BAB II
TINJAUAN PUSTAKA

2.1 Tinjauan Pustaka

Dwi Wijonarko, pada tahun 2014 merancang sebuah sistem monitoring jaringan menggunakan Zabbix Server pada Ubuntu 12.04 LTS untuk memantau jaringan di Dinas KOMINFO Kota Malang, seluruh kantor SKPD dan seluruh kelurahan di Kota Malang. Dimana sebelumnya dilakukan uji coba terlebih dahulu menggunakan jaringan komputer di POLITEKNIK Kota Malang. Dari penelitian ini didapatkan kesimpulan bahwa Zabbix dapat memberikan informasi kondisi server secara *realtime* seperti suhu, kecepatan lintas data, kinerja dan media penyimpanan yang tersedia. Adanya notifikasi berupa email juga sangat membantu *administrator* (Wijonarko, 2014).

Pada tahun 2010 Dedy Cahyadi, Fahrul Agus, Mahfud Iman, melakukan penelitian menggunakan *Network Monitoring System* untuk memantau kondisi jaringan di Pemprov Kaltim dengan tujuan sebagai bahan pertimbangan untuk keperluan pengembangan jaringan disana. Setelah dilakukan pemantauan disana ditemukan masalah seperti *flooding* atau kondisi dimana lalu lintas jaringan dibanjiri oleh paket-paket data dan *down* atau kondisi dimana tidak ada lalu lintas keluar masuk jaringan. Dari masalah ini diidentifikasi 2 faktor penyebabnya yaitu faktor teknis (asupan daya listrik tidak stabil, dan infrastruktur jaringan sudah tidak layak pakai) dan faktor non teknis (*force majeur,* kurangnya dukungan dalam operasional). Lalu dari identifikasi masalah diatas pemprov Kalimantan Timur dianjurkan untuk menyediakan peralatan cadangan, jalur *backup*, prosedur *Disaster Recovery System,* membuat kebijakan dalam pengelolaan jaringan serta memberikan dukungan dana dan sumber daya manusia (Cahyadi, Agus, & Iman, 2010).

Herman Kuswanto pada penelitiannya ditahun 2018, membahas tentang pengguanaan Nagios pada Ubuntu server 14.04.1 untuk mengawasi jaringan dengan menggunakan email untuk memberikan notifikasi apabila ada kesalahan pada jaringan. Dari hasil penelitian yang dilakukan didapat kesimpulan bahwa aplikasi

Nagios dapat mendeteksi apabila ada kondisi *Up* atau *Down* pada jaringan yang sedang diawasi secara *realtime*, notifikasi akan langsung tampil pada *web interface* dari Nagios dan akan mengirimkan notifikasi berupa email dalam waktu kurang dari 1 menit. Penggunakan Nagios juga dapat mempermudah dalam mengawasi kondisi jaringan sehingga mempermudah dalam *troubleshooting* masalah jaringan (Kusmanto, 2018).

Indra Thamrin, Justinus Andjarwirawan, & Agustinus Noertjahyana pada tahun 2017 membuat penelitian yang membahas tentang penggunaan *software* Zabbix untuk menjadi perangkat *monitoring* jaringan dengan memanfaatkan fitur SMS (*Short Message Service)* API (*Application Programable Interface*) dan *Telegram* API yang ditawarkan Zabbix sebagai sistem pemberitahuan kepada *administrator* apabila terjadi masalah dalam jaringan. Pada penelitian ini yang diawasi adalah *traffic* dari jaringan. Dari penelitian yang telah dilakukan didapat hasil bahwa Zabbix dapat menampilkan hasil grafik yang akurat mulai dari *traffic* saat ini, *traffic* tertinggi serta terendah. *Notifikasi* SMS API dan *Telegram* API yang diterapkan juga dapat berjalan dengan baik dengan mampu memberi notifikasi kepada *administrator* ketika terjadi *error* pada jaringan tersebut (Thamrin, Andjawirawan, & Noertjahyana, 2017).

