

BAB II

DASAR TEORI

2.1 KAJIAN PUSTAKA

Pada studi yang dilakukan oleh peneliti [1], dilakukan uji kuat sinyal dengan menggunakan beberapa jenis bahan penghalang seperti Triplek, Kotak Beton, dan Kotak Kramik. Hasil analisis menunjukkan bahwa adanya penghalang menyebabkan pengurangan kekuatan sinyal WiFi. Selain itu, semakin jauh jarak antara pengirim (*transmitter*) dan penerima (*receiver*), sinyal akan mengalami penurunan kekuatan (melemah). Hal ini menandakan bahwa jarak merupakan faktor penting yang mempengaruhi kualitas sinyal WiFi yang dihasilkan. Penelitian ini memberikan pemahaman lebih lanjut tentang bagaimana bahan-bahan penghalang berperan dalam memengaruhi kekuatan sinyal WiFi dan bagaimana jarak memainkan peran penting dalam menentukan kualitas sinyal.

Penelitian [5] fokusnya adalah "Analisis *Quality of Service* (QoS) Jaringan *Wireless* 2,4 GHz dan 5 GHz di Dalam Ruangan dengan Hambatan Kaca". Penelitian ini menggunakan metode QoS (*Quality of Service*) dengan mengukur beberapa parameter, termasuk *Throughput*, *Delay*, *Jitter*, dan *Packet loss*. Pengujian dilakukan dalam dua kondisi, yaitu dengan menggunakan hambatan kaca dan tanpa hambatan. Hasil penelitian menunjukkan bahwa parameter *Jitter* mengalami interferensi yang disebabkan oleh hambatan kaca, sementara parameter lainnya seperti *Throughput*, *Delay*, dan *Packet loss* tidak terpengaruh oleh hambatan tersebut. Selain itu, penelitian ini menemukan bahwa pada frekuensi 5 GHz, *Throughput* memiliki nilai yang lebih besar dibandingkan dengan frekuensi 2,4 GHz. Dengan demikian, penelitian ini membuktikan bahwa frekuensi 5 GHz lebih unggul dalam menghasilkan kecepatan rata-rata transfer data dalam satuan bit per detik. Dengan temuan-temuan ini, penelitian [5] memberikan kontribusi penting dalam memahami kualitas layanan jaringan *Wireless* di dalam ruangan, terutama dalam mengatasi hambatan seperti kaca, serta memberikan informasi tentang keunggulan frekuensi 5 GHz dalam hal *Throughput* atau kecepatan transfer data.

Penelitian [6] membahas Analisis *Quality Signal* WiFi (QSW) pada jaringan *Hotspot* RT/RW berdasarkan jenis halangan dan lokasi. Penelitian ini mengukur *Signal to Noise Ratio* (SNR) untuk mengevaluasi kecepatan internet yang dihasilkan oleh WiFi berdasarkan jarak dan jenis halangan. Dalam pengujian, beberapa jenis halangan yang digunakan termasuk kayu, bahan sintetis, kaca, air, batu bata, marmer, keramik, kertas, beton, dan logam. Jarak pengukuran dalam penelitian ini varian, mulai dari 10 meter hingga 100 meter. Parameter penelitian [6] juga mencakup pengukuran *Level Signal* dan *Level Noise*. Dari hasil pengamatan, ditarik kesimpulan bahwa *Level Signal* pada jaringan WiFi yang diamati memiliki nilai yang memadai, artinya sinyal cukup kuat. Selain itu, *Level Noise* pada jaringan WiFi yang diamati juga memiliki nilai yang baik, yang berarti bahwa gangguan sinyal yang tidak diinginkan tidak mempengaruhi sinyal yang sedang diteliti. Penelitian ini memberikan wawasan tentang kualitas sinyal WiFi pada jaringan *Hotspot* RT/RW dengan mempertimbangkan berbagai jenis halangan dan lokasi, serta menunjukkan bahwa sinyal WiFi memiliki performa yang cukup baik dalam mengatasi gangguan dan memberikan kecepatan internet yang memadai.

2.2 DASAR TEORI

2.2.1 Jaringan Komputer

Jaringan komputer merupakan suatu sistem telekomunikasi yang memungkinkan komputer saling berinteraksi dan bertukar data. Jaringan komputer dibangun dengan menggabungkan perangkat keras dan perangkat lunak. Di dalamnya terdapat peran khusus, yaitu *client* yang menerima atau meminta layanan, dan *server* yang memberi atau mengirim data. Jaringan komputer berfungsi secara aktif ketika dua komputer atau lebih saling berkomunikasi atau bertukar data di dalamnya.[7]

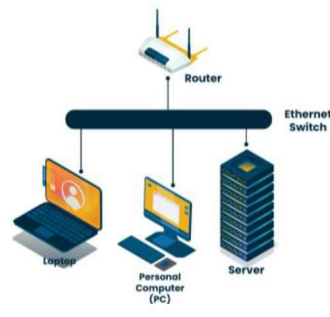
Setiap komputer yang saling terhubung harus memiliki setidaknya satu *network card*, yang dapat dihubungkan secara nirkabel atau melalui kabel sebagai sarana transmisi data. Selain itu, terdapat perangkat lunak untuk sistem operasi jaringan sehingga membuat jaringan komputer secara langsung. Peralatan

pendukung tambahan, seperti *Hub*, *Switch*, *router*, dan sebagainya diperlukan untuk membuat jaringan komputer yang lebih luas. [7]

Ada beberapa jenis jaringan komputer yang sering kita lihat, yaitu:

A. *Local Area Network* (LAN)

LAN merupakan jenis jaringan komputer yang mencakup area kecil, seperti jaringan kampus, kantor, sekolah, rumah, atau jaringan dengan skala yang lebih terbatas. Saat ini, *switch* digunakan sebagai perangkat yang memungkinkan *transfer* data dengan kecepatan 10, 100, atau 1000 Mbit/s. Selain teknologi *ethernet*, jaringan LAN juga sering menggunakan teknologi 802.11b (WiFi). Dalam konteks ini, *hotspot* adalah salah satu contoh teknologi yang menyediakan koneksi LAN melalui WiFi. Perbedaan mendasar dengan konsep terminal dump adalah bahwa setiap *node* atau komputer dalam jaringan LAN memiliki daya komputasi sendiri. Selain itu, tergantung pada hak akses yang telah ditentukan, setiap komputer di LAN juga dapat mengakses sumber daya lainnya di dalam jaringan. Sumber daya tersebut bisa berupa data atau perangkat, seperti *printer*. Pengguna LAN memiliki akses ke aplikasi yang sesuai, yang memungkinkan mereka berkomunikasi dengan pengguna lain di dalam jaringan.[8]. Topologi *Local Area Network* (LAN) dapat dilihat pada Gambar 2.1.



