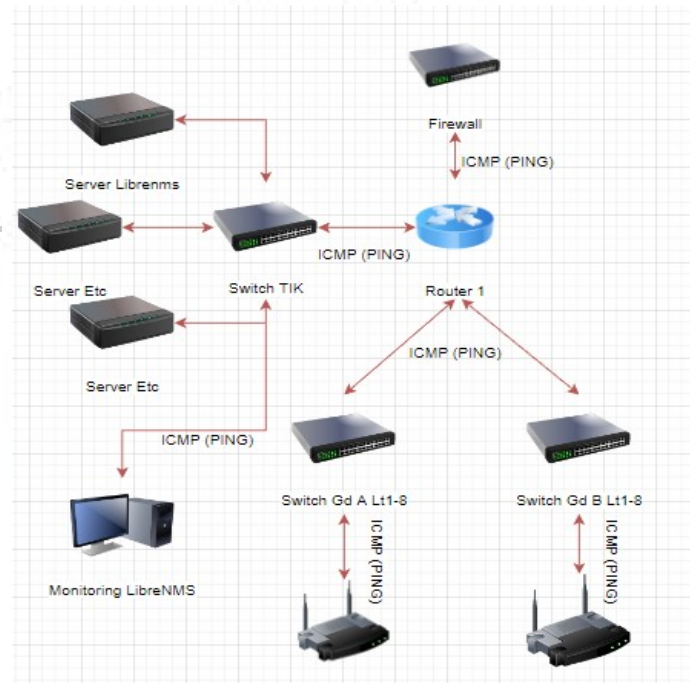
KELAS A		KELAS B		KELAS C	
Subnetmask	CIDR	Subnetmask	CIDR	Subnetmask	CIDR
255.0.0.0	/8	255.255.0.0	/16	255.255.255.0	/24
255.128.0.0	/9	255.255.128.0	/17	255.255.255.128	/25
255.192.0.0	/10	255.255.192.0	/18	255.255.255.192	/26
255.224.0.0	/11	255.255.224.0	/19	255.255.255.224	/27
255.240.0.0	/12	255.255.240.0	/20	255.255.255.240	/28
255.248.0.0	/13	255.255.248.0	/21	255.255.255.248	/29
255.252.0.0	/14	255.255.252.0	/22	255.255.255.252	/30
255.254.0.0	/15	255.255.254.0	/23	255.255.255.254	/31

Gambar 2.3 Segmentasi IP

2.1.5 ICMP (Internet Control Message Protocol)

Menurut Alif (2017) IP menggunakan metode unreliable pada saat pengiriman data ke jaringan. Tidak ada proses untuk menentukan masalah saat pengiriman data ke jaringan. Karena didesain sedemikian adalah untuk membuat sumber daya jaringan lebih efisien. Jika terdapat kegagalan seperti router mati, atau jika device tujuan tidak terhubung ke jaringan, maka data tidak dapat terkirim. ICMP merupakan komponen dari protokol TCP/IP yang membantu IP untuk mengidentifikasi kesalahan-kesalahan itu.

Internet Control Message Protocol (ICMP) adalah protokol yang bertugas mengirimkan pesan-pesan kesalahan dan kondisi lain yang memerlukan perhatian khusus. Dengan menganalisa performansi ICMP dalam kaitannya dengan sistem keamanan komputer pada protokol TCP/IP maka dapat diperoleh karakteristiknya yang terdiri dari format paket datagram IP dan format paket datagram ICMP.



Gambar 2.4 Sistem Kerja *ICMP*

2.1.6 Simple Network Management Protocol (SNMP)

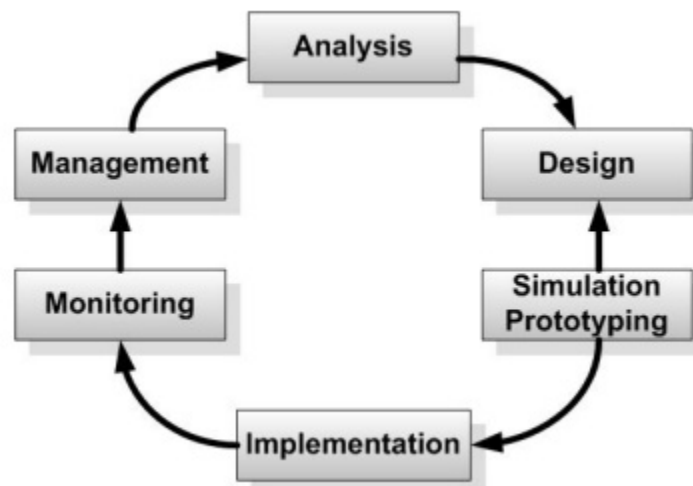
Simple Network Management Protocol atau umumnya dikenal dengan nama SNMP adalah protokol standar yang telah muncul sebagai teknologi andal yang dapat diimplementasikan dalam manajemen jaringan. SNMP menyediakan cara untuk mengumpulkan informasi, mengontrol, memanipulasi, mengkonfigurasi maupun saling bertukar informasi antar perangkat yang berada di dalam suatu jaringan. Hal ini akan membantu untuk memantau, mengaudit, mendeteksi kesalahan dalam jaringan dan mengkonfigurasi perangkat jauh secara real-time.

