BAB II
DASAR TEORI

2.1 Kajian Pustaka

Penelitian Yudi Mulyanto pada tahun 2019 yang berjudul *"Analisis Dan Pengembangan Infrastruktur Jaringan Komputer Dalam Mendukung Implementasi Sekolah Digital"* merancang infrastruktur jaringan di SD Negeri 2 Sumbawa karena sebelumnya pada sekolah tersebut infrastruktur jaringannya hanya melayani satu *Local Area Network Saja* (LAN). Dalam mendukung aktifitas digitalisasi di sekolah tersebut membutuhkan infrastruktur jaringan yang lebih reliabel dan fungsional. Dengan infrastruktur jaringan yang reliabel memudahkan aktifitas belajar mengajar, penilaian, dan pengembangan skill. Penelitian ini merancang infrastruktur jaringan menggunakan perangkat mikrotik, *windows server* 2012, dan perangkat jaringan lainnya dengan menggunakan metode *Network Development Life Cycle* (NDLC). Pengujian dalam penelitian ini yaitu tes koneksi dari router ke internet. Hasil dari penelitian ini dalam merancang infrastruktur jaringan Pada saat ping dilakukan oleh router ke gateway yang ada pada modem dengan IP 192.168.1.1 hasilnya adalah waktu pengiriman 0 ms dengan jarak pengiriman antara satu paket dengan paket lainya 64 sedangkan ukuran paket hanya 56 byte. Sementara untuk tes koneksi dengan www.google.com memperoleh IP 172.217.4.196 dengan waktu pengiriman paket 230 ms[2].

Penelitian Taufik Rahman pada tahun 2020 yang berjudul *"Perancangan Jaringan Virtual Local Area Network (VLAN) & DHCP Pada PT NAVICOM Indonesia Bekasi"* merancang jaringan *Virtual Local Area Network* (VLAN) di PT NAVICOM Indonesia untuk meningkatkan keamanan jaringan menggunakan jaringan VLAN karena terdapat permasalahan dimana setiap divisi saling mengakses data pada computer yang ada dan data tidak terpisah dari jaringan. Penelitian ini merancang jaringan VLAN menggunakan aplikasi *cisco packet tracer*. Pengujian pada penelitian ini dilakukan dengan cara tes ping antar komputer. Hasil dari penelitian ini adalah keamanan dari setiap komputer lebih aman menggunakan jaringan VLAN karena pada jaringan VLAN dapat membuat konfigurasi jaringan mana saja yang saling terhubung[3].

Penelitian Kevin Kurniawan pada tahun 2022 yang berjudul *"Analisis Quality of Service (QoS) Pada Routing Protocol Open Shortest Path First (OSPF)"* menganalisa parameter *Quality of Service* (OSPF) pada protokol *Open Shortest Path First* (OSPF) dengan membandingkan performasi antara *routing statis* dengan *routing dinamis.* Penelitian ini dilakukan untuk mengetahuhi protokol *routing* mana yang memiliki kinerja terbaik. Pada penelitian ini menggunakan aplikasi GNS 3 dan aplikasi *wireshark network analyzer.* Pengujian pada penelitian ini dilakukan dengan melakukan 5 kali pengukuran dengan parameter *Quality of Service* (QoS) yaitu throughput, delay, dan jitter serta mengukur waktu konvergensi pada *routing* OSPF. Hasil pengujian yang didapat menunjukkan bahwa routing protocol OSPF lebih baik dengan pengukuran delay saat kondisi normal dan saat terjadi pemutusan jalur juga lebih optimal untuk hasil parameter throughput, delay dan jitter dibandingkan dengan routing statis. Sedangkan hasil pengujian Waktu Konvergensi menunjukkan bahwa routing OSPF memiliki nilai 2,4 ms dan 1,2 dengan menggunakan 5 router dan pada 3 router memiliki nilai 0,45. Dengan demikian semakin kecil jumlah node, maka jaringan OSPF semakin cepat waktu konvergensi yang diperlukan[4].

