

BAB II

LANDASAN TEORI

2.1 Tinjauan Jurnal

Wireless Fidelity (WiFi) merupakan teknologi jaringan nirkabel yang diperkenalkan pada tahun 1999 oleh lembaga sertifikasi jaringan di Amerika Serikat [5]. Teknologi ini memungkinkan beberapa perangkat terhubung dalam satu jaringan nirkabel, dengan jangkauan rata-rata hingga 30 meter dari *access point*. Untuk menunjang konektivitas tersebut, dibutuhkan perangkat *Access Point* (AP) yang berfungsi menghubungkan perangkat pengguna ke jaringan lokal melalui gelombang radio. Dalam implementasi skala kecil, pengelolaan AP mungkin masih dapat dilakukan secara manual. Namun, seiring meningkatnya jumlah *access point* dalam suatu gedung, pengelolaan menjadi semakin kompleks. Hal ini dapat menyulitkan administrator dalam memantau kinerja, mengatur konfigurasi, serta menjaga kestabilan koneksi jaringan. Oleh karena itu, dibutuhkan sistem manajemen jaringan yang terpusat, efisien dan mudah dioperasikan guna memudahkan pengawasan dan pengendalian seluruh *access point* secara optimal [6].

Teknologi Wifi memiliki sejumlah keunggulan yang menjadikannya pilihan utama dalam implementasi jaringan nirkabel. Beberapa kelebihan Wifi antara lain fleksibilitas dalam mobilitas pengguna, kemudahan akses internet di berbagai lokasi, serta efisiensi dalam konsumsi energi listrik. Namun, di balik keunggulan tersebut, Wifi juga memiliki kelemahan, seperti kerentanan terhadap penyadapan, harga perangkat yang relatif mahal, serta penurunan kualitas sinyal dalam kondisi tertentu. Seiring meningkatnya kebutuhan konektivitas, masalah umum seperti lemahnya sinyal

access point, koneksi yang lambat, dan *bandwidth* yang tidak stabil sering menjadi kendala, sehingga mengganggu kenyamanan pengguna dalam mengakses jaringan secara optimal. Hal ini menunjukkan bahwa kemudahan akses tidak selalu diikuti dengan kestabilan dan keamanan jaringan yang memadai [7].

Keamanan jaringan merupakan aspek krusial dalam teknologi Wifi karena sifatnya yang terbuka dan rentan terhadap penyalahgunaan. Administrator berperan penting dalam mengendalikan akses, memantau aktivitas, dan mencegah pelanggaran terhadap sumber daya jaringan. Oleh karena itu, perancangan infrastruktur jaringan harus mengedepankan perlindungan data dan kestabilan sistem. Selain itu, untuk menjaga kualitas layanan, diperlukan penerapan *Quality of Service* (QoS) yang memungkinkan pengelolaan performa jaringan melalui parameter seperti *throughput*, *jitter* dan *packet loss*. Integrasi antara keamanan dan QoS menjadi kunci dalam membangun jaringan nirkabel yang andal dan terlindungi [8].

UniFi Cloud Gateway menyediakan solusi manajemen jaringan terpusat dengan fitur monitoring, manajemen perangkat dan kebijakan keamanan, sehingga mampu mengoptimalkan kinerja jaringan dalam satu platform terpadu. [9]

Berdasarkan beberapa penelitian sebelumnya [6], [7], [8], [10], mayoritas penelitian menunjukkan bahwa keterbatasan perangkat *access point standalone* menjadi hambatan utama dalam pengelolaan jaringan WiFi skala besar. Solusi yang direkomendasikan secara konsisten adalah penerapan sistem manajemen jaringan berbasis *cloud* yang mendukung pengelolaan terpusat, integrasi fitur QoS, serta penguatan sistem keamanan melalui konfigurasi *firewall*. Pendekatan ini dinilai mampu meningkatkan efisiensi pemantauan, memperluas cakupan sinyal, serta menjaga stabilitas dan kualitas koneksi secara berkelanjutan.