Dengan adanya SNMP kita tidak perlu memeriksa satu-persatu setiap server, tetapi kita cukup mengakses satu komputer untuk melihat kondisi seluruh server dan router. Hal ini disebabkan server dan router akan bertindak sebagai SNMP-server yang bertugas untuk menyediakan request SNMP dari komputer lain. Satu PC akan bertindak sebagai SNMP Agent yaitu komputer yang mengumpulkan informasi-informasi dari SNMP-server. SNMP menggambarkan sebuah relasi antara Client/Server. Program Client (disebut Network Manager) membuat koneksi virtual ke sebuah program server (disebut SNMP Agent) mengeksekusinya dalam remote network device. Database yang dikontrol oleh SNMP Agent akan diarahkan ke sebagai SNMP Management Information Base (MIB), dan merupakan sebuah standar dari set statistik dan kontrol nilai. Selain itu SNMP mengizinkan perpanjangan dari nilai-nilai standar dengan nilai-nilai spesifik ke agent tertentu melalui penggunaan private MIB. Sebelum melanjutkan ada baiknya kita mengetahui apa itu Manager, MIB, dan Agent, berikut penjelasannya :

- Manager, yaitu bertugas sebagai manajemen jaringan yang mengumpulkan data informasi dari elemen-elemen jaringan yang ingin dimonitoring. Bentuk dari manager ini berupa perangkat lunak yang memiliki fungsi antarmuka yang baik bagi penggunaannya dalam hal ini network administrator jaringan.
- MIB (Management Information Base), yaitu database dari data informasi yang dikumpulkan oleh manager dari agen yang tersimpan dalam database server. Struktur data dalam MIB ini bersifat hirarki dan memiliki aturan sedemikian rupa sehingga informasi setiap variabel dapat dikelola atau ditetapkan dengan mudah.
- Agent, yaitu suatu elemen jaringan yang dimonitoring atau dikontrol oleh manager. Pada umumnya perangkat jaringan seperti router dan server difungsikan sebagai agen dalam sistem manajemen jaringan. Hal ini disebabkan lalu lintas trafik data dengan jumlah yang besar melalui atau bermuara pada kedua perangkat jaringan tersebut. Setiap agen mempunyai database yang bersifat lokal dengan variabel-variabel tertentu, artinya secara default informasi disimpan dalam disk lokal dan digunakan oleh sistem operasi internal. Protokol SNMP yang diaktifkan pada suatu agen akan menjadikan data informasi agen seperti aktifitas trafik, dan keadaan proses di sistem internal dan kapasitas sistem dapat dikirim ke manager untuk dikelola lebih lanjut.

2.1.7 Network Development Life Cycle (NDLC)

Menurut Goldman dan Rawles (2014) NDLC adalah suatu pendekatan yang memiliki tahap atau bertahap untuk melakukan analisa dan membangun suatu rancangan dengan menggunakan siklus lebih spesifik terhadap kegiatan pengguna. Secara umum, lifecycle pengembangan network mengikuti pendekatan PPDIIO (Prepare, Plan, Design, Implement, Operate, dan Optimize). Penelitian yang digunakan pada penelitian ini adalah PPDIIO (Prepare, Plan, Design, Implement, Operate, Optimize). Sehingga pada penelitian ini digunakan dalam perancangan monitoring jaringan menggunakan notifikasi Telegram.