2.2 Dasar Teori

2.2.1 Jaringan Komputer

Di dunia sekarang ini, teknologi berkembang pesat, begitu pula dengan perkembangan jaringan komputer. Peran teknologi memungkinkan informasi terkirim dan dikomunikasikan lebih cepat tanpa batasan jarak, ruang, dan waktu. Secara umum jaringan komputer merupakan kumpulan komputer-komputer yang saling terhubung di seluruh dunia. Jaringan komputer memungkinkan untuk bertukar data. Jaringan komputer adalah hubungan antara dua komputer atau lebih yang dapat saling berhubungan, dan tujuan utamanya adalah pertukaran data. Keberadaan jaringan komputer memungkinkan terjadinya pertukaran informasi dan berbagi sumber daya. Pengguna dapat berkomunikasi satu sama lain dan mengakses informasi[5]. Prinsip dasar dalam suatu sistem jaringan ini adalah proses pengiriman data atau informasi dari pengirim kepada penerima melalui suatu media komunikasi tertentu. Tujuan dibangunnya suatu jaringan komputer adalah untuk

membawa data-informasi dari pengirim menuju kepada penerima secara cepat dan tepat tanpa adanya gangguan melalui media transmisi atau media komunikasi tertentu[6].

2.2.1.1 Sifat Jaringan Komputer

1) *Scalability*

   Jaringan komputer dapat disesuaikan dengan kebutuhan, dapat berkembang, menghilangkan batasan geografis/fisik.

2) *Resource sharing*

   Pemakaian bersama (berbagi) *resource* (sumber daya) *software hardware*.

3) *Connectivity*

   Mudah terhubung dan dihubungkan. Dalam sekumpulan *node*, *link*, *graph*. Memanfaatkan device : router, *switch*, hub, *wired*, *wireless*.

4) *Reliability*

   Jaringan komputer dapat diukur performansinya, keandalan suatu jaringan.

2.2.1.2 Pembagian Jaringan Komputer

a. Berdasarkan distribusi sumber informasi/data:
   1. Jaringan Terpusat
   2. Jaringan Terdistribusi
b. Berdasarkan jangkauan geografis:
   1. *Local Area Network* (LAN)
   2. *Metropolitan Area Network* (MAN)
   3. *Wide Area Network* (WAN)
c. Berdasarkan peranan dan hubungan tiap komputer dalam memproses data :
   1. *Peer to peer*
   2. *Client Server*
d. Berdasarkan media transmisi data :
   1. Jaringan berkabel *(wired network*)

2. Jaringan nirkabel (*wireless network*)[7].

2.2.1.3 Jenis – Jenis Jaringan Komputer

Jaringan komputer di bagi menjadi 3 diantaranya :

1) *Local Area Network* (LAN)

   Local Area Network (LAN) adalah jaringan yang terdiri dari beberapa komputer yang saling terhubung dalam area yang relatif kecil seperti gedung, kampus, atau kantor. LAN biasanya digunakan untuk memfasilitasi komunikasi dan berbagi sumber daya antara karyawan dalam sebuah perusahaan. Komputer dalam LAN terhubung menggunakan kabel seperti *Ethernet* atau Wi-Fi. LAN biasanya digunakan untuk memfasilitasi akses ke internet dan berbagi sumber daya seperti *printer* dan *file*.

2) *Wide Area Network* (WAN)

   Wide Area Network (WAN) adalah jaringan yang terdiri dari beberapa LAN yang terhubung bersama dalam area yang lebih luas, seperti kota atau negara. WAN menggunakan koneksi jarak jauh seperti *leased line* atau jaringan nirkabel untuk menghubungkan LAN yang berbeda. WAN biasanya digunakan untuk memfasilitasi komunikasi antara karyawan di lokasi yang berbeda, seperti cabang perusahaan yang berbeda di berbagai kota atau negara.

3) *Metropolitan Area Network* (MAN)

   Metropolitan Area Network (MAN) adalah jaringan yang lebih besar dari LAN tetapi lebih kecil dari WAN. MAN terdiri dari beberapa LAN yang terhubung bersama dalam area yang lebih besar seperti kota atau wilayah. MAN biasanya digunakan untuk memfasilitasi komunikasi dan berbagi sumber daya antara karyawan di beberapa lokasi dalam area yang lebih luas seperti kota atau wilayah[8].

2.2.1.4 Perangkat yang umum digunakan jaringan komputer

Perangkat jaringan komputer yang secara umum digunakan adalah sebagai berikut :

a. *Network Interface Card* (NIC)

   Network Interface Card sering disebut juga dengan kartu jaringan, kartu dengan rangkaian elektronik tertentu yang digunakan untuk menghubungan komputer ke jaringan.

b. Kabel Jaringan

   Kabel jaringan yang digunakan oleh jaringan terdiri dari tiga jenis, diantaranya adalah kabel UTP, kabel *coaxial* dan kabel *fiber optic*.