Gambar 2.1 *Local Area Network* (LAN) [9]

B. *Metropolitan Area Network* (MAN)

MAN (*Metropolitan Area Network*) umumnya beroperasi dalam satu negara dan mencakup area yang lebih luas daripada LAN. Jaringan komputer ini menghubungkan beberapa jaringan area lokal bersama untuk membentuk lingkungan yang lebih besar. Contoh penggunaan MAN dapat ditemukan dalam jaringan bank, seperti sistem perbankan *online*. Setiap bank memiliki pusat administrasi dan kantor cabang, dan di setiap kantor tersebut terdapat jaringan

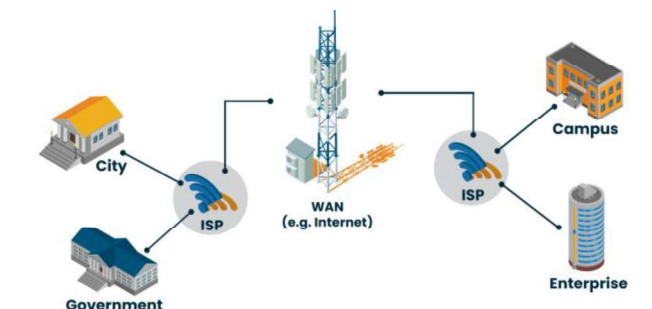
LAN. Melalui penggabungan jaringan LAN di setiap kantor, sebuah MAN terbentuk. MAN mampu mendukung transfer data teks dan suara, dan bahkan dapat terhubung dengan jaringan televisi kabel atau gelombang radio. Jaringan ini dirancang untuk menghubungkan wilayah geografis yang lebih luas dalam satu area metropolitan [8]. Topologi *Metropolitan Area Network* (MAN) dapat dilihat pada Gambar 2.2.



Gambar 2.2 Metropolitan Area Network (MAN) [9]

C. *Wide Area Network* (WAN)

WAN merupakan jenis jaringan komputer yang mencakup wilayah lebih luas dibandingkan jaringan MAN [10]. WAN merupakan kumpulan dari LAN atau *workgroup* yang dihubungkan melalui perangkat komunikasi seperti *modem* dan jaringan internet. Jangkauan wilayah WAN mencakup kantor pusat dan kantor cabang, serta dapat menghubungkan antar kantor cabang. Dengan menggunakan sistem jaringan WAN, pertukaran data antar kantor dapat dilakukan dengan cepat dan relatif hemat biaya. Jaringan WAN memungkinkan koneksi antara kantor pusat dan kantor cabang melalui berbagai sarana, termasuk penggunaan *notebook* dan komputer di kota atau negara lain yang terhubung melalui internet [8]. Topologi *Wide Area Network* (WAN) dapat dilihat seperti pada Gambar 2.3.



Gambar 2.3 Wide Area Network (WAN) [9]

D. Internet

Internet adalah istilah yang mengacu pada jaringan interkoneksi yang menghubungkan berbagai jenis komputer melalui berbagai saluran telekomunikasi seperti telepon, tautan radio, satelit, dan lainnya. Jaringan ini membentuk suatu sistem global yang menghubungkan komputer di seluruh dunia, sehingga disebut sebagai jaringan komputer global. Asal kata "INTERNET" berasal dari kata "*inter*" dalam bahasa Latin, yang berarti "antar" atau "antara". Miliaran komputer dari seluruh dunia terhubung bersama-sama untuk membentuk internet melalui jaringan komputer yang saling terkoneksi. Internet menggunakan kemajuan media komunikasi, seperti telepon dan satelit, serta protokol standar komunikasi untuk menghubungkan berbagai jenis komputer dan jaringan dengan sistem operasi dan aplikasi yang berbeda di seluruh dunia.[11]

2.2.2 Media Penghantar

Berdasarkan media penghantar jaringan komputer dibagi menjadi 2, yaitu:

A. *Wired Network*

Jaringan milik pribadi yang mencakup area beberapa kilometer di dalam gedung disebut *Wired Network*. Jenis jaringan ini digunakan untuk memfasilitasi penggunaan bersama sumber daya seperti *printer* dan *scanner*, serta bertukar informasi antar komputer. LAN (*Local Area Network*) merupakan salah satu contoh jaringan yang menggunakan *Wired Network* sebagai media penghubung untuk menghubungkan komputer pribadi dan *workstation* di dalam kantor atau pabrik perusahaan. [12]

B. *Wireless Network*

Perbedaan utama antara jaringan *Wireless* dan jaringan kabel terletak pada cara mereka menghubungkan perangkat. Jaringan *Wireless* tidak menggunakan kabel atau tautan fisik untuk menghubungkan perangkat yang terhubung satu sama lain.

Ini yang membuat jaringan *Wireless* sangat berbeda dengan jaringan kabel. Sebagai gantinya, jaringan *Wireless* menggunakan udara sebagai media transmisi, di mana informasi dikirimkan melalui gelombang radio atau elektromagnetik. [13]

2.2.3 Tipe Jaringan

Dalam mengatur sebuah jaringan komputer terdapat 2 tipe jaringan sendiri, yaitu:

A. *Peer to Peer*

Jaringan *Peer to Peer* adalah tipe jaringan *workgroup*, di mana setiap PC dapat berfungsi sebagai *client* dan *server* secara bersamaan [14]. Dalam jaringan ini, tidak ada kebutuhan untuk memiliki *server* terpisah karena sumber daya seperti *printer* dan *file* dapat dibagi secara langsung antara dua atau lebih komputer yang terhubung dalam jaringan *peer-to-peer* (P2P). [15]

B. *Client Server*

Dalam model *client-server*, *client* adalah perangkat yang mengajukan permintaan informasi, sementara *server* adalah perangkat yang merespons permintaan tersebut. *Server* berfungsi untuk memproses permintaan data dari *client* dan mengirimkan satu atau lebih data sebagai *respons* kembali ke *client*. [14] [15]

2.2.4 Topologi Jaringan

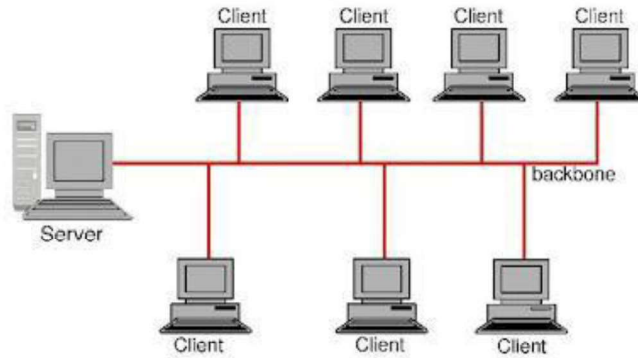
Jaringan Komputer juga memiliki berbagai jenis topologi yang dapat diimplementasikan yaitu Topologi *Bus*, Topologi *Ring*, Topologi *Star*, Topologi *Mesh*, Topologi *Tree*. [16]

A. Topologi *Bus*

Dalam Topologi *Bus*, terdapat satu jalur garis lurus sebagai fitur utama. Ciri khas dari topologi ini adalah bahwa setiap koneksi saling tergantung satu sama lain. Artinya, jika ada koneksi yang hilang atau terputus, maka seluruh koneksi akan terpengaruh, menyebabkan kesulitan dalam mengembalikan koneksi. Meskipun topologi ini menyediakan koneksi yang saling terhubung, namun tidak membentuk jalur yang tertutup. [10]

Topologi *Bus* menghubungkan semua terminal ke satu jalur komunikasi yang ditutup pada kedua ujungnya menggunakan *terminator*. Fungsi *terminator* adalah untuk mencegah sinyal dari keluar kembali dan diterima oleh stasiun jaringan. Selain itu, *terminator* juga berfungsi sebagai perangkat yang memberikan hambatan listrik untuk menyerap sinyal pada ujung transmisi. [16]

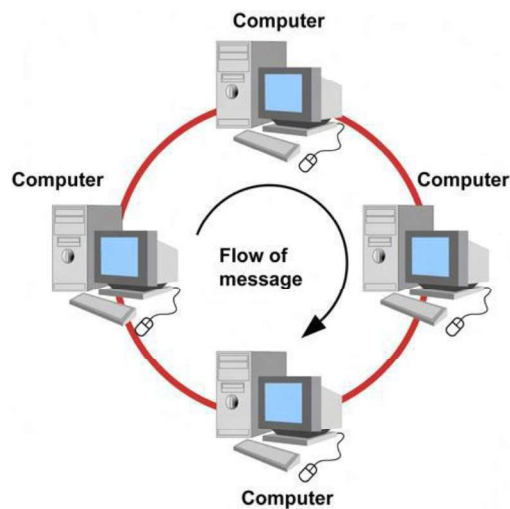
Setiap perangkat harus menggunakan jalur secara bergantian, karena rata-rata kecepatan *transfer* data sangat lambat. Topologi *Bus* diilustrasikan seperti pada Gambar 2.4.