Gambar 2.5 Siklus NDLC

Sumber: <http://repositori.unsil.ac.id/>

Adapun langkah-langkah penggunaan tahapan penelitian PPDIIO dilakukan sampai optimize. Tahapan penelitian akan dijelaskan sebagai berikut:

1. Prepare merupakan analisis masalah dengan melakukan studi literatur mengenai Telegram Bot API untuk notifikasi jaringan serta mengidentifikasi masalah dan sistem seperti yang diperlukan untuk mengatasi masalah tersebut.
2. Plan merupakan tahapan perancangan tentang sistem dan analisis kebutuhan yang akan dibuat apakah sesuai dengan kebutuhan yang diperlukan. Tahapan ini juga merencanakan susunan penelitian agar terorganisir dengan baik.
3. Design merupakan tahapan dilakukannya perancangan sistem yang akan dibangun. Mulai dari topologi hingga konfigurasi sistem yang dirancang.

4. Implement merupakan tahapan dimana melakukan monitoring jaringan serta penerapan notifikasi Telegram Bot API.
5. Operate merupakan percobaan dalam menjalankan program bot yang telah dibuat. Program bot diujicobakan ke dalam sistem monitoring agar setiap langkah dapat diamati saat melakukan pengujian. Data yang didapat pada tahapan ini menentukan apakah sistem dapat menjawab permasalahan yang telah dirumuskan.
6. Optimize melakukan pengoptimalan dalam setiap komponen perancangan. Mulai dari hardware, software dan kebutuhan perancangan bot yang lain seperti pengawasan terhadap pengaruh jaringan serta penambahan tiap komponen yang diperlukan.

2.1.8 Jaringan Internet

Menurut Andika (2019) Internet adalah jaringan komputer global yang saling terhubung secara global dan digunakan untuk berbagi informasi, komunikasi, dan akses ke berbagai sumber daya digital. Internet memungkinkan pengguna untuk mengirim dan menerima data dalam berbagai bentuk, seperti teks, gambar, video, dan suara, melalui protokol komunikasi yang disebut TCP/IP (Transmission Control Protocol/Internet Protocol). Internet memiliki beberapa komponen penting, termasuk infrastruktur fisik seperti kabel serat optik, satelit, dan jaringan nirkabel yang menghubungkan perangkat-perangkat komputer di seluruh dunia. Selain itu, internet juga melibatkan perangkat keras seperti server yang menyimpan dan mengelola informasi, serta perangkat lunak seperti browser web yang digunakan untuk mengakses dan menavigasi melalui konten online.

Dalam kehidupan sehari-hari, internet memberikan akses ke berbagai layanan dan sumber daya seperti pencarian informasi, media sosial, e-mail, perbankan online, belanja elektronik, dan hiburan digital. Internet juga menjadi fondasi bagi berbagai inovasi dan teknologi baru seperti Internet of Things (IoT), kecerdasan buatan, dan komputasi awan.

Namun, penting untuk diingat bahwa internet juga memiliki risiko dan tantangan seperti privasi dan keamanan data, penyebaran informasi palsu, kecanduan digital, dan kesenjangan akses. Oleh karena itu, penting bagi pengguna internet untuk menjaga keselamatan dan privasi mereka serta menggunakan internet dengan bijak.

A Sejarah Internet

Menurut Onno Purbo (2018) sejarah internet dimulai pada tahun 1969 ketika Departemen Pertahanan Amerika, U.S. DARPA (Defense Advanced Research Projects Agency) memutuskan untuk mengadakan riset tentang bagaimana caranya menghubungkan sejumlah komputer sehingga membentuk jaringan organik. Program riset ini dikenal dengan nama AILPAIET (Advanced Research project Agency Net). Pada tahun 1971, sudah lebih dari 10 komputer yang berhasil dihubungkan satu sama lain sehingga mereka bisa saling berkomunikasi dan membentuk sebuah jaringan.

Karena komputer yang membentuk jaringan semakin hari semakin bertambah jumlahnya, maka dibutuhkan sebuah protokol resmi yang diakui oleh semua jaringan. Pada tahun 1982 dibentuk Transmission Control Protocol atau TCP dan Internet Protocol atau lebih dikenal sebagai IP. Sementara itu di Eropa muncul jaringan komputer tandingan yang dikenal dengan EUnet (The European Network), yang menyediakan jasa jaringan komputer di negara-negara Eropa yakni Belanda, Inggris, Denmark, dan Swedia. Jaringan EUnet menyediakan jasa email dari newsgroup USENET.