c. Hub

   Hub merupakan suatu perangkat yang digunakan untuk menghubungkan antar komputer dalam pertukaran data. Hub ini juga dapat dikatakan sebagai *central node* yang mana merupakan perangkat yang sangat penting. Sebab aliran data akan melewati perangkat ini sebelum data tersebut sampai pada tujuannya.

d. Switch

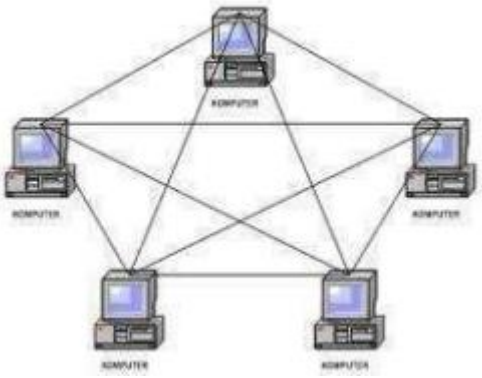
   Switch ini merupakan perangkat yang model serta fungsinya hampir mirip dengan hub yaitu sebagai jembatan dalam suatu jaringan. *Switch* ini dapat membaca alamat MAC address serta dapat mengalihkan jalur jaringan. Secara umum jumlah *port* pada *switch* lebih banyak dibandingkan dengan perangkat hub[9].

2.2.1.5 Topologi Jaringan Komputer

Topologi jaringan merupakan berbagai *node*, perangkat, dan koneksi jaringan yang saling berkaitan antara satu dengan yang lainnya secara logis dan teratur. Dimana untuk menghubungkan berbagai jenis *node*, perangkat, dan koneksi jaringan ini bisa dengan kabel maupun nirkabel[10]. Topologi jaringan yang umum dipakai adalah sebagai berikut :

a. Topologi Jaringan *Mesh*

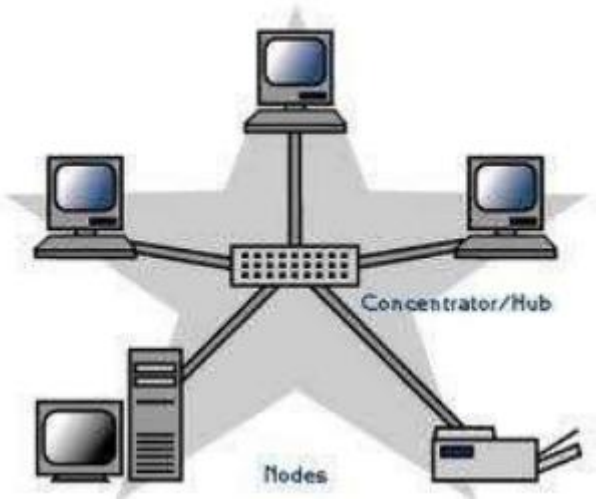
   Topologi ini menerapkan hubungan antar sentral secara penuh. Tingkat kerumitan jaringan sebanding dengan meningkatnya jumlah sentral yang terpasang. Selain kurang ekonomis, dalam pengoperasiannya toplogi mesh juga relatif mahal.



Gambar 2. 1 Topologi jaringan *mesh*

b. Topologi Jaringan *Star*

Dalam topologi ini, salah satu *device* dibuat sebagai sentral pusat. Jika dibandingkan dengan sistem *mesh*, sistem ini mempunyai tingkat kerumitan sehingga sistem menjadi lebih ekonomis, tetapi beban yang dipikul sentral pusat cukup berat. Dengan demikian kemungkinan tingkat kerusakan dan gangguan lebih besar.

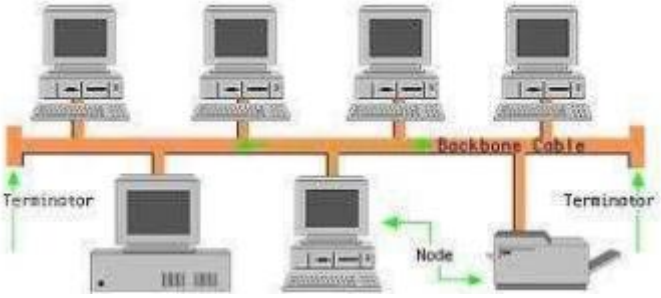


Gambar 2. 2 Topologi jaringan *star*

c. Topologi Jaringan *Bus*

Pada topologi ini semua alat dihubungkan secara langsung pada media transmisi dengan konfigurasi yang disebut *bus*. Transmisi sinyal dari suatu alat tidak dikirim secara bersamaan dalam dua arah. Hal ini berbeda dengan yang ada pada topologi jaringan *mesh* atau *star*, yang pada kedua sistem tersebut dapat dilakukan komunikasi antar alat secara