Gambar 2.4 Topologi *Bus* [7]

B. Topologi *Ring*

Topologi *Ring* adalah jenis topologi jaringan di mana setiap titik di sisi kanan dan kiri terhubung ke dua titik lainnya sehingga membentuk suatu lingkaran yang menghubungkan komputer pertama dan terakhir. Pada Topologi *Ring*, titik yang juga disebut *repeater* berfungsi untuk memperkuat sinyal pada setiap rangkaian, memastikan sinyal dan aliran data tetap stabil. Metode ini memungkinkan aliran data bisa bergerak searah jarum jam atau berlawanan arah jarum jam, tergantung pada kebutuhan dan konfigurasi yang digunakan [10]. Topologi *Ring* diilustrasikan seperti pada Gambar 2.5

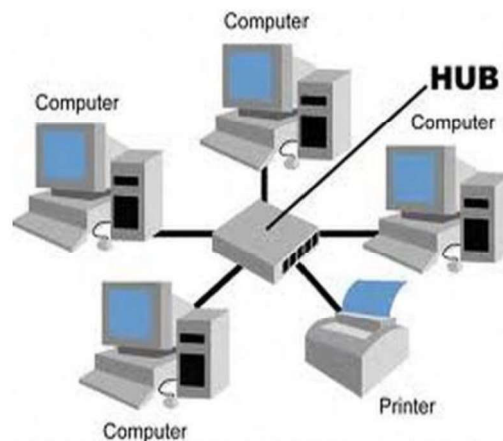


Gambar 2.5 Topologi *Ring* [16]

C. Topologi *Star*

Setiap *node* dalam topologi ini terhubung ke *Hub*, membuatnya tampak seperti bintang. Oleh karena itu, *Hub* selalu terlibat dalam setiap transfer data. *Client* memiliki kabel sendiri untuk langsung terhubung ke komputer *server*, dan media transmisi topologi ini bersifat tertutup. Memastikan bahwa meskipun satu klien gagal, klien lain masih dapat berkomunikasi atau terhubung dengan komputer server. [10]

Cara kerjanya adalah ketika ingin bertukar data, data tersebut akan mengalir terlebih dahulu ke *HUB* atau *Switch* sebelum akhirnya menuju ke komputer yang meminta atau menerima data tersebut [7]. Topologi *Star* diilustrasikan seperti pada Gambar 2.6.



Gambar 2.6 Topologi *Star* [16]

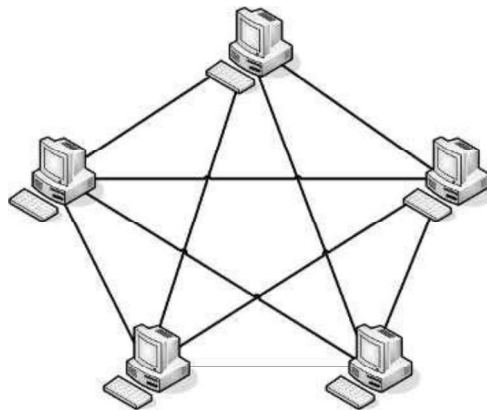
D. Topologi *Mesh*

Topologi *Mesh* adalah jenis topologi jaringan di mana setiap komputer dalam jaringan dapat terhubung satu sama lain kapan saja dan melalui berbagai jalur yang tersedia. Data dapat ditransfer secara langsung dan cepat ke komputer tujuan tanpa perlu melalui komputer lain karena setiap komputer memiliki koneksi langsung dengan komputer tujuan. [7]

Tiap komputer dalam topologi ini memiliki minimal dua jenis koneksi. Pertama, koneksi menghubungkannya ke komputer lain dalam jaringan, dan kedua, koneksi menghubungkannya ke *File Server*.

Namun, karena topologi ini memerlukan pengelolaan koneksi yang rumit dan sulit dikendalikan, sebaiknya topologi ini digunakan dalam skala yang lebih

kecil daripada dalam jaringan yang lebih besar [7]. Topologi *Mesh* diilustrasikan seperti pada Gambar 2.7.

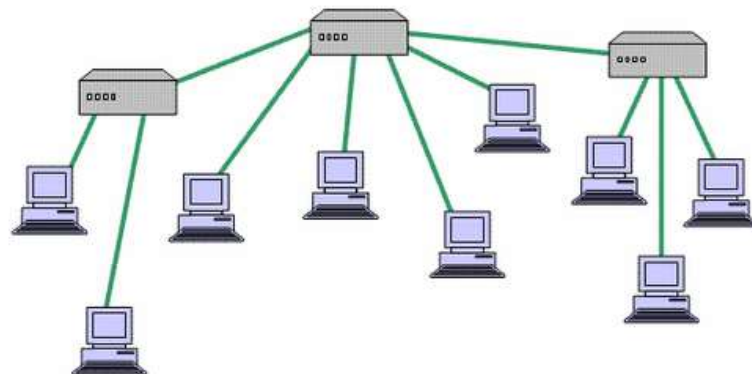


Gambar 2.7 Topologi *Mesh* [16]

E. Topologi *Tree*

Topologi *Tree* merupakan kombinasi desain dari Topologi *Bus* dan Topologi *Ring*, namun yang membedakannya adalah hanya *hub* yang dihubungkan secara langsung, dan setiap *hub* berfungsi sebagai akar dari sekelompok *node*. Dalam topologi ini, *node* dapat berupa *hub* atau perangkat-perangkat lainnya yang terhubung ke *hub* tersebut.[17]

Sebagai contoh, dalam Topologi *Tree*, terdapat banyak jaringan *Star* yang terhubung ke *Hub* pusat, kemudian terdapat jalur yang menghubungkan *Hub* tersebut ke titik-titik berikutnya. *Hub* tersebut juga terhubung ke satu *Hub* utama, yang berperan sebagai akar dari seluruh jaringan data dan menghubungkan semua komputer dalam sistem tersebut [10]. Topologi *Tree* diilustrasikan seperti pada Gambar 2.8.



Gambar 2.8 Topologi *Tree* [17]

2.2.5 Komponen Jaringan Komputer

Pada jaringan komputer terdapat berbagai komponen pendukung untuk membangun suatu jaringan, yaitu:

A. *Ethernet Card/LAN Card*

LAN Card adalah perangkat jaringan yang memungkinkan perangkat lain terhubung dan berbagi data di dalam jaringan. Untuk memastikan transfer data yang optimal, kabel digunakan sebagai media penghubung dalam *LAN Card*. Selain itu, *LAN Card* juga memiliki kemampuan untuk mengubah aliran data dari *paralel* menjadi *serial*, sehingga data dapat dikirim melalui media jaringan kabel UTP (*Unshielded Twisted Pair*) dengan efisiensi yang baik [18]. Bentuk *LAN Card* dapat dilihat seperti pada Gambar 2.9.