Tabel II. 1 Tabel Jurnal

N o	Peneliti (Tahun)	Judul	Metode	Hasil Utama	Kelebihan	Kekurangan
1	Ronald David Marcus dan Annisa Dwi Prameswari (2022)	Manajemen dan Keamanan Jaringan Nirkabel Berbasis Wireless Gateway Security Controlling System	Flowchart	Kemudahan dalam mengelola Jaringan Wifi dalam skala yang luas	Membentuk suatu jaringan wireless dengan system pengendali yang terpusat	Keterbatasan fitur salah satunya ialah pengawasan lalu lintas data
2	Muhamad Agil Faizi dan Febrian Wahyu Christanto (2024)	Manajemen Perangkat Jaringan <i>Access Point</i> Menggunakan UniFi Controller di Jaringan Kampus	Network Development Life Cycle (NDLC)	Hasil penelitian menunjukkan bahwa implementasi konfigurasi <i>access point</i> menggunakan UniFi Controller dapat meningkatkan kecepatan internet dari 2 Mbps menjadi 10 Mbps, serta memiliki kualitas layanan jaringan wireless yang baik dengan Throughput 1276 kbps, Packet loss 0%, dan Jitter 4.8 ms	Implementasi konfigurasi <i>access point</i> menggunakan UniFi Controller dapat meningkatkan kinerja jaringan wireless di Universitas Muhammadiyah Semarang	Keterbatasan fitur salah satunya ialah pengawasan lalu lintas data
3	Akbar Averian, Avon Budiono, Umar Yunan Kurnia Septo Hediyanto (2023)	Analisis dan Pengoptimalisasi Jaringan Wireless Local Area Network (WLAN) Pada PT.XYZ Dengan Menggunakan Metode Network Development Life Cycle (NDLC)	Network Development Life Cycle (NDLC)	Hasil penelitian ini menunjukkan bahwa dengan mengganti <i>access point</i> dan melakukan perubahan konfigurasi, dapat menghindari interferensi dan overlapping channel, sehingga jaringan wireless menjadi lebih optimal.	Optimalisasi jaringan dilakukan dengan pemilihan channel yang tepat untuk menghindari interferensi, seperti penggunaan channel 1, 6, dan 11 pada frekuensi 2.4 GHz, serta pemanfaatan spektrum 5 GHz yang lebih bersih dari overlapping. Penempatan AP di area strategis membantu pemerataan sinyal. Kelebihannya adalah peningkatan stabilitas dan cakupan jaringan	Berdasarkan hasil penelitian yang dilakukan dalam pengoptimalisan jaringan wireless PT.XYZ dengan menggunakan NDLC dengan kondisi jaringan wireless yang masih belum optimal dalam penggunaannya berupa perangkat, konfigurasi dan penempatan.

4	Mokhammad Gustiawan, Ristu Juli Yudianto, Johanes Pratama, Abdurrahman Fauzi (2021)	Implementasi Jaringan Hotspot Di Perkantoran Guna Meningkatkan Keamanan Jaringan Komputer	Network Development Life Cycle (NDLC)	Untuk menganalisis dan melakukan implementasi jaringan hotspot dan pada Perkantoran sehingga kantor dapat memberikan fasilitas hotspot berbasis mikrotik, membagi bandwidth pada jaringan hotspot secara merata kepada setiap pelanggan dan membatasi penggunaan bandwidth sesuai dengan waktu yang tertera pada paket voucher	Dengan digunakannya Mikrotik RouterOS pada jaringan hotspot, maka admin dapat membatasi penggunaan bandwidth pelanggan berdasarkan paket voucher yang telah dibuat dan tidak terjadi tarik menarik bandwidth antar pelanggan karena pembagian bandwidth yang sama rata.	Belum tersedia sistem pemantauan jaringan secara terpusat, sehingga konfigurasi masih dilakukan secara manual pada setiap perangkat
---	---	---	---------------------------------------	--	---	---

Berdasarkan beberapa studi sebelumnya [6], [7], [8], [10], dapat disimpulkan bahwa jaringan nirkabel membutuhkan pengelolaan yang canggih untuk menjamin efisiensi dan keamanan. Oleh karena itu, penelitian