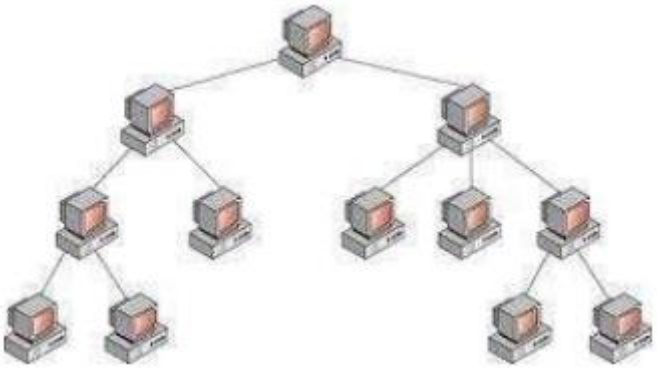
bersamaan. Topologi jaringan *bus* tidak umum digunakan untuk interkoneksi antar alat, tetapi biasanya digunakan pada sistem jaringan komputer.



Gambar 2. 3 Topologi jaringan *bus*

d. Topologi Jaringan *Tree*

Disebut juga sebagai topologi jaringan bertingkat. Topologi ini biasanya digunakan untuk interkoneksi antar alat dengan hirarki yang berbeda. Untuk hirarki yang lebih rendah digambarkan pada lokasi yang rendah dan semakin ke atas mempunyai hirarki semakin tinggi. Topologi jaringan jenis ini cocok digunakan paada sistem jaringan komputer.

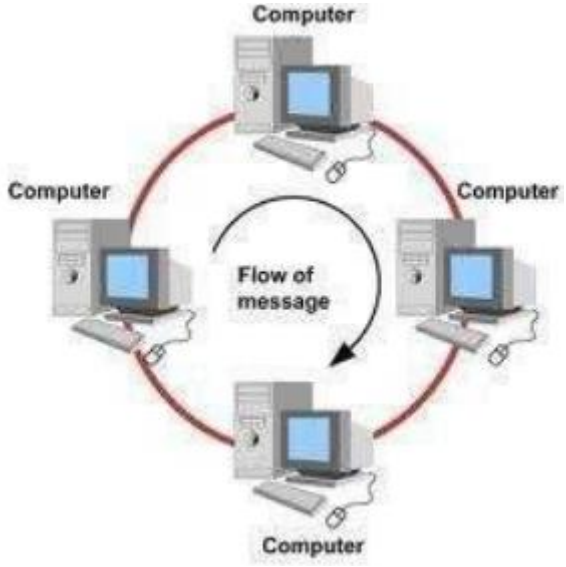


Gambar 2. 4 Topologi Jaringan *tree*

e. Topologi Jaringan *Ring*

Untuk membentuk jaringan ini, setiap alat harus dihubungkan seri satu dengan yang lain dan hubungan ini membentuk *loop* tertutup. Dalam sistem ini setiap alat dirancang agar dapat berinteraksi dengan alat yang berdekatan maupun berjauhan. Dengan demikian kemampuan melakukan *switching* ke berbagai arah. Keuntungan dari topologi ini antara lain adalah tingkat kerumitan jaringan rendah (sederhana), juga

bila ada gangguan atau kerusakan pada suatu alat maka aliran data dapat dilewatkan pada arah lain dalam sistem[11].



Gambar 2. 5 Topologi jaringan *ring*

2.2.2 OSI (*Open Ssystem Interconnection*) *Layer*

OSI (*Open System Interconnection*) dibuat oleh ISO (*International Standart Organization*) dengan tujuan membuat suatu standarisasi protokol, yang bekerja sesuai dengan protokol tersebut. OSI adalah untuk menjelaskan cara agar informasi dari satu aplikasi di komputer dapat bergerak melalui jaringan ke aplikasi di komputer lain, memiliki proses panjang melalui lapisan-lapisan jaringan computer. 7 model OSI layer :

1. *Physical Layer*

   Physical layer bekerja dengan dengan mendefinisikan media transmisi jaringan, metode pensinyalan, sinkronisasi bit, arsitektur jaringan, dan pengkabelan.

2. *Data Link Layer*

   Data Link Layer berfungsi untuk menentukan bit-bit data yang kemudian di kelompokkan menjadi *frame*. *Layer* ini juga berfungsi dalam koreksi kesalahan, *flow control*, pengalamatan perangkat keras dan menentukan bagaimana perangkat-perangkat jaringan saling beroperasi.