Gambar 2.9 LAN Card [19]

B. *NIC (Network Interface Card)*

Perangkat yang dikenal sebagai *NIC (Network Interface Card)* didesain untuk terhubung langsung ke komputer dan memungkinkan komputer-komputer dalam jaringan berkomunikasi satu sama lain. *NIC* bertanggung jawab dalam menentukan bagaimana bit data seperti *voltage*, arus, gelombang elektromagnetik, dan berbagai besaran fisik lainnya dibentuk. *NIC* berperan pada *layer* pertama dalam model OSI (*Open Systems Interconnection*), yang dikenal sebagai *layer* fisik, di mana *NIC* mengatur aspek fisik dalam transmisi data dalam jaringan.[14]. Bentuk dari *Network Interface card* dapat dilihat seperti pada Gambar 2.10.



Gambar 2.10 Network Interface card [14]

C. *Hub*

Hub adalah komponen jaringan komputer yang berfungsi sebagai penghubung untuk menggabungkan beberapa perangkat ke dalam jaringan. Namun, *Hub* memiliki beberapa kekurangan, salah satunya adalah jika *Hub* mengalami masalah atau kerusakan, maka transmisi data dalam jaringan akan terganggu atau bahkan tidak dapat berfungsi sama sekali. Hal ini menyebabkan *Hub* tidak dapat mengatur kecepatan pengiriman data ke komputer lain.

Cara kerja *Hub* adalah dengan menyalin data dari sumber yang terhubung ke port *Hub*. Jika ada lima komputer yang terhubung ke satu *Hub* dalam satu ruangan, hanya satu komputer yang dapat mengirim data pada saat yang sama. *Hub* akan berbagi data dari satu komputer ke semua komputer yang terhubung. Salah satu kelemahan *Hub* adalah tidak dapat mendistribusikan data secara merata di antara setiap *port*, yang berbeda dengan *switch* yang dapat melakukannya. Ketika *volume* trafik terlalu tinggi di *Hub*, kemungkinan terjadinya tabrakan data (*collision*) saat pengiriman data menjadi lebih tinggi [14]. Bentuk dari *Ethernet Hub* dapat dilihat seperti pada Gambar 2.11.



Gambar 2.11 *Ethernet Hub* [14]

D. *Switch*

Mirip dengan *Hub*, *Switch* memiliki kemampuan untuk mengetahui alamat MAC (*Media Access Control*) yang digunakan untuk mengarahkan data ke tujuan yang tepat. Namun, untuk mengurangi lalu lintas di jaringan, *Switch* menggunakan daftar alamat MAC yang terhubung dengan *port* tertentu untuk menentukan ke mana paket data harus dikirim. Kemampuan ini memungkinkan *port-switch* lain tetap berfungsi secara optimal, bahkan jika salah satu *port* sedang sibuk [19]. Bentuk dari *Switch* dapat dilihat seperti pada Gambar 2.12.



Gambar 2.12 *Switch* [19]

E. *Router*

Router adalah perangkat yang berfungsi menghubungkan dua atau lebih segmen jaringan dengan lapisan OSI I, II, dan III yang berbeda [15]. Sebagai contoh, dalam sebuah perusahaan yang memiliki sepuluh komputer *client* yang menggunakan alamat IP 192.168.0.XXX (Jaringan A), tetapi koneksi internet dari ISP menggunakan alamat IP 202.201.200.XXX (Jaringan B), maka diperlukan sebuah *router* dengan setidaknya dua *port*. Jaringan A terhubung ke satu *port*, sementara Jaringan B terhubung ke *port* lainnya. *Router* berperan dalam mengatur aliran data antara kedua segmen jaringan yang berbeda tersebut [15]. Bentuk dari *router* dapat dilihat seperti pada Gambar 2.13.



Gambar 2.13 Router [19]

F. *Repeater*

Repeater adalah perangkat yang berfungsi untuk memperkuat sinyal. Perangkat ini digunakan ketika ingin menghubungkan perangkat dengan jarak yang berjauhan. Kualitas transmisi data pada kartu *ethernet* hanya dapat dipertahankan untuk jangka waktu tertentu dan dalam rentang terbatas sebelum mengalami penurunan kualitas. Oleh karena itu, *repeater* berperan dalam menjaga integritas sinyal dan mencegah terjadinya degradasi selama paket data mencapai tujuannya. [15]

G. *Bridge*

Bridge adalah perangkat yang berfungsi untuk menghubungkan dua jaringan. Fungsi *bridge* ini memungkinkan penghubung antara jaringan yang memiliki berbagai topologi dan media komunikasi yang berbeda. Sebagai contoh, ketika dua lokasi perusahaan menggunakan dua jenis sistem jaringan yang berbeda,

salah satu menggunakan kabel *coaxial* dan yang lainnya menggunakan kabel *fiber optic*, *bridge* dapat digunakan untuk menggabungkan kedua sistem tersebut.

Selain itu, *bridge* juga mampu menghubungkan jaringan dengan topologi *star* ke jaringan dengan topologi *ring*, sehingga mempermudah komunikasi antarjaringan. *Bridge* memiliki *buffer* yang cukup untuk menangani ketidaksesuaian data yang dikirim dan diterima pada kecepatan yang berbeda di antara kedua jaringan yang dihubungkannya. [15]

H. *Modem*

Modem adalah perangkat yang memiliki singkatan dari "*modulation demodulation*" yang berfungsi untuk mengubah sinyal *analog* menjadi sinyal *digital*, serta mengubah sinyal *digital* menjadi sinyal *analog*. Komputer menggunakan *modem* untuk terhubung ke internet. Selain itu, *modem* juga dapat menghubungkan dua komputer melalui saluran telepon, memungkinkan pertukaran data antara kedua perangkat tersebut. [15]

I. Kabel

Salah satu aspek yang sangat krusial adalah kabel, karena kabel berfungsi sebagai penghubung antara dua komputer atau lebih sehingga memungkinkan pertukaran data, serta berperan sebagai penghantar arus listrik. Ada berbagai jenis kabel yang digunakan dalam perangkat komputer. Beberapa di antaranya adalah *Unshielded Twisted Pair* (UTP), *Kabel Foiled Twisted Pair* (FTP), *Kabel Shielded Twisted Pair* (STP), dan berbagai jenis kabel lainnya. [18]

2.2.6 Jaringan *Wireless*

A. *Wireless Fidelity*

WiFi adalah istilah yang merupakan kependekan dari *Wireless Fidelity*, yang merujuk pada serangkaian standar untuk komunikasi dalam jaringan nirkabel (*Wireless Local Area Network/WLAN*) yang didasarkan pada spesifikasi IEEE 802.11.[6]

Salah satu media untuk mengirim dan menerima sinyal serta data dalam sistem adalah WiFi. WiFi memiliki berbagai jenis sinyal seperti 802.11a, 802.11b, 802.11g, 802.11n, dan 802.11ac. Pada bulan Desember 2013, IEEE menetapkan 802.11ac sebagai standar teknologi terbaru dalam jaringan nirkabel [20]. Teknologi jaringan *Wireless* generasi kelima ini, 802.11ac, menawarkan *Throughput* yang

tinggi. Pada teknologi ini, beberapa faktor penting harus dipertimbangkan, termasuk jarak, mitigasi interferensi, dan koneksi.

Standar teknologi 802.11ac menyediakan dua jenis frekuensi gelombang elektromagnetik, yaitu 2,4 GHz dan 5 GHz. Pita 5 GHz menawarkan lebar pita yang lebih besar dan kinerja yang lebih tinggi, namun memiliki interferensi yang lebih tinggi pada pita 2,4 GHz. [21]

B. Standar WiFi

1. Standar 802.11

Pada Juni tahun 1997, standar awal 802.11 diperkenalkan, dan pada tahun 1999, dilakukan pembaruan untuk mengikuti perkembangan teknologi komunikasi. [22] Standar 802.11 dari generasi ke generasi dapat dilihat pada Tabel 2.1.