Untuk menyeragamkan alamat di jaringan komputer yang ada, maka pada tahun 1984 diperkenalkan sistem nama domain, yang kini kita kenal dengan DNS atau Domain Name System. Oikarinen (1988) menemukan sekaligus memperkenalkan IRC atau Internet Relay Chat. Setahun kemudian, jumlah komputer yang saling terhubung kembali melonjak 10 kali lipat dalam setahun. Tak kurang dari 100.000 komputer kini membentuk sebuah jaringan. Kemudian pada tahun 1990 Tim Berners Lee menemukan program editor dan browser yang bisa menjelajah antara satu komputer dengan komputer lainnya, yang membentuk jaringan itu.

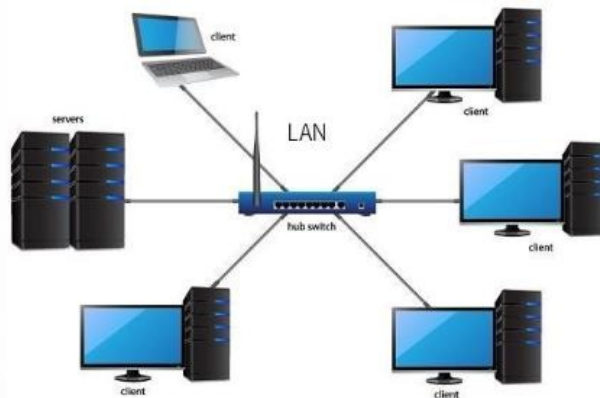
Program inilah yang disebut WWW atau World Wide Web. Tahun 1992, komputer yang saling tersambung membentuk jaringan sudah melampaui sejuta komputer, dan di tahun yang sama muncul istilah surfing the internet. Tahun 1994, situs internet telah tumbuh menjadi 3000 alamat halaman, dan untuk pertama kalinya virtual-shopping atau e-retail muncul di internet. Dunia langsung berubah, ditahun yang sama Yahoo! Didirikan, yang juga sekaligus kelahiran Netscape Navigator 1.0 yang dikembangkan oleh Netscape Communications Corporation pada tahun 1994.

B. Klasifikasi Jaringan

Klasifikasi jaringan komputer berdasarkan skala dibagi dalam empat bagian skala yang dimaksud disini adalah ukuran dari daerah cakupan jaringan komputer.

1. LAN (*Local Area Network*)

Local area network adalah jaringan lokal atau jaringan private yang ada dalam satu gedung atau dalam satu ruangan. LAN biasa di gunakan untuk jaringan kecil yang menggunakan satu resource secara bersama-sama, misalnya penggunaan printer secara bersama-sama, penggunaan media penyimpanan secara bersama, dan lain-lain.



Gambar 2.6 Local Area Network (LAN)

Sumber: <https://www.dataglobal.co.id/>

2. MAN (*Metropolitan Area Network*)

Metropolitan Area Network adalah pengembangan dari LAN yang menggunakan metode yang sama dengan LAN tetapi daerah cakupannya lebih luas.

Daerah cakupan LAN yang hanya ada pada satu ruangan atau gedung, tetapi pada MAN cakupannya bisa merupakan satu RT atau beberapa kantor yang berada dalam kompleks yang sama.



Gambar 2.7 Metropolitan Area Network (MAN)

Sumber: <https://www.dataglobal.co.id/>

3. WAN (*Wide Area Network*)

Wide Area Network dengan cakupan yang lebih luas lagi, cakupannya meliputi satu kawasan, satu pulau atau satu negara bahkan benua. Sedangkan metode yang di pakai dalam WAN hampir sama dengan yang di pakai di dalam LAN dan MAN.



Gambar 2.8 Wide Area Network (WAN)