3. *Network Layer*

Network Layer berkerja setelah *data link layer*.pada *layer* ini *frame* akan di teruskan ke *network layer* kemudian *network layer* akan membuat *header* paket-paket yang berisi IP, baik IP pengirim maupun penerima data.

4. *Transport Layer*

   Layer ini akan melakukan pemecahan data ke dalam paket-paket data serta memberikan nomor urut pada paket-paket yang dipecah tersebut sehingga dapat disusun kembali ketika sudah sampai di sisi penerima data.

5. *Session Layer*

   Layer ini akan mendefenisikan bagaimana koneksi dapat dibuat, dipelihara atau dihancurkan.

6. *Presentation Layer*

   Presentation Layer merupakan lapisan keenam yang bekerja dengan mentranslasikan format data yang hendak di transmisikan oleh aplikasi melalui jaringan ke dalam format yang ditransmisikan melalui jaringan.

7. *Application Layer*

   Merupakan *layer* antarmuka dengan *end user* dengan aplikasi yang bekerja menggunakan fungsionalitas jaringan, melakukan pengaturan bagaimana aplikasi bekerja dan memberikan pesan kesalahan apabila terjadi kesalahan[12].

2.2.3 VLAN (*Virtual Local Area Network*)

Keterbatasan LAN melahirkan sebuah teknologi VLAN yang memungkinkan adanya konfigurasi dari suatu jaringan komputer secara *virtual* (virtualisasi). *Virtual Local Area Network* (VLAN) merupakan sebuah metode yang sering digunakan untuk mendistribusikan beberapa *segment* jaringan yang berbeda pada perangkat *router* dengan *interface ethernet* fisik yang terbatas. Dengan adanya VLAN ini dapat membuat sangat banyak segment LAN dalam sebuah *interface*. Hal ini mengakibatkan suatu *network* dapat dikonfigurasi secara *virtual* tanpa harus menuruti lokasi fisik peralatan. Penggunaan VLAN akan membuat pengaturan jaringan menjadi sangat fleksibel dimana dapat dibuat segmen yang bergantung pada organisasi atau departemen tanpa bergantung pada lokasi *workstation*. Kelebihan dari model jaringan dengan VLAN adalah bahwa tiap-tiap *workstation/*

user yang tergabung dalam satu VLAN dapat tetap saling berhubungan walaupun terpisah secara fisik.

VLAN bisa membatasi pengguna yang bisa mengakses suatu data, sehingga mengurangi kemungkinan terjadinya penyalahgunaan hak akses. Rancang bangun VLAN dapat dilakukan dengan memanfaatkan simulasi jaringan dengan *Cisco Packet Tracer*. *Software* ini berfungsi untuk membuat model suatu jaringan komputer dan mensimulasikan suatu jaringan. *Virtual* LAN terbangun karena adanya konsep *subneting* dan LAN (*Local Area Network*). *Virtual* LAN dapat disebut juga sebagai pengembangan dari LAN. Jaringan LAN merupakan jaringan yang berada pada satu *broadcast domain*. *Switch* akan memperlakukan semua *interface* pada *switch* tersebut berada pada *broadcast domain* yang sama, oleh karena itu semua piranti yang terhubung ke *switch* berada dalam satu jaringan LAN. Penerapan manajemen jaringan LAN dapat diterapkan dengan menggunakan VLAN untuk manajemen jaringan, dan segmentasi jaringan. Manajemen segmentasi jaringan menggunakan VLAN diterapkan dengan membuat pengelompokan jaringan menjadi beberapa kelompok jaringan *virtual* dan pengalamatan secara *logic* dengan *subnetting* untuk pembatasan *host* pada suatu jaringan dan memanfaatkan *Managable Switch* yang menjadi komponen utama jaringan LAN[13].

2.2.3.1 Mekanisme VLAN

Sub-jaringan, atau *subnet* adalah pembagian secara yang terlihat secara fisik dari IP jaringan. Praktik membagi jaringan menjadi dua atau lebih jaringan disebut *Subnetting*. Semua komputer yang termasuk dalam sebuah *subnet* di alamatkan dengan *bit-group* umum, identik, dan paling signifikan dalam alamat IP *Address* mereka. Hal ini menyebabkan pembagian logis dari alamat IP ke dua bidang, jaringan atau *routing prefix* dan sisa *field* atau pengenal *host*. *Field* sisanya adalah pengidentifikasi untuk *host* tertentu atau antarmuka jaringan. Ada 3 metode yang digunakan untuk menerapkan VLAN yaitu :

1. *Port Based*

Vlan dibagi berdasarkan *port*, metode konfigurasi yang paling banyak digunakan, sering diimplementasikan dimana DHCP digunakan untuk memberikan alamat IP ke *host*.