Susmini Indriani Lestariningati dan Fathur Rozak pada tahun 2014 melakukan penelitian yang membahas tentang pembangunan aplikasi monitoring jaringan yang berbasis *web* dengan menggunakan SNMP (*Simple Network Monitoring Protocol*). Pada penelitian ini terdapat 2 komponen utama yaitu *manager* yang merupakan server dari NMS serta *agent* yang merupakan *client* yang terdiri dari PC maupun *router.* Untuk pengambilan data, sistem ini menggunakan SNMP sebagai medianya. Untuk membuat dan menjalakan antarmukanya sistem ini menggunakan aplikasi SNMP versi 5.6.1.1, Mysql versi 5.6.12, PHP 5.4.12, Apache 2.4.4 yang dijalakan pada sistem operasi Windows 7 dan Linux Ubuntu 12.04. Dari penelitian ini dihasilkan sebuah sistem monitoring berbasis web yang dapat menampilkan status dari *agent* yang dimonitor dengan mengambil dan menerima data dari *agent* melalui protokol SNMP (Lestariningati, & Rozak, 2014).

2.2 Landasan Teori

2.2.1 *NMS (Network Monitoring System)*

NMS (Network Monitoring System) adalah suatu sistem yang dibuat untuk mengawasi suatu jaringan tertentu dengan tujuan untuk menjaga agar jaringan dapat bekerja sesuai dengan mestinya. Pemanfaatan sistem monitoring jaringan dapat memudahkan pengelola jaringan dalam memonitor jaringanya dan dapat dimonitor dari manapun selama masih terhubung dengan internet (Wijonarko, 2014).

Fungsi dari NMS adalah untuk mengawasi masalah-masalah terjadi pada jaringan dan memberikan notifikasi kepada *administrator,* masalah itu bisa berupa koneksi jaringan yang down atau kurang memadai atau komputer klien yang sudah tidak mampu untuk mengerjakan tugasnya dengan baik, maka NMS akan memberikan notifikasi kepada *administrator.*

Sebagai contoh apabila ada perangkat dalam sebuah jaringan yang terintegrasi dengan NMS mengalami *overload* pada *memory* maka NMS akan mengirimkan notifikasi kepada *administrator* bahwa suatu perangkat mengalami *overload* pada *memory*.

Konsep *Network Monitoring System* (NMS) sebenarnya sederhana yaitu sistem ekstra atau kumpulan sistem yang memiliki tugas mengamati/memonitor sistem-sistem terhadap kemungkinan terjadinya masalah-masalah pada sistem tersebut untuk dapat dideteksi secara dini.

Apabila sistem yang sedang dimonitor mengalami kerusakan maka sistem ini dapat mengirim notifikasi lewat SMS (*Short Message Service*) atau email kepada *administrator* sesuai dengan pengaturan yang diuat. Jika kriteria krisis yang dipilih tidak tepat maka kemungkinan sistem akan memberi peringatan terus menerus.

2.2.2 Zabbix

Zabbix merupakan aplikasi pemantauan ketersediaan dan performa jaringan komputer kode terbuka (*opensource*) (Santosa, 2010). Dengan Zabbix, *administrator* dapat mudah mengetahui kondisi server, jaringan dan juga akan mendapatkan notifikasi apabila terjadi suatu gangguan.

Keunggulan dari *software* ini adalah gratis dengan UI (*User Interface)* yang dapat mudah dimengerti karena sudah menggunakan UI berbasis *graphic* atau biasa disebut GUI (*Graphic User Interface*). Dengan UI yang mudah dimengerti penggunaan Zabbix juga menjadi lebih mudah. Zabbix juga dapat membuat *map* dari suatu jaringan dan menampilkan grafik dari kondisi jaringan yang sedang diawasi.