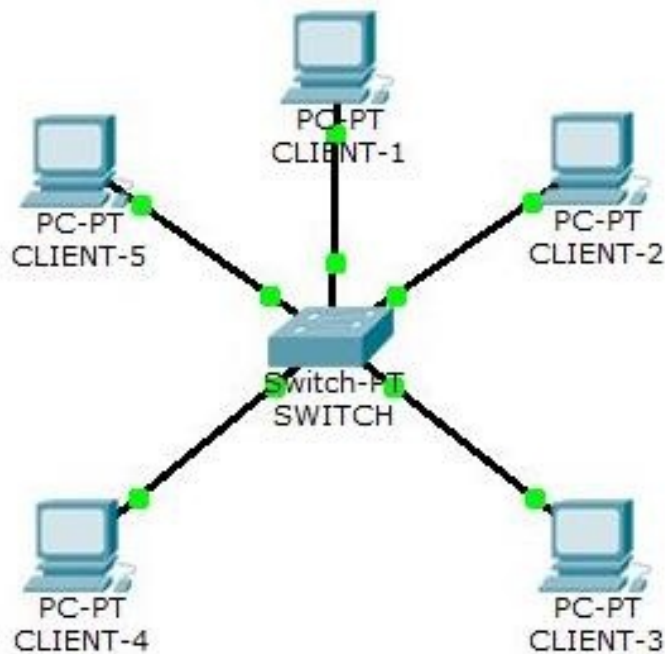
Sumber: <https://www.dataglobal.co.id/>

2.1.9 Topologi Jaringan

Topologi jaringan merujuk pada pola atau struktur fisik dari bagaimana perangkat-perangkat komputer di dalam jaringan saling terhubung. Ini mencakup bagaimana perangkat-perangkat tersebut diatur, dihubungkan, dan berkomunikasi satu sama lain.

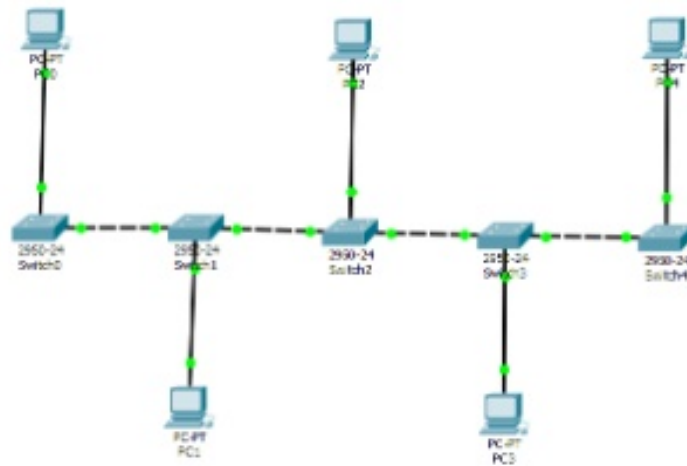
Berikut adalah beberapa jenis topologi jaringan yang umum digunakan:

1. Topologi Bintang: Dalam topologi ini, setiap perangkat terhubung langsung ke satu titik pusat atau switch. Jika salah satu perangkat mati atau mengalami masalah, perangkat lainnya tidak terpengaruh.



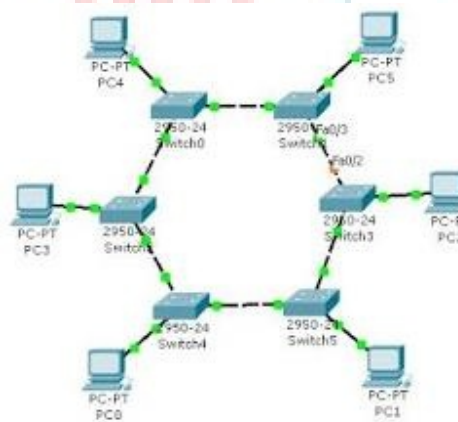
Gambar 2.9 Gambar Topologi *Star*

2. Topologi Bus: Dalam topologi ini, semua perangkat terhubung ke kabel tunggal yang disebut bus. Data dikirimkan melalui kabel dan diterima oleh semua perangkat. Jika ada gangguan pada kabel, seluruh jaringan dapat terpengaruh.



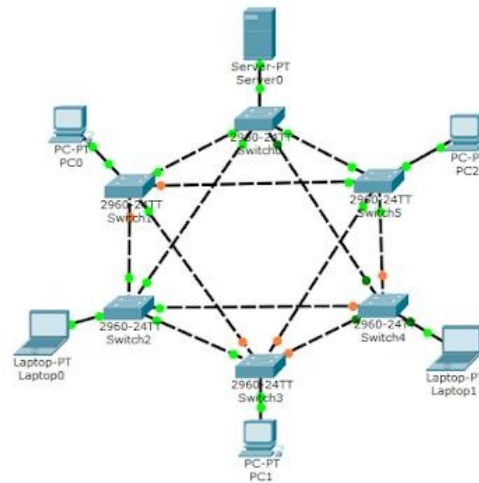
Gambar 2.10 Topologi Bus

3. Topologi Cincin (Ring): Dalam topologi ini, setiap perangkat terhubung ke perangkat sebelumnya dan sesudahnya, membentuk cincin tertutup. Data dikirimkan dalam satu arah melalui cincin. Jika salah satu perangkat bermasalah, dapat mengganggu seluruh jaringan.