2. MAC *Based*

   Vlan dibagi berdasarkan MAC *address*, setiap alamat harus dimasukkan kedalam *switch* dan dikonfigurasi secara individual.

3. *Protocol Based*

   Vlan dibagi berdasarkan *protocol layer* 3 atau IP, dikonfigurasi seperti MAC *address* tapi menggunakan alamat IP[14].

2.2.4 IP *Address*

Setiap perangkat komputer yang terhubung di dalam jaringan, pasti memiliki ID tersendiri dalam jaringan tersebut, yaitu yang dinamakan dengan IP (*Internet Protokol*). IP terdiri dari deretan bilangan biner antara 32 bit sampai 128 bit. Panjang dari IP ini adalah 32 bit untuk IP versi 4 dan 128 bit untuk IP versi 6. Angka tersebut akan menunjukan alamat dari komputer atau host dalam sebuah jaringan berbasis TCP/IP[15].

2.2.4.1 IP Publik

IP Publik adalah IP *address* yang bisa diakses di internet. IP publik juga dikenal sebagai alamat IP unicast yang dapat dirutekan secara global. Ketika perangkat memiliki IP publik dan terhubung ke internet, perangkat ini juga dapat diakses dari mana saja melalui internet. Namun, tidak dapat menginstall IP publik secara manual. Ada aturan untuk mengatur IP publik. Yaitu dengan meminjam ISP untuk mendapatkan *public* IP *address*.

2.2.4.2 IP *Private*

Dalam skema IP *address*, IP *private* merupakan IP *address* yang digunakan untuk jaringan lokal. IP *private* tidak tersedia di internet dan tidak dapat diakses di internet. Dalam implementasinya, pada jaringan nyata, jaringan area lokal biasanya menggunakan IP *private*, kemudian ditambahkan router untuk menghubungkan jaringan lokal. Saat menetapkan IP address, ada 3 jenis IP:

- *Host address*, IP *address* dapat ditambahkan ke perangkat jaringan seperti komputer atau router agar mereka dapat terhubung satu sama lain. *Host* IP *server* unik, karena alamat IP *server* yang tidak dapat ditemukan di jaringan.
- *Network address*, IP *address* mewakili alamat jaringan. Semua *server* di jaringan memiliki alamat jaringan yang sama. *Network address* adalah IP pertama dalam subnet IP.
- *Broadcast address*, jenis IP *address* yang digunakan untuk mengirim data ke semua *host* yang masih berada dalam jaringan yang sama. *Broadcast address* adalah IP terakhir dalam subnet IP[16].

2.2.5 OSPF (*Open Shortest Path First*)

Open Shortest Path First (OSPF) adalah *protocol routing link state* dan digunakan untuk menghubungkan router-router yang berada dalam satu *Autonomus System* (AS), sehingga *protocol routing* ini termasuk juga dalam kategori *Interior Gateway Protocol* (IGP). Sehingga OSPF hanya dapat bekerja dalam jaringan internal suatu organisasi atau perusahaan. Pada jaringan internal, administrator jaringan memiliki hak penuh untuk mengatur dan memodifikasinya. Selain itu OSPF merupakan protokol perutean yang menggunakan konsep perutean hierarkis, artinya OSPF membagi-bagi jaringan menjadi beberapa tingkatan. Tingkatan-tingkatan ini diwujudkan dengan menggunakan sistem pengelompokan area. Dengan menggunakan konsep perutean hierarki ini sistem penyebaran informasi dalam protokol OSPF menjadi lebih teratur dan tersegmentasi, sehinggga tidak menyebar secara sembarangan. Efek dari keteraturan penyebaran perutean ini adalah penggunaan *bandwith* jaringan menjadi lebih efisien, lebih cepat mencapai konvergensi, dan lebih akurat dalam menentukan rute-rute terbaik menuju ke sebuah lokasi.