Administrator dapat mengatur berapa periode penggiriman laporan, bisa setiap hari, setiap minggu, atau setiap bulan. *Administrator* juga dapat memilih notifikasi apa yang akan dipakai, bisa menggunakan e-mail maupun SMS (*Short Messange Service*).

a) Fitur Zabbix

Dalam menjalankan fungsinya Zabbix memiliki beberapa fitur yang disuguhkan bagi penggunanya diantaranya:

1) *User Friendly*, UI yang digunakan Zabbix sangat mudah untuk dimengerti bahkan bagi orang yang masih awam, karena sudah menggunakan UI berbasis GUI dan tampilannya juga menarik.
2) *Real time Monitoring.*
3) Mampu memberikan notifikasi kepada *administrator* berupa e-mail atau SMS.
4) Filter untuk laporan *traffic*, *Admini*strator dapat membuat laporan dengan *template* yang berbeda-beda.
5) *Multi Operating System.*
6) Sisi Keamanan cukup unggul karena adanya *authentification* dengan *IP addresses.*

b) Komponen Zabbix :

Zabbix memiliki beberapa komponen utama didalam nya untuk menjalankan tugasnya, yaitu:

1) Zabbix Server

   Zabbix seerver merupakan kompenan utama Zabbix. Komponen inilah yang akan menerima data dari klien untuk kemudian ditampilkan di halaman *dashboard*.

2) Zabbix Agent

Zabbix *agent* merupakan komponen yang bertugas untuk mengambil data dari klien untuk kemudian dikirimkan ke server.

3) Zabbix *Web Interface*

Disinilah data yang sudah diterima oleh server akan ditampilkan, setelah melakukan beberapa pengaturan, maka data akan tertampil pada halaman *dasboard*.

c) *Problem By Severity*

Zabbix memiliki klasifikasi sendiri terdahap masalah yang terjadi pada perangkat jaringan. Klasifikasi ini dibagi dengan beberapa tingkatan berdasarkan seberapa pentingnya masalah itu. Tabel 2.1 *Problem by severity* menunjukan tingkatan menurut klasifikasi Zabbix sesuai dengan panduan dari *website* resmi Zabbix.

Tabel 2.1 Problem by severity

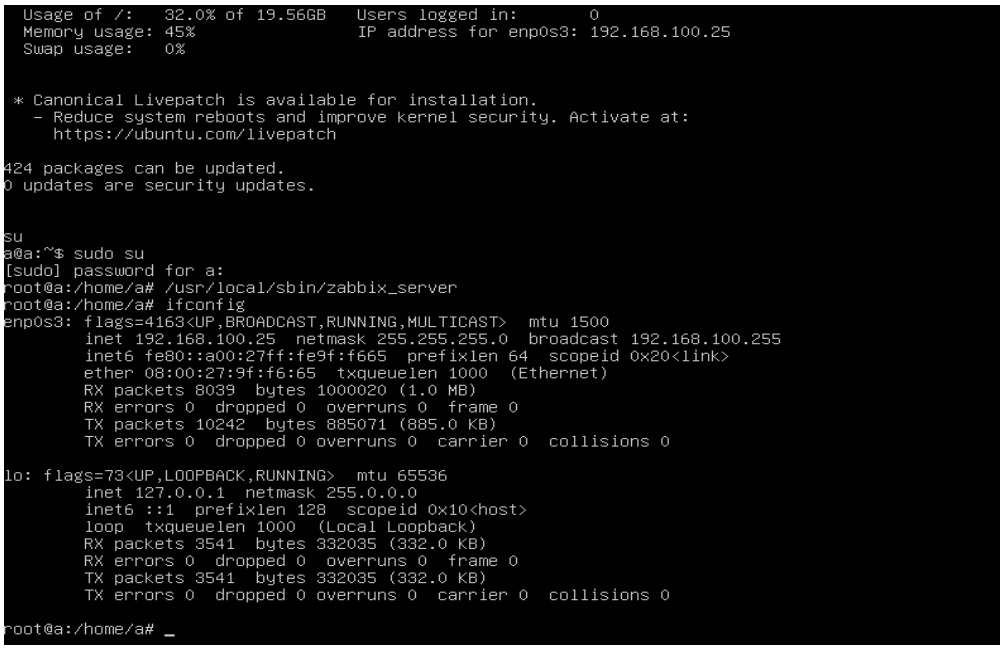
Severity	Keterangan	Warna
Not Clasiffied	Tidak terklasifikasi atau masalah yang belum diketahui.	Abu-abu
Information	Merupakan notifikasi yang hanya berupa informasi.	Hijau terang
Warning	Saat muncul notifikasi ini *administrator* dihimbau untuk waspada.	Kuning
Average	Notifikasi untuk masalah yang biasanya sering muncul.	Oranye
High	Apabila muncul notifikasi ini maka anrtinya ada sesuatu hal penting yang terjadi.	Merah
Disaster	Bencana	Merah terang