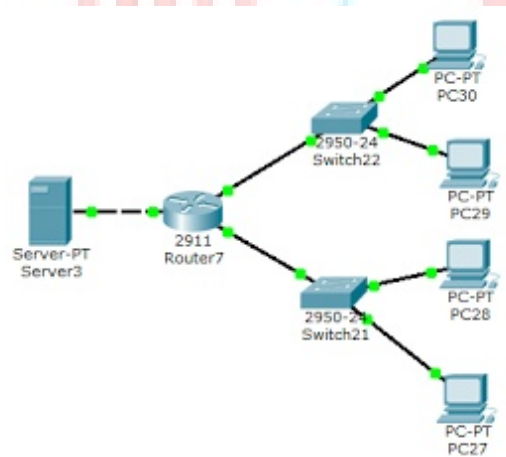
Gambar 2.11 Topologi Ring

4. Topologi Mesh: Dalam topologi ini, setiap perangkat terhubung langsung ke setiap perangkat lain dalam jaringan. Ini memastikan redundansi dan keterhubungan yang tinggi, sehingga jika satu jalur mengalami gangguan, ada jalur alternatif yang dapat digunakan.



Gambar 2.12 Topologi Mesh

5. Topologi Pohon: Dalam topologi ini, perangkat-perangkat dihubungkan dalam hierarki seperti struktur pohon, dengan satu perangkat pusat yang menghubungkan beberapa perangkat cabang. Ini memungkinkan skala besar dan pemantauan yang efisien.



Gambar 2.13 Topologi Tree

Setiap jenis topologi memiliki kelebihan dan kelemahan tertentu tergantung pada kebutuhan dan lingkungan jaringan yang digunakan. Pemilihan topologi yang tepat akan mempengaruhi performa, skalabilitas, kehandalan, dan efisiensi jaringan.

2.1.10 Monitoring

Monitoring adalah proses pemantauan dan pengawasan secara terus-menerus terhadap suatu sistem, proses, atau aktivitas dengan tujuan mengumpulkan informasi yang relevan mengenai kondisi, kinerja, atau perubahan yang terjadi. Pengertian monitoring menurut ahli dapat berbeda-beda, namun pada dasarnya memiliki konsep yang serupa. Berikut ini adalah pengertian monitoring menurut beberapa ahli:

Menurut ITIL (Information Technology Infrastructure Library):

"Monitoring adalah kegiatan pengumpulan data dalam suatu lingkungan TI, dilakukan secara terus-menerus atau periodik, yang dilakukan untuk mendapatkan informasi mengenai kinerja, kualitas, atau keandalan suatu sistem, proses, atau layanan."

Menurut Jim Highsmith (Ahli Manajemen Proyek):

"Monitoring adalah kegiatan pemantauan secara terus-menerus untuk mendapatkan gambaran nyata mengenai kinerja proyek dan menentukan apakah proyek tersebut berjalan sesuai dengan rencana atau tidak."

Menurut Gartner:

"Monitoring adalah proses pengawasan dan evaluasi terus-menerus terhadap suatu sistem, aplikasi, atau infrastruktur untuk mendeteksi masalah, mengukur kinerja, dan melaporkan informasi yang relevan kepada pemangku kepentingan."

Menurut Robert L. Goodwin (Ahli Manajemen):

"Monitoring adalah kegiatan pengawasan yang melibatkan pengukuran, pengamatan, dan pemantauan terhadap proses, aktivitas, atau sistem guna memastikan bahwa tujuan, standar, atau kriteria yang ditetapkan tercapai atau terpenuhi."

Dalam semua definisi ini, monitoring diartikan sebagai kegiatan yang berkelanjutan untuk mengumpulkan informasi yang relevan, menganalisisnya, dan mengambil tindakan yang diperlukan berdasarkan hasil pemantauan. Tujuan dari monitoring adalah untuk mengidentifikasi masalah, mengukur kinerja, mengoptimalkan proses, dan memastikan bahwa tujuan yang ditetapkan tercapai.