2. Standar 802.11a

Dirilis pada bulan September 1999, standar 802.11a beroperasi pada frekuensi 5 GHz dan 3,7 GHz dengan lebar kanal 20 MHz. Kecepatan datanya mencapai 54 Mbps. Standar ini menggunakan antena SISO (*Single Input Single Output*). Dengan frekuensi 5 GHz, jangkauan cakupan dalam ruangan mencapai 35 m dan luar ruangan dapat mencakup hingga 125 m, sementara dengan frekuensi 3,7 GHz, jangkauan cakupan luar ruangan bisa mencapai 5 km[22]

3. Standar 802.11b

Dikenalkan pada bulan September tahun 1999, standar 802.11b beroperasi pada frekuensi 2,4 GHz dengan lebar kanal 22 MHz, mampu mencapai kecepatan 11 Mbps. Seperti 802.11a, standar ini juga menggunakan antena SISO. Jangkauan sinyal dalam ruangan adalah 35 meter dan luar ruangan mencapai 140 meter[22]

4. Standar 802.11g

Dirilis pada tahun 2003 dengan kecepatan unduh hingga 54 Mbps, standar 802.11g beroperasi pada frekuensi 2,4 GHz dengan lebar kanal 20 MHz. Cakupan sinyal mencapai 38 meter dalam ruangan dan 140 meter di luar ruangan [22].

5. Standar 802.11n

Diperkenalkan pada tahun 2009, standar 802.11n menggunakan 2 antena untuk fungsi transmisi dan penerimaan data. Teknologi MIMO (*Multi Input Multi Output*) digunakan dalam standar ini, yang memungkinkan beberapa sinyal radio dikordinasikan secara bersamaan. Akibatnya, jangkauan dan *Throughput*

meningkat, dan lebar kanal berubah dari 20 MHz menjadi 40 MHz. Kecepatan maksimal standar WiFi ini adalah 300 Mbps. Jangkauan sinyal mencapai hingga 75 meter dalam ruangan dan 250 meter di luar ruangan [20].

6. Standar 802.11ac

Standar WiFi generasi kelima, 802.11ac, diperkenalkan pada Desember 2013 dengan frekuensi 5 GHz. Terdapat 4 opsi lebar kanal dalam standar ini, yaitu 20 MHz, 40 MHz, 80 MHz, dan 160 MHz. Dibandingkan dengan standar lainnya, 802.11ac memiliki peningkatan kinerja yang signifikan dan cakupan yang lebih luas. Standar ini menggunakan teknologi MU-MIMO (*Multi-user, Multiple Input, Multiple Output*), memungkinkan sekelompok pengguna dan terminal nirkabel berkomunikasi satu sama lain. Kecepatan teoretis mencapai 7 Gbps, tetapi keterbatasan chipset hanya memungkinkan 1,7 Gbps [20].

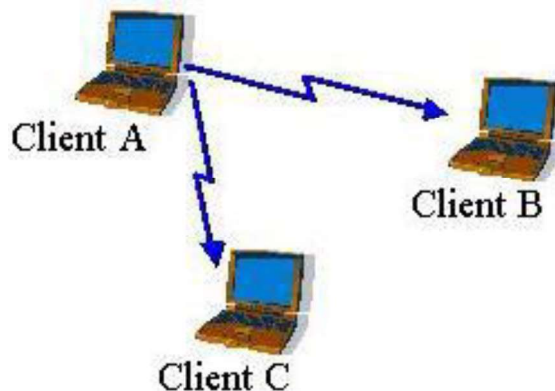
Tabel 2.1 Standard 802.11 [23]

<i>Standard</i>	<i>Year Release</i>	<i>Frequency Band</i>	<i>Bandwidth</i>	<i>Modulation</i>	<i>Max. Data Rate</i>
802.11	1997	2,4 GHz	20 MHz	DSSS, FHSS	2 Mbps
802.11a	1999	5 GHz, 3,7 GHz	20 MHz	OFDM (SISO)	54 Mbps
802.11b	1999	2,4 GHz	20 MHz	DSSS (SISO)	11 Mbps
802.11g	2003	2,4 GHz	20 MHz	DSSS, OFDM (SISO)	54 Mbps
802.11n	2009	2,4 GHz, 5 GHz	20 MHz, 40 MHz	OFDM (MIMO)	600 Mbps
802.11ac	2013	5 GHz	20 MHz, 40 MHz, 80 MHz, 160 MHz	OFDM (MU-MIMO)	7 Gbps

2.2.7 Mode Jaringan WiFi

A. Mode *Ad-Hoc*

Mode *Ad-hoc* atau *Independent Basic Service Set (IBSS)* juga dikenal sebagai jaringan *peer-to-peer*. Mode ini digunakan ketika pengguna saling mengetahui *Service Set Identifier (SSID)* masing-masing. Pada organisasi yang terdiri dari beberapa komputer yang dilengkapi dengan *Wireless Network Interface Card (Wireless NIC)*, mode *Ad-hoc* digunakan untuk membuat koneksi antara perangkat (*server*) dan perangkat lain (*client*) tanpa menggunakan *access point* sebagai pusat pengontrol. Dalam mode ini, komunikasi langsung terjadi antara perangkat-perangkat tanpa adanya infrastruktur jaringan pusat. [24] Mode *Ad-Hoc* diilustrasikan seperti pada Gambar 2.14.

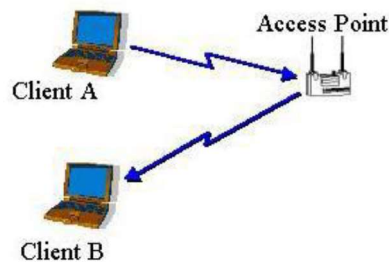


Gambar 2.14 Jaringan *Ad-Hoc* [24]

B. Mode Infrastruktur

Wireless LAN menggunakan *SSID (Service Set Identifier)* sebagai nama jaringan nirkabelnya. Nama ini dapat mencakup maksimal 32 karakter dalam sistem penamaan *SSID*. *SSID* dirancang dengan tingkat keamanan yang baik, sehingga memiliki banyak variasi yang memungkinkan.

Dengan menggunakan *SSID*, *Wireless LAN* dapat diidentifikasi. Ketika beberapa komputer terhubung ke *SSID* yang sama, sebuah jaringan infrastruktur terbentuk. Dalam mode infrastruktur ini, *access point* berperan sebagai pusat komunikasi yang mengatur dan mengkoordinasi koneksi antara perangkat-perangkat yang terhubung ke jaringan nirkabel tersebut [24]. Mode Infrastruktur diilustrasikan seperti pada Gambar 2.15.



Gambar 2.15 Jaringan Infrastruktur [24]

2.2.8 Kekuatan Sinyal WiFi

Kualitas sinyal WiFi dapat diukur menggunakan standar berdasarkan kekuatan sinyalnya. Semakin baik kualitas sinyalnya, semakin tinggi pula kecepatan konektivitasnya. Besaran sinyal WiFi diukur dalam dBm (*decibel milliwatt*), yang merupakan nilai mutlak dari unit daya dan dihitung sebagai nilai daya $10\log/1mW$. Semakin besar nilai dBm yang ditunjukkan, semakin rendah kekuatan sinyalnya. Misalnya, sinyal -75 dBm lebih kuat atau lebih baik dibandingkan sinyal -90 dBm [1]. Standar Kualitas untuk variabel kualitas *Signal to Noise Ratio* (SNR) pada indikator *Signal Level* adalah seperti pada Tabel 2.2.