2.2.3 Linux Ubuntu 18.04 Server

Linux dalam arti luas adalah sistem operasi yang telah dilengkapi program-program untuk bekerja di terminal seperti DOS dan aplikasi desktop seperti windows atau machintos. Dalam arti sempit atau pengertian teknis, linux adalah kernel atau inti dari sistem operasi yang bersifat *open source*.(Rusmanto, 2005).

Ubuntu merupakan distro linux berbasi debian yang disponsori secara resmi oleh canonical LTD, yang berasal dari Afrika Selatan. Nama Ubuntu sendiri merupakan istilah dari Afrika Selatan yang artinya "Kemanusiaan Kepada Sesama".

Linux Ubuntu 18.04 *Bionic Beaver* adalah sistem operasi *open source* yang rilis pada 26 April 2018. Versi ini merupakan versi yang bersifat LTS (*Long Term Service*) yang artinya pengguna akan mendapat support jangka panjang selama 5 tahun sampai tahun 2023. Tampilan dari linux Ubuntu 8.04 server dapat dilihat pada Gambar 2.1 Tampilan Ubuntu 18.04 Server.



Gambar 2.1 Tampilan Ubuntu 18.04 Server

a) Filosofi Ubuntu

Adapaun filosofi yang dianut Ubuntu adalah:

1) Bahwa *software* harus bebas biaya

2) bahwa *software* harus bisa digunakan dalam bahasa lokal masing-masing dan untuk orang-orang yang mempunyai keterbatasan fisik
3) bahwa pengguna harus mempunyai kebebasan untuk mendapatkan, mengubah, dan mendistribusikan perangkat lunak sesuai dengan apa yang mereka butuhkan tanpa halangan apapun.

2.2.4 Windows 10

Sistem operasi komputer adalah perangkat lunak komputer atau *software* yang bertugas untuk melakukan kontrol dan manajemen perangkat keras dan juga operasi-operasi dasar sistem, termasuk menjalankan *software* aplikasi seperti program-program pengolah data yang bisa digunakan untuk mempermudah kegiatan manusia (Haryanto, 2012).

Windows 10 merupakan seri dari sistem operasi Windows yang diluncurkan pada Juli 2015. Windows sendiri merupakan sistem operasi berbasis GUI yang diciptakan oleh Microsoft. Dengan adanya teknologi GUI atau *Graphic User Interface* pengoperasian komputer menjadi lebih mudah karena pengguna tidak harus menghafalkan perintah-perintah untuk menjalankan program didalam komputer.

Fungsi dari Windows ini kurang lebih sama dengan sistem operasi lain yakni menjadi jembatan antara perangkat lunak yang akan diakses pengguna dengan perangkat keras yang bertugas untuk menjalankan prosesnya, sehingga keduanya dapat bekerja secara konsisten dan stabil. Mengelola sumber daya yang tersedia serta mengelola sistem I/O (*Input/Output*). Tampilan dari Windows dapat dilihat pada Gambar 2.2 Contoh tampilan Windows 10

Gambar 2.2 Contoh tampilan Windows 10

2.2.5 Mikrotik

Mikrotik merupakan sistem operasi router, yang di-*release* dengan nama mikrotik routerOs yang mampu diinstall pada komputer biasa, tidak seperti sistem operasi router lainya yang hanya bisa diinstall pada hardware tertentu. Mikrotik memiliki fitur yang sangat lengkap diantaranya : *Firewall* dan NAT, *Routing*, *Hotspot*, *Point to Point Tunneling Protocol*, DNS server, DHCP server, Manajemen *Bandwidth*, Konfigurasi Keamanan dan masih banyak fitur lainya (http://mikrotik.co.id/). Mudah dikonfigurasi dan tentunya harganya yang murah. Jadi Mikrotik RouterOs difungsikan untuk membagi-bagi koneksi Internet ke beberapa komputer pengguna *user* (Riadi, 2011).