Untuk dapat menangani jaringan yang berskala besar, maka OSPF menerapkan konsep area dalam implementasinya, yaitu *single area* untuk jaringan berskala kecil dan *multi area* untuk jaringan berskala besar. Router yang menjalankan OSPF hanya akan bertukar informasi *route* (*routing update*) dengan router OSPF lainnya yang berada dalam satu *autonomus system* (AS). Router OSPF

akan mengirimkan beberapa paket OSPF lainnya yang kesemuanya digunakan membentuk *table routing*. Pada OSPF dikenal kondisi *adjency* antar router. Sebelum router-router tersebut bertukar informasi *routing*, maka sebuah router harus terlebih dahulu mencapai kondisi *adjency* (bertetangga dan bersepakat) dengan router tetangganya. Router-router tidak akan bertukar *routing* update jika kondisi *adjency* belum tercapai. OSPF mengumpulkan informasi *link state* dari *router* yang ada dan membangun sebuah grafik topologi dari jaringan. Rute paket, OSPF menghitung *shortest path tree* untuk setiap rute menggunakan metode yang didasarkan pada algoritma *dijkstra*. Untuk menentukan jalur terpendek, OSPF membutuhkan pemberian bobot setiap link di jaringan. Link bobot didistribusikan sebagai *link state*[17].

2.2.5 Protokol Transmisi

Dalam jaringan internet terdapat dua jenis protokol yang umum digunakan yaitu *Transmission Control Protocol* (TCP) dan *User Datagram Protocol* (UDP) dimana penggunaannya dapat disesuaikan dengan kebutuhan setiap pengguna apakah lebih mementingkan kecepatan transfer data atau keakuratan data. TCP dan UDP merupakan protokol pada *Layer Transport*. Pada saat transfer data melalui jaringan jika dilihat dari *Open Systems Interconnection* (OSI) *layer*, *layer* yang berfungsi untuk menangani proses transfer data yaitu *Layer Transport*. Pada *layer transport* terdapat dua protokol utama yang paling sering digunakan yaitu TCP dan UDP. TCP memiliki kemampuan untuk memastikan setiap data yang dikirimkan akan sampai secara utuh ke penerima, sehingga tidak perlu khawatir data yang dikirimkan tidak sampai ke penerima secara utuh. Sedangkan UDP memilki kemampuan dalam kecepatan pengiriman data dan lebih unggul dari TCP dalam hal kecepatan[18].

2.2.6 QoS (*Quality Of Service*)

Quality Of Service (QOS) merupakan suatu metode dalam melakukan pengukuran seberapa baik layanan jaringan. Dengan QoS administrator jaringan dapat mengetahui dan menangani permasalahan-permasalahan yang terjadi pada lalu lintas aliran paket dalam jaringan, seperti dapat memberikan prioritas trafik

tertentu pada jaringan suatu metode yang dapat digunakan dalam pengukuran seberapa baik sebuah layanan jaringan. QOS dapat digunakan untuk mengukur sebuat atribut performa yang sudah dispesifikan dan diasosiasikan dengan suatu *service*. Parameter QOS menurut standar TIPHON sebagai berikut :

a. *Throughput*

Throughput hampir sama dengan *bandwidth*, hanya saja *throughput* bersifat dinamis dan bisa berubah-ubah tergantung trafik yang sedang terjadi sedangkan *bandwidth* bersifat permanen. Rumus untuk pengukuran throughput adalah sebagai berikut :

$$Throughput = \frac{Jumlah\ data\ yang\ dikirim}{Waktu\ pengiriman\ data}$$

Tabel 2.1 Standar *Throughput* menurut TIPHON[4]

Kategori	*Throughput*	Indeks
Sangat Bagus	>2,1 Mbps	4
Bagus	1200 kbps – 2,1 Mbps	3
Sedang	700 – 1200 kbps	2
Buruk	338 – 700 kbps	1
Sangat Buruk	0 – 338 kbps	0

b. *Delay*

Delay merupakan waktu yang dibutuhkan data untuk menempuh jarak dari asal ke tujuan. *Delay* dapat dipengaruhi oleh jarak, media fisik, kongesti atau juga waktu proses yang lama. Rumus untuk pengukuran *delay* adalah sebagai berikut :

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

Tabel 2.2 Standar *delay* menurut TIPHON[4]

Kategori	*Delay*	Indeks
Sangat Bagus	<150 ms	4
Bagus	150 – 300 ms	3
Sedang	300 – 450 ms	2

Tabel 2.3 Standar *delay* menurut TIPHON[4]

Buruk	>450 ms	1

c. *Jitter*

Jitter dapat diartikan sebagai gangguan pada komunikasi digital maupun analog yang disebabkan oleh perubahan sinyal karena referensi posisi waktu. *Jitter* dapat mengakibatkan hilangnya data, terutama pada pengiriman data dengan kecepatan tinggi. Variasi *jitter* biasanya berkaitan erat dengan *delay*, *delay* menunjukkan variasi yang cukup besar dalam transmisi data pada jaringan. Rumus untuk pengukuran *jitter* adalah sebagai berikut :

$$Jitter = \frac{Total\ variasi\ delay}{Total\ paket\ yang\ diterima}$$

Tabel 2.4 Standar *jitter* menurut TIPHON[4]