Tabel 2.2 Skala Kualitas WiFi [1]

Nilai Kekuatan Sinyal (dBm)	Indikator Warna	Kategori
<-60 dBm	Hijau	Sangat Baik
-61 s/d -70	Hijau	Baik
-71 s/d -80	Kuning	Cukup Buruk
-80 s/d -90	Orange	Buruk
>-90	Merah	Sangat Buruk

2.2.9 Keamanan Jaringan *Wireless*

A. WEP (*Wired Equivalent Privacy*)

WEP merupakan sebuah sistem keamanan yang digunakan dalam jaringan komputer berbasis kabel (*Wired LAN*) yang menggunakan *enkripsi*. Sistem ini

memanfaatkan algoritma RC4 untuk melakukan proses *enkripsi* dan dekripsi data. Algoritma RC4 adalah salah satu algoritma yang digunakan untuk mengamankan data sehingga hanya orang yang memiliki kunci enkripsi yang dapat membaca data aslinya. [25]

B. WPA (*WiFi Protected Access*)

WPA diperkenalkan oleh *WiFi Alliance* pada akhir tahun 2002. *WiFi Alliance with Electronics Engineers (IEEE)* menciptakan keamanan dari kelemahan yang terdapat pada protokol WEP. WPA dibuat kompatibel dengan semua perangkat yang ada. Perhatian utama pada WPA yaitu untuk mengatasi kekurangan WEP tanpa melakukan perubahan pada alat yang sudah ada.

Hal ini dilakukan dengan memasukkan (TKIP) *Temporal Key Integrity Protocol* untuk enkripsi dan 802.1X EAP untuk tujuan autentikasi sebagai penawaran keamanan yang tinggi. Untuk menghindari *Information Fabrication (bit flipping)*, WPA menghadirkan kalkulasi *Message Integrity Check (MIC)* yang dikenal dengan nama "*Michael*". [25]

C. WPA2 (*WiFi protected Access 2*)

WPA2 adalah sebuah standar keamanan yang sepenuhnya mengikuti IEEE 802.11 dan merupakan peningkatan dari keamanan WPA sebelumnya. WPA2 memperkuat perlindungan informasi dengan menggunakan mode enkripsi *Cipher Block Chaining Message Authentication Code Protocol (CCMP)* dengan menggunakan blok *Cipher Advanced Encryption Standard (AES)*.

Dalam WPA2, terdapat dua jenis autentikasi yang dapat digunakan, yaitu WPA2-*Personal* dan WPA2-*Enterprise*. WPA2 juga memastikan integritas informasi melalui proses validasi pesan *Cipher Block Chaining*. Selain itu, WPA2 juga melindungi jaringan dari serangan *Replay* dengan menggunakan nomor paket 48-bit. Semua fitur ini menjadikan WPA2 sebagai standar keamanan yang lebih kuat dan lebih handal dalam melindungi jaringan nirkabel. [25]

2.2.10 Kelebihan dan Kekurangan Jaringan *Wireless*

Dengan menggunakan jaringan nirkabel (*Wireless*), cakupan jaringan dapat menjadi lebih luas dibandingkan dengan jaringan yang menggunakan media kabel [26].

Berikut adalah beberapa keuntungan dalam menggunakan jaringan nirkabel:

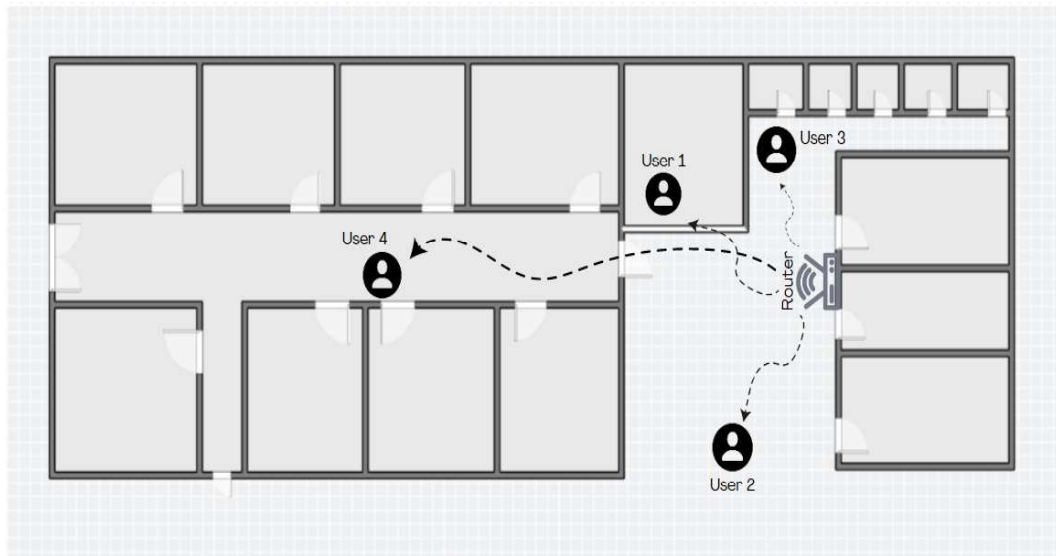
1. Mobilitas tinggi : Pengguna dapat dengan mudah berpindah tempat tanpa terikat oleh kabel, sehingga memungkinkan mobilitas yang tinggi.
2. Kemudahan dan kecepatan instalasi : Pengaturan jaringan nirkabel lebih mudah dan cepat dibandingkan dengan jaringan kabel tradisional, karena tidak memerlukan pemasangan kabel fisik.
3. Menurunkan biaya kepemilikan : Penggunaan jaringan nirkabel dapat mengurangi biaya instalasi dan pemeliharaan kabel, sehingga mengurangi biaya kepemilikan jaringan.
4. Fleksibel : Jaringan nirkabel dapat dengan mudah diubah dan diperluas sesuai dengan kebutuhan tanpa perlu menambah kabel fisik baru.
5. *Scalable* : Jaringan nirkabel dapat dengan mudah diperluas untuk menampung lebih banyak perangkat atau pengguna seiring dengan pertumbuhan kebutuhan jaringan. [26]

Selain keunggulan-keunggulannya, jaringan nirkabel juga memiliki beberapa kelemahan, di antaranya:

1. Resiko *Delay* : Jaringan nirkabel dapat mengalami keterlambatan (*Delay*) dalam mengirimkan dan menerima data, terutama jika ada gangguan atau kendala dalam kanal transmisi.
2. Biaya peralatan yang mahal : Perangkat dan infrastruktur untuk mendukung jaringan nirkabel cenderung lebih mahal dibandingkan dengan jaringan kabel tradisional, terutama jika dibutuhkan teknologi dan fitur yang lebih canggih.
3. Masalah propagasi radio : Sinyal radio dalam jaringan nirkabel dapat terhalang, dipantulkan, atau terganggu oleh berbagai hambatan fisik seperti dinding, gedung, atau perangkat elektronik lainnya, yang dapat menyebabkan degradasi sinyal dan performa jaringan.
4. Keamanan dan kerahasiaan data kurang terjamin. : Jaringan nirkabel lebih rentan terhadap serangan keamanan, seperti peretasan dan penyadapan data, jika tidak diatur dan dienkripsi dengan baik. Hal ini dapat mengancam kerahasiaan dan integritas data yang dikirimkan melalui jaringan tersebut. [23]