a) Fitur Mikrotik

Fitur dari mikrotik dapat dilihat pada Tabel 2.2 Fitur Mikrotik

Tabel 2.2 Fitur Mikrotik

Fitur	Keterangan
NAT (*Network Address Translation*)	*Network Address Translation* berfungsi untuk menyamarkan ip publik ke ip privat
Routing-Static	*Static Routing* adalah jenis *routing* dimana tabel *routing* akan dibuat secara manual. Mulai dari ip *address* hingga *gateway* harus ditulis manual pada sisi pengguna.
Data Rate Management	Pengelolaan kecepatan transmisi data dalam satuan *bit persecond* (bps).
Hotspot	Sebuah area dimana perangkat yang memiliki fitur *Wireless Fidelity* (*Wi-Fi)* dapat terkoneksi ke jaringan.
Point-to-Point tunneling protocols	Protokol (seperangkat aturan komunikasi) yang memungkinkan perusahaan memperluas jaringan perusahaan mereka sendiri melalui "terowongan" pribadi melalui Internet publik.
IPSec	Seperangkat aturan untuk mengaman transmisi data pada jaringan TCP/IP (*Transfer Control Protocol/Internet Protocol*)
Web proxy	Perantara antara pengguna dengan server sehingga pengguna tidak akan berhubungan langsung dengan server yang ada di internet.

Tabel 2.2 Fitur Mikrotik (Lanjutan)

Fitur	Keterangan
DHCP (*Dynamic Host Configuration Protocol)*	Konfigurasi *routing* dimana tabel *routing* akan dibuat otomatis. Fitur ini juga akan mencari rute tercepat dalam pengiriman data.
Monitoring	Mikrotik memiliki fitur *monitoring* dengan sebuah aplikasi bernama *The Dude* yang memang dirancang untuk mengawasi suatu jaringan komputer yang terintegrasi dengan Mikrotik.
SNMP (*Simple Network Monitoring Protocol)*	Seperangkat aturan standar yang digunakan untuk mengawasi perangkat yang terdapat pada jaringan.
NTP (*Network Time Protocol*)	Protokol untuk melakukan sinkronasi waktu.
VRRP (*Virtual Router Redudancy Protocol*)	Sebuah antarmuka (*virtual*) dari sistem operasi Mikrotik yang memungkinkan untuk menjadikan beberapa router dari jaringan lokal yang satu *segment* untuk menjadi gateway.
UPnP	*Universal Plug and Play* merupakan fitur yang memungkinkan perangkat yang terhubung untuk tegabung secara otomatis dalam jaringan tanpa perlu konfigurasi secara manual.

Tabel 2.2 Fitur Mikrotik (Lanjutan)

Fitur	Keterangan
MNDP (*Mikrotik Neighbors Discovery Protocol*)	Merupakan lapisan ke-2 *broadcast domain* yang mengijinkan perangkat yang mendukung MNDP untuk saling "menemukan".
Firewall	Firewall adalah sistem keamanan untuk mengelola dan memantau trafik masuk dan keluar berdasarkan aturan keamanan (*security rules*) yang sudah ditentukan. Firewall berfungsi mencegah akses yang tidak diinginkan dari atau ke dalam jaringan atau server.

b) Fungsi Mikrotik

Mikrotik banyak digunakan untuk mengkonfigurasi sebuah jaringan mulai dari tipe *routing* yang akan digunakan, pembagian *bandwidth* bagi masing-masing *user* serta dapat juga untuk mengatur pengaman jaringan serta mengawasi jaringan tersebut.

c) Mikrotik *RouterBoard*

RouterBoard merupakan produk mikrotik yang berbentuk fisik atau *hardware* yang sudah terpasang Mikrotik OS didalamnya sehingga pengguna hanya perlu melakukan *setting* lewat *software* WinBox.