Kategori	*Jitter*	Indeks
Sangat Bagus	0 ms	4
Bagus	0 – 75 ms	3
Sedang	75 – 125 ms	2
Buruk	125 – 225 ms	1

d. *Packet loss*

Packet loss adalah parameter untuk menggambarkan sebuah kondisi dimana jumlah total paket hilang. Sejumlah paket yang hilang tersebut didapatkan ketika terjadinnya suatu tabrakan antar paket. Rumus untuk pengukuran *packet loss* adalah sebagai berikut :[4].

$$Packet\ Loss = \frac{(Paket\ yang\ dikirim - paket\ yang\ diterima)}{Paket\ yang\ dikirim} x100\%$$

Tabel 2.5 Standar *packet loss* menurut TIPHON[4]

Kategori	*Packet Loss*	Indeks
Sangat Bagus	0 – 2%	4
Bagus	3 – 14%	3

Tabel 2.6 Standar *packet loss* menurut TIPHON[4]

Sedang	12 – 24%	2
Jelek	25%	1

2.2.7 GNS3

Graphical Network Simulator 3 (GNS3) merupakan sebuah simulator yang dapat melakukan simulasi jaringan yang komplek. Simulator ini dapat mensimulasikan suatu rancangan jaringan sebelum di implementasikan pada kondisi *real* di lapangan, simulasi menggunakan GNS3 bekerja tanpa harus memiliki perangkat jaringan seperti *router* dan switch. GNS3 dapat digunakan untuk berbagai simulasi diantaranya untuk simulasi IPsec-VPN *Tunneling* dan menganalisa berbagai macam tipe serangan pada jaringan[19].

2.2.8 *Wireshark*

Wireshark merupakan *tools* yang bertujuan untuk menganalisa paket data yang ada pada jaringan internet. *Wireshark* juga termasuk *Network Packet Analyzer* yang fungsinya untuk menangkap semua data informasi yang ada saat komunikasi data di jaringan internet dan menampilkan informasi data tersebut sedetail mungkin. *Wireshark* juga *tools* yang fleksibel dalam artian *Wireshark* bisa memeriksa data baik itu yang terjadi pada jaringan internet kabel maupun *wireless. Wireshark* adalah *tools open source* terkemuka yang banyak di gunakan untuk melakukan analisis dan pemecah masalah jaringan, Memungkinkan untuk mengetahui masalah di jaringan. Dengan segala kemampuan yang dimilikinya, *wireshark* digunakan oleh *network professional* untuk keperluan analisis, *troubleshooting*, *pengembangan software* dan protokol, serta digunakan juga untuk tujuan edukasi
Cara kerja *wireshark* adalah sebagai berikut:

1. *Wireshark* memulai dengan merekam data yang dikirim melalui jaringan, baik itu dalam bentuk paket jaringan atau *frame ethernet*.
2. *Wireshark* kemudian menganalisis data yang telah direkam dan menampilkan informasi tentang setiap paket yang dikirim melalui jaringan, termasuk protokol yang digunakan, alamat sumber dan tujuan, isi paket, dan banyak lagi.

3. Setelah itu, pengguna dapat mengambil tindakan yang sesuai berdasarkan informasi yang ditampilkan oleh *wireshark*, seperti memecahkan masalah jaringan, mengoptimalkan kinerja jaringan, atau mengidentifikasi masalah keamanan.

Manfaat *Wireshark* adalah sebagai berikut:

1. Memecahkan masalah jaringan: *wireshark* dapat membantu administrator jaringan untuk memecahkan masalah jaringan dengan melihat lalu lintas jaringan dan menentukan apakah ada masalah dengan jaringan, seperti paket yang hilang atau lalu lintas yang lambat.
2. Menganalisis keamanan: *wireshark* dapat digunakan untuk menangkap dan menganalisis lalu lintas jaringan untuk mencari tahu apakah ada serangan atau aktivitas jahat yang terjadi pada jaringan.
3. Memantau kinerja jaringan: *wireshark* dapat membantu administrator jaringan untuk memantau kinerja jaringan dan mengidentifikasi titik-titik yang menyebabkan kinerja lambat atau masalah lainnya[20].