2.2.11 *Line of Sight* (LOS)

Line of Sight (LOS) menggambarkan situasi di mana pemancar dan penerima memiliki garis pandang yang jelas tanpa ada hambatan fisik di antara keduanya, seperti yang terlihat pada Gambar 2.16. Meskipun kondisinya LOS, belum tentu jalur tersebut bebas dari gangguan. Beberapa faktor seperti penyerapan sinyal, refleksi sinyal, dan pemisahan sinyal tetap harus dipertimbangkan meskipun garis pandang terjaga. [1]



Gambar 2.16 Skenario Kondisi *Line of Sight* (LOS)[27]

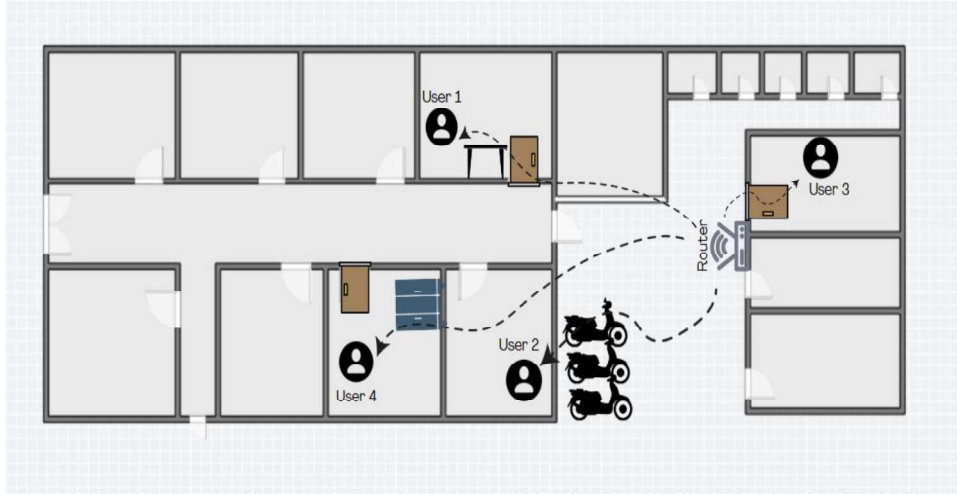
2.2.12 *Non Line of Sight* (NLOS)

Suatu kondisi yang dikenal sebagai *Non-Line of Sight* terjadi ketika penghalang tipis atau tebal, menghalangi pengirim dan penerima di jalur transmisi seperti skenario pada Gambar 2.17. [28]

Non Line of Sight (NLOS) adalah metode komunikasi yang umum digunakan karena gelombang radio yang dipancarkan oleh base station atau perangkat portabel (handset) dapat mengalami berbagai hambatan berdasarkan bentuk dan bahan bangunan sekitarnya. Dalam situasi NLOS, gelombang radio mengalami fenomena seperti refleksi, defleksi, refraksi, dan penetrasi.

Dinding, atap, dan lantai adalah beberapa contoh penghalang yang sering dijumpai. Kehilangan jalur saluran transmisi dipengaruhi oleh hambatan-hambatan tersebut. Istilah "pathloss" merujuk pada perbedaan level sinyal saat pengiriman

dan level sinyal saat diterima, yang mencerminkan tingkat redaman yang dialami oleh sinyal selama proses transmisi.[28]



Gambar 2.17 Skenario Kondisi *Non Line of Sight (NLOS)*[27]

2.2.13 *Quality of Service (QoS)*

Quality of Service (QoS) bukanlah sekadar fitur jaringan, melainkan sebuah konsep arsitektur end-to-end. QoS pada suatu jaringan mengacu pada tingkat kecepatan dan kemampuan yang digunakan untuk menyampaikan berbagai jenis data dalam proses komunikasi. Dengan menggunakan QoS, seorang administrator jaringan dapat memberikan prioritas khusus pada jenis trafik tertentu.

QoS memiliki kemampuan baik secara kuantitatif maupun kualitatif untuk mendefinisikan layanan yang disediakan, memastikan bahwa penggunaan jaringan berlangsung dengan optimal dan sesuai dengan kebutuhan yang ditetapkan.[29]

QoS juga dapat dianggap sebagai kumpulan teknik untuk mengelola *bandwidth*, *Jitter*, *Delay*, *Throughput*, dan *Packet loss* pada aliran paket yang berada dalam suatu jaringan [20]. Indeks Parameter QoS dapat dilihat pada Tabel 2.3.

Tabel 2.3 Indeks *Parameter QoS* [29]

Score	Persentase	Indeks
3,8 – 4	95 % – 100%	Sangat Bagus

Score	Persentase	Indeks
3 – 3,79	75 % – 95,75 %	Bagus
2 – 2,99	50 % – 74,75 %	Sedang
1 – 1,99	25 % – 49,75 %	Buruk

Sumber : *TIPHON* [30]

Adapun parameter-parameter pengukuran QoS yang digunakan pada penelitian ini, yaitu:

A. *Bandwidth*

Bandwidth mengacu pada lebar rentang frekuensi yang digunakan oleh sinyal dalam media transmisi. Istilah ini sering digunakan untuk menggambarkan kemampuan transfer data dalam suatu jaringan, yang menunjukkan jumlah data yang dapat ditransfer dari satu lokasi ke lokasi lain dalam periode waktu tertentu (biasanya dihitung dalam detik). [29]

B. *Throughput*

Throughput adalah kemampuan suatu jaringan untuk melakukan pengiriman data. Biasanya, *Throughput* dikaitkan dengan *bandwidth*, tetapi *Throughput* dapat berfluktuasi berdasarkan lalu lintas jaringan saat data sedang dikirim atau diterima. Sementara itu, *bandwidth* cenderung lebih stabil. [29]

Beberapa faktor yang mempengaruhi *bandwidth* dan *Throughput* antara lain perangkat jaringan yang digunakan, jenis data yang ditransfer, jumlah pengguna dalam jaringan, topologi jaringan, spesifikasi komputer klien atau pengguna, server komputer, interferensi listrik, serta kondisi cuaca. *Throughput* juga dikenal sebagai kecepatan transfer data efektif yang diukur dalam *bit per second* (bps) [29]. Rumus mencari *throughput* dapat dilihat pada persamaan 2.1. Kategori *Throughput* dapat dilihat pada Tabel 2.4.

$$Throughput (bps) = \frac{Paket\ data\ yang\ diterima}{Waktu\ Pengiriman} \quad (2.1)$$

Tabel 2.4 Kategori *Throughput* [29]

Kategori	<i>Throughput</i>	Indeks
Sangat Baik	>2,1 Mbps	4

Kategori	Throughput	Indeks
Baik	1200 kbps – 2,1 Mbps	3
Cukup	700 kbps – 1200 kbps	2
Kurang	338 kbps – 700 kbps	1
Buruk	0 – 338 kbps	0

Sumber : TIPHON [30]

C. *Packet loss*

Packet loss menggambarkan situasi di mana sejumlah paket data hilang selama proses transmisi. Hal ini bisa terjadi akibat adanya tabrakan (*collision*) atau kepadatan (*congestion*) pada jaringan. Dalam kondisi *Packet loss*, paket data tidak berhasil mencapai tujuan yang dituju saat proses pengiriman [29] Rumus perhitungan *packet loss* dapat dilihat pada persamaan 2.2. Kategori *Packet loss* dapat dilihat pada Tabel 2.5. Berikut adalah beberapa faktor yang dapat menyebabkan *Packet loss* :