2.1.11 Metode Blackbox Testing

Menurut (Greenit, 2018) Metode Black Box Testing yaitu pengujian yang dilakukan untuk eksekusi melalui data uji dan memeriksa fungsional dari perangkat lunak. Pengamatan hasil ini melalui data uji dan memeriksa fungsional yang didapat dari perangkat lunak itu sendiri. Pada pengujian black box testing ini dapat mengevaluasi pada tampilan luarnya saja (interface) fungsionalnya, dan tidak melihat apa yang sesungguhnya terjadi dalam proses detailnya. Hanya mengetahui proses input dan output-nya saja. Black Box Testing juga memiliki fungsi-fungsi adalah sebagai berikut:

1. Menemukan fungsi-fungsi yang salah atau hilang didalam suatu software.
2. Mencari kesalahan interface yang terjadi pada saat software dijalankan.
3. Untuk mengetahui kesalahan dalam struktur data atau akses database eksternal didalam suatu aplikasi.
4. Menguji kinerja dari software tersebut.
5. Menginisialisasikan dan mencari kesalahan dari terminasi software itu sendiri.

2.2 Tinjauan Studi

Adapun beberapa jurnal-jurnal dari penelitian yang terdahulu dan memiliki manfaat bagi penulis untuk dijadikan acuan guna mendapatkan pengetahuan dan teori yang memiliki kaitan dengan penelitian saat ini. Berikut ini adalah beberapa referensi jurnal yang dijadikan pendukung untuk penelitian ini :

1. Artikel hasil penelitian yang dilakukan oleh I Wayan Krisna Saputra, Dewa Made Wiharta, dan Nyoman Putra Sastra pada tahun 2020 yang berjudul **“IMPLEMENTASI SISTEM PEMANTAUAN JARINGAN MENGGUNAKAN LIBRENMS PADA JARINGAN KAMPUS UNIVERSITAS UDAYANA”** yang dipublikasikan oleh Jurnal SPEKTRUM, Vol. 7, No. 2 Juni 2020 Didalam Artikel ini berisi tentang membahas mengenai suatu permasalahan pada Universitas Udayana yang merupakan lembaga pendidikan tinggi yang telah menerapkan sistem

pembelajaran secara online. Sistem ini tentunya memerlukan akses internet yang cepat dan memadai agar mahasiswa dapat mengakses sistem pembelajaran secara nyaman dan efisien. Dalam memenuhi kebutuhan akan teknologi internet, sudah menjadi keharusan bagi institusi untuk menyediakan infrastruktur yang mampu menjaga agar layanan internet dapat berjalan dengan lancar. Pemantauan kondisi jaringan memerlukan aplikasi yang disebut dengan istilah Network Monitoring System.

2. Artikel hasil penelitian yang dilakukan oleh Alfian Tegar Putra Afandi ,dan Asmunin pada tahun 2019 yang berjudul “**Implementasi Network Monitoring System Menggunakan Librenms Berbasis Docker Container**” yang dipublikasikan oleh ejournal unesa, Vol. 5, No. 1 Mey 2019 Didalam Artikel ini berisi tentang sebuah instansi, jaringan selalu dibutuhkan untuk memenuhi kebutuhan transfer data dan sinkronasi dari setiap perangkat yang dipakai. Terutama pada era pandemi covid-19 hampir segala kegiatan dilakukan secara daring menyebabkan peningkatan penggunaan jaringan pada instansi. Hal ini tentu harus didukung dengan pemantauan secara intensif terhadap perangkat jaringan pada sebuah instansi untuk menjaga layanan tersebut agar tetap stabil saat digunakan oleh pengguna. Salah satu hal yang dapat dilakukan adalah penerapan Network Monitoring System yang bertujuan untuk memantau kondisi pada perangkat jaringan apakah dalam keadaan baik ataupun sebaliknya dengan bantuan aplikasi Librenms. Librenms merupakan aplikasi pemantau jaringan yang bersifat open source dan memiliki banyak fitur. Seperti: dapat melakukan pemindaian perangkat jaringan secara otomatis, pemantauan terhadap kondisi trafik penggunaan data, pemantauan kondisi pada perangkat jaringan yang direpresentasikan menggunakan Rrdtool sebagai pembuat grafik. Sistem ini juga dapat berjalan pada platform docker yang didalamnya terdapat aplikasi librenms beserta aplikasi pendukung lainnya yang dikonfigurasi dan dijalankan secara bersamaan menggunakan docker compose. Dengan adanya docker, aplikasi yang dijalankan dapat berjalan secara terisolasi dalam sebuah container tanpa memerlukan hypervisor dan OS tambahan, sehingga dapat mengurangi penggunaan sumber daya komputer server dalam menjalankan virtualisasi.