RouterBoard ini sama seperti komputer biasa hanya saja ukurannya lebih kecil karena fungsinya yang dikhususkan untuk *routing.*

d) RouterOS

Sebuah OS (*Operating System*) berbasis Unix yang dapat membuat PC memiliki kemampuan seperti sebuah *router* untuk mengatur *firewall, hotspot, proxy, routing, NAT, bandwidth management* dan fungsi *router* lainnya.

2.2.6 *Data Traffic*

Data Traffic atau lalu lintas data adalah lalu lintas dari data yang keluar masuk pada jaringan komputer. Kepadatan lalu lintas data ini akan dipengaruhi oleh jumlah data dan ukuran *bandwidth*. Apabila data yang masuk banyak dan *bandwidth* yang digunakan sempit maka akan terjadi kemacetan lalu lintas data yang menyebabkan data menjadi lama untuk dikirim. Sehingga dibutuhkan *bandwidth* yang lebar untuk memenuhi lalu lintas data yang padat.

2.2.7 *Bandwidth*

Bandwidth adalah suatu nilai konsumsi transfer data yang dihitung dalam bit/detik atay yang biasanya di sebut dengan *bit per second* (bps), antara server dan client dalam waktu tertentu. Atau bisa didefinisikan sebagai lebar cakupan frekuensi yang dipakai oleh sinyal dalam medium transmisi (Sora N, 2015).Setiap jaringan biasanya memiliki batasan tertentu terhadap *bandwidth* yang dapat digunakan tiap pengguna, semakin besar kapasitas *bandwidth* maka semakin banyak data yang dapat dikirim dalam satu detik.

Kapasitas *bandwidth* jaringan komunikasi dapat mempengaruhi kinerja jaringan tersebut, apakah cepat atau lambat. Namun, tentu saja masih ada faktor lain yang mempengaruhinya, misalnya *latency*, *packet loss*, dan lain-lain.

2.2.8 *Throughput*

Throughput adalah *bandwidth* aktual. Jika *bandwidth* adalah batas maksimum, *throughput* adalah sesuai dengan data aktual yang mengalir pada media transmisi. *Throughput* merupakan salah satu parameter yang menunjukan kinerja dari suatu sistem komunikasi data (Arwani, 2015).

Misalnya, jika menggunakan internet pada *bandwidth* 5 *Mega bit persecond* (Mbps), dan terlihat kecepatan 4,2 Mbps saat mengunduh file dari internet, kecepatan ini disebut *throughput*, sehingga dapat disimpulkan bahwa *throughput* lebih kecil dari *bandwidth*.

Throughput adalah bandwidth aktual, diukur dalam satuan waktu tertentu dan dalam kondisi jaringan tertentu yang digunakan untuk mentransfer file dengan ukuran tertentu.

2.2.9 VirtualBox

Gambar 2.3 Oracle VirtualBox

VirtualBox adalah *software* virtualisasi. yang memiliki kemampuan untuk membuat lingkung hidup virtual untuk OS (Indyawan, 2018). VirtualBox merupakan *software virtual machine* buatan Oracle. Logo dari VirtualBox dapat dilihat pada Gambar 2.3 Oracle VirtualBox. VirtualBox ini berfungsi untuk membuat satu atau beberapa sistem operasi secara *virtual* di dalam sistem operasi utama. Sehingga seakan-akan terdapat komputer dalam komputer. *Software* ini sangat berguna untuk membuat simulasi jaringan karena dapat membuat komputer *virtual* sehingga tidak diperlukan banyak komputer saat simulasi. Pada penelitian ini VirtualBox yang digunakan adalah versi 5.2.32 yang dirilis pada Juli 2019.

Untuk bisa terkoneksi dengan jaringan, VirtualBox memiliki beberapa metode, metode ini dapat dilihat dari Tabel 2.3 Metode koneksi jaringan VirtualBox.