1. Saat ada *overload* trafik pada jaringan.
2. Kemacetan (*Congestion*) dalam jaringan yang menyebabkan paket-paket data tidak dapat terkirim secara efisien.
3. *Error* yang terjadi pada media fisik.
4. *Buffer* yang terlalu penuh (*overflow*) dapat menyebabkan berbagai masalah, termasuk kegagalan pada sisi penerima. [29]

Tabel 2.5 Kategori *Packet loss* [31]

Kategori	Packet loss	Indeks
Sangat Baik	0 – 2%	4
Baik	3 – 14%	3
Cukup	15 – 24%	2
Buruk	>25%	1

Sumber : TIPHON [30]

$$Packet Loss (\%) = \frac{Paket\ data\ dikirim - Paket\ data\ diterima}{Paket\ data\ dikirim} \times 100 \quad (2.2)$$

D. Delay

Delay adalah waktu total yang dibutuhkan oleh paket data selama proses transmisi dari satu lokasi ke lokasi tujuan. *Delay* pada jaringan terdiri dari beberapa komponen [29], yaitu:

1. *Delay processing*: Waktu yang diperlukan oleh perangkat jaringan untuk memproses paket data, seperti melakukan pemrosesan *header* dan perubahan format data.
2. *Delay packetization*: Waktu yang dibutuhkan untuk mengumpulkan data dari aplikasi dan membaginya menjadi paket-paket yang sesuai dengan protokol jaringan yang digunakan.
3. *Delay serialization*: Waktu yang diperlukan untuk mengubah paket data menjadi serangkaian *bit* yang akan dikirim melalui media transmisi.
4. *Delay Jitter buffer*: Waktu penundaan yang terjadi ketika paket data tiba di penerima dengan kecepatan yang tidak konsisten. *Jitter buffer* digunakan untuk mengompensasi variasi waktu kedatangan paket-paket tersebut.
5. *Delay network*: Waktu yang diperlukan oleh paket data untuk melakukan perjalanan melalui jaringan, termasuk waktu yang diperlukan untuk melewati *router* dan *switch*.

Upaya dilakukan untuk mengelola dan mengurangi *Delay* sebanyak mungkin agar pengalaman pengguna dalam berkomunikasi dan mengakses data lebih responsif dan efisien. Rumus perhitungan dapat dilihat pada persamaan 2.3. Kategori *Delay* dapat dilihat pada Tabel 2.6.

$$Delay (ms) = \frac{Total\ Delay}{Total\ paket\ yang\ diterima} \quad (2.3)$$

Tabel 2.6 Kategori Delay [29]

Kategori	Besar Delay	Indeks
Sangat Baik	<150 ms	4
Baik	150 – 300 ms	3
Cukup	300 – 450 ms	2
Buruk	>450 ms	1

Sumber : *TIPHON* [30]

E. *Jitter*

Dalam jaringan IP, *Jitter* mengacu pada variasi waktu keterlambatan antara kedatangan paket data. Variasi ini disebabkan oleh beban trafik yang berfluktuasi dan jumlah tabrakan paket (*congestion*) di jaringan IP. Ketika terjadi trafik yang lebih tinggi atau *congestion* pada jaringan, nilai *Jitter* akan meningkat. Hal ini berdampak pada kualitas layanan (QoS) jaringan, karena nilai *Jitter* yang tinggi akan menurunkan kualitas QoS secara proporsional.

Untuk memperoleh nilai QoS jaringan yang baik, penting untuk menjaga nilai *Jitter* seminimal mungkin. Upaya dilakukan untuk mengelola dan mengurangi *Jitter* agar data dapat diterima dengan keterlambatan yang konsisten dan stabil. Pengendalian *Jitter* menjadi kunci untuk memastikan bahwa aplikasi dan layanan di jaringan dapat berjalan dengan baik [29]. Rumus mencari *Jitter* dapat dilihat pada persamaan 2.4. Kategori *Jitter* dapat dilihat pada Tabel 2.7.

$$Jitter (ms) = \frac{\text{Total variasi delay}}{\text{Total paket yang diterima}} \quad (2.4)$$

Tabel 2.7 Kategori *Jitter* [30] [32]

Kategori	<i>Jitter</i> (ms)	Indeks
Sangat Baik	0 ms	4
Baik	1 s/d 75 ms	3
Cukup	75 s/d 125 ms	2
Buruk	125 s/d 225 ms	1

2.2.14 Penempatan *Posisi Access Point*

Salah Dalam sektor *Infrastructure Network*, salah satu tantangan yang dihadapi adalah optimasi penempatan *access point*. Sebelum melakukan implementasi, perencanaan pengembangan jaringan WiFi harus mempertimbangkan berbagai faktor dan melakukan analisis teoretis agar penempatan *access point* berjalan secara efektif.

Ini melibatkan tidak hanya pemasangan *infrastruktur access point*, tetapi juga memperhatikan aspek-aspek seperti kekuatan daya pancar sinyal *access point*, desain dan struktur ruangan, interferensi gelombang radio, hambatan sinyal, serta

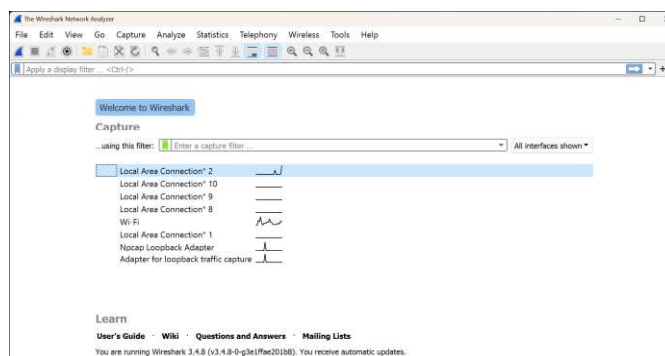
penghalang yang dapat mempengaruhi penerimaan sinyal dari *access point* ke perangkat penerima.

Penempatan *access point* di posisi yang tepat di tengah-tengah ruangan atau lokasi menjadi metode yang berpengaruh dalam memastikan cakupan jaringan WiFi yang optimal. Lokasi *access point* memiliki dampak signifikan terhadap area cakupan sinyal WiFi, karena jangkauan perangkat penerima sangat dipengaruhi oleh lokasi *access point*. Dengan penempatan *access point* yang tepat, area cakupan sinyal WiFi dapat dioptimalkan sehingga penggunaan jaringan WiFi menjadi lebih efisien dan efektif.[33]

2.2.15 Software Network Analyzer

Salah satu perangkat lunak yang sering digunakan oleh *Network Administrator* adalah *Wireshark*, sebuah *Software Network Analyzer*. *Wireshark* memiliki kemampuan untuk menganalisis berbagai jenis jaringan, baik yang berbasis kabel maupun nirkabel (*Wireless*). Perangkat lunak ini digunakan untuk tujuan pendidikan, analisis, pengembangan perangkat lunak dan protokol komunikasi, serta sebagai solusi untuk mengatasi permasalahan jaringan.

Wireshark dapat menangkap dan menganalisis paket-paket data yang berada dalam jaringan. Dengan perangkat lunak ini, berbagai jenis paket informasi yang dikirim dalam berbagai format protokol dapat dengan mudah dianalisis oleh *Network Administrator*. *Wireshark* menjadi alat yang sangat berguna dalam memantau lalu lintas jaringan, memecahkan masalah koneksi, dan memahami interaksi antara perangkat yang terhubung dalam suatu jaringan [34]. Tampilan dari *Wireshark* dapat dilihat pada Gambar 2.18.



Gambar 2.18 Tampilan Software Wireshark [34]