3. Artikel hasil penelitian yang dilakukan oleh Muhtar Efendy, dan Mochamad Mizanul Achlaq pada tahun 2022 yang berjudul **“Implementasi Sistem Monitoring Dan Backup Konfigurasi Perangkat Jaringan Menggunakan Librenms Di Pt. Data Utama Dinamika”** yang dipublikasikan oleh ejournal poltektegal, Vol. 11, No. 4 (2022) Didalam Artikel ini berisi tentang sebuah pt yang memerlukan sistem monitoring jaringan diperlukan untuk mengetahui dalam sebuah jaringan adanya permasalahan dan monitoring tersebut memerlukan sebuah aplikasi Network Monitoring System. Ada beberapa macam aplikasi monitoring jaringan yang tersedia secara gratis maupun berbayar. LibreNMS merupakan salah satu aplikasi monitoring jaringan yang dapat digunakan secara gratis yang berbasis PHP, MYSQL, SNMP. LibreNMS merupakan aplikasi monitoring jaringan yang mempunyai banyak fitur yang menyediakan dukungan untuk berbagai perangkat jaringan. Penggunaan LibreNMS berpotensi untuk membantu administrator jaringan memonitoring jaringan agar dapat berjalan dengan lancar serta apabila ada permasalahan dapat segera dilakukan perbaikan. Dan LibreNMS dapat ditambahkan sebuah fitur yang Device Backup Integration yaitu Oxidized untuk mencadangkan secara otomatis konfigurasi perangkat jaringan yang telah ditambahkan agar saat perangkat jaringan tidak bisa digunakan dapat mengambil backup file konfigurasi yang telah dicadangkan dan tanpa perlu melakukan konfigurasi dari awal saat mengganti perangkat jaringan dengan yang baru. Hasil penelitian ini bertujuan untuk membuat sebuah sistem monitoring dan pencadangan otomatis untuk perangkat jaringan di PT. Data Utama Dinamika menggunakan LibreNMS.

4. Penelitian Empat yang dilakukan oleh Bambang Sunardi (2020) dengan judul **“Rancang Bangun Aplikasi Monitoring Jaringan Menggunakan SNMP (Simple Network Management Protocol) dengan Sistem Peringatan Dini dan Mapping Jaringan”** penelitian pada jurnal ini membahas mengenai suatu permasalahan pada PT Anugerah Komputer yang merupakan perusahaan yang bergerak dibidang IT yang telah menerapkan sistem kerja secara online. Sistem ini tentunya memerlukan akses internet yang cepat dan memadai agar karyawan dapat mengakses sistem secara nyaman dan efisien. Dalam memenuhi kebutuhan akan teknologi internet, sudah menjadi keharusan bagi institusi untuk menyediakan infrastruktur yang mampu

menjaga agar layanan internet dapat berjalan dengan lancar. Pemantauan kondisi jaringan memerlukan aplikasi yang disebut dengan istilah Network Monitoring System.

5. Penelitian Kelima yang dilakukan oleh Andrew (2018) dengan judul **“Network Development Life Cycle (NDLC) Dalam Perancangan Jaringan Komputer Pada Rumah Shalom Mahanaim “** penelitian pada jurnal ini membahas mengenai suatu permasalahan pada jaringan computer di Rumah Shalom Mahanim. Sistem ini tentunya memerlukan akses internet yang cepat dan memadai agar karyawan dapat mengakses sistem secara nyaman dan efisien. Dalam memenuhi kebutuhan akan teknologi internet, sudah menjadi keharusan bagi institusi untuk menyediakan infrastruktur yang mampu menjaga agar layanan internet dapat berjalan dengan lancar. Pemantauan kondisi jaringan memerlukan aplikasi yang disebut dengan istilah Network Monitoring System.

6. Penelitian Keenam yang dilakukan oleh Bambang Sudarmono (2020) dengan judul **“Rancang Bangun Aplikasi Monitoring Jaringan Menggunakan SNMP (Simple Network Management Protocol) dengan Sistem Peringatan Dini dan Mapping Jaringan“** penelitian pada jurnal ini membahas mengenai suatu permasalahan pada PT Anugerah Komputer yang merupakan perusahaan yang bergerak dibidang IT yang telah menerapkan sistem kerja secara online. Sistem ini tentunya memerlukan akses internet yang cepat dan memadai agar karyawan dapat mengakses sistem secara nyaman dan efisien. Dalam memenuhi kebutuhan akan teknologi internet, sudah menjadi keharusan bagi institusi untuk menyediakan infrastruktur yang mampu menjaga agar layanan internet dapat berjalan dengan lancar. Pemantauan kondisi jaringan memerlukan aplikasi yang disebut dengan istilah Network Monitoring System.