Tabel 2.3 Metode koneksi jaringan VirtualBox

Metode	Keterangan
Not attached	Terdapat *network adapter* tetapi tidak terhubung ke jaringan.
NAT (Network Address Translation)	Menyamarkan IP *private* agar dikenali sebagai IP public sehingga bisa terhubung dengan internet.
NAT Network	Sama seperti NAT hanya saja dapat menghubungkan *virtual machine* yang sama-sama menggunakan NAT *Network.*
Bridged Adapter	Dengan metode ini VirtualBox dapat menggunakan *network adapter* fisik secara penuh.
Internal Network	Membuat jaringan virtual yang terisolasi dari luar, yang artinya hanya dapat diakses lewat *virtual machine* yang menggunakan metode jaringan *internal network* dengan nama yang sama.
Host-Only	Sebuah adapter virtual yang dibuat untuk menghungkan komputer fisik dengan *virtual machine.*

2.2.10 IP (*Internet Protocol*) *Addresses*

IP *Addresses* merupakan alamat identifikasi unik yang dimiliki oleh setiap komputer dan perangkat lainnya yang terhubung di dalam jaringan komputer dan memiliki 2 bagian utama yaitu *Net Id* dan *Host Id*. Kata unik yang berarti disini adalah bahwa setiap komputer atau perangkat yang terhubung lainnya tersebut

memiliki alamat yang tidak boleh sama di dalam satu jaringan komputer (Efendi, 2015).

Pada penelitian ini yang digunakan adalah IPv4 (*Internet Protocol version* 4) dimana IP ini memiliki beberapa kelas yaitu kelas A, kelas B, kelas C, kelas D dan kelas E dengan klasifikasi yang dapat dilihat pada Tabel 2.4 Klasifikasi IPv4.

Tabel 2.4 Klasifikasi IPv4

Kelas	Oktet Pertama (Desimal)	Oktet Pertama (Biner)	Penggunaan
A	1-126	0xxx xxxx	Jaringan komputer skala besar
B	128-191	10xx xxxx	Jaringan komputer skala menengah
C	192-223	110x xxxx	Jaringan komputer skala kecil
D	224-239	1110 xxxx	Alamat *multicast*
E	240-255	1111 xxxx	Alamat untuk percobaan atau eksperimen

a) IP *address* Kelas A

IP *address* kelas A adalah IP *address* yang digunakan untuk jaringan komputer berskala besar. IP kelas A ini mampu menyediakan 126 jaringan dengan dengan setiap jaringan bisa memiliki 16777214 *host*.

Alamat IP kelas A banyak digunakan untuk jaringan komputer berskala besar. IP Kelas A memiliki jumlah jaringan 126 dan setiap jaringan mampu untuk menampung 16777214 *host*. *Range* IP *address* kelas A mulai 1.xxx.xxx.xxx sampai 126.xxx.xxx.xxx.

b) IP *Address* Kelas B

Kelas IP *address* yang satu ini diperuntukan bagi jaringan komputer dengan skala menengah sampai bersar, IP Kelas B menyediakan 16384 jaringan dan setiap jaringan menampung hingga 65534 host. Nomor urut pada dua bit pertama dalam oktet pertama selalu diset dengan nilai 10 dalam bilangan biner. Sementara untuk

14 bit berikutnya digunakan untuk melengkapi dua oktet pertama sebagai *network identifier*. Untuk 16 bit berikutnya (dua oktet terakhir) berfungsi sebagai *host identifier*. *Range* IP *address* kelas B mulai dari 128.0.xxx.xxx sampai 191.255.xxx.xxx.

c) IP *Address* Kelas C

Kelas IP *address* yang satu ini biasanya digunakan untuk jaringan komputer skala kecil. IP *address* kelas C menyediakan 2097152 jaringan dan setiap jaringan dapat menampung 254 *host*. Pada tiga bit pertama pada oktet pertama selalu bernilai 110 (dalam bilangan biner) kemudian 21 bit berikutnya (tiga oktet pertama) membentuk *network identifier*. Kemudian untuk 8 bit berikutnya (Oktet terakhir) digunakan untuk *host identifier*. *Range* IP *address* kelas C mulai dari 192.0.0.xxx sampai 255.255.255.xxx.

d) IP *Address* Kelas D

Kelas alamat IP ini digunakan untuk IP *multicast*, empat bit pertama pada oktet pertama bernilai 1110 (bilangan biner) dan sekaligus sebagai *network identifier*. Kemudian 28 bit betikutnya digunakan untuk *host identifier*. *Range* IP kelas D mulai dari 224.0.0.0 sampai 239.255.255.255.

e) IP *Address* Kelas E

IP *address* kelas E digunakan untuk eksperimen. empat bit pertama pada oktet pertama kelas IP *address* ini diset dengan nilai 1111 bilangan biner dan sekaligus sebagai *network identifier* . Kemudian untuk 28 bit berikutnya digunakan untuk *host identifier*. *Range* IP kelas E mulai dari 240.0.0.0 sampai 254.255.255.255.

2.2.11 BSOD (*Blue Screen Of Death)*

BSOD merupakan suatu notifikasi dari sistem operasi khususnya Windows ketika terjadi error pada sistem dan tidak bisa me-*recover*-nya atau memperbaikinya (Efendi, 2014). BSOD ini bisa muncul ketika sistem Windows gagal melewati *critical error* yang terjadi, sehingga proses *reboot system* dibutuhkan dan seringkali mengganggu bahkan menghilangkan data yang sedang

kita kerjakan. BSOD merupakan tipe *error* terburuk yang terjadi pada komputer, karena *error* ini akan mematikan seluruh sistem.

BSOD ini biasanya terjadi karena adanya masalah pada *hardware* ataupun *software driver* dari *hardware*. Untuk *software* biasa selain *driver hardware* biasanya tidak akan menyebabkan BSOD melainkan hanya akan menyebabkan munculnya peringatan pada layar tanpa mengganggu sistem operasinya.

2.2.12 Topologi jaringan

Topologi jaringan adalah suatu metode yang digunakan untuk menghubungkan dua komputer atau lebih, berdasarkan hubungan geometris antara unsur-unsur dasar penyusun jaringan, yaitu node, link, dan station.

Berikut adalah macam-macam topologi jaringan komputer

a. Topologi Bus

Topologi ini adalah topologi yang pertama kali digunakan untuk menghubungkan komputer. dalam topologi ini masing-masing komputer aka terhububng ke satu kabel panjang dengan beberapa terminal, dan pada akhir dari kable harus di akhiri dengan satu terminator.

b. Topologi Star

Topologi star adalah topologi dengan node inti/tengah yang dihubungan dengan node lainnya.

c. Topologi Ring

Pada Topologi cincin, masing-masing titik/node berfungsi sebagai repeater yang akan memperkuat sinyal disepanjang sirkulasinya, artinya masing-masing perangkat saling bekerjasama untuk menerima sinyal dari perangkat sebelumnya kemudian meneruskannya pada perangkat sesudahnya, proses menerima dan meneruskan sinyal data ini dibantu oleh token.

d. Topologi Mesh

Topologi mesh adalah topologi gabungan dari topologi Ring dan Star. Topologi mesh adalah suatu bentuk hubungan antar perangkat dimana setiap perangkat terhubung secara langsung ke perangkat lainnya yang ada di dalam

jaringan. Akibatnya, dalam topologi mesh setiap perangkat dapat berkomunikasi langsung dengan perangkat yang dituju (dedicated links).

e. Topologi Tree

Topologi jaringan komputer Tree merupakan gabungan dari beberapa topologi star yang dihubungan dengan topologi bus, jadi setiap topologi star akan terhubung ke topologi star lainnya menggunakan topologi bus, biasanya dalam topologi ini terdapat beberapa tingkatan jaringan, dan jaringan yang berada pada tingkat yang lebih tinggi dapat mengontrol jaringan yang berada pada tingkat yang lebih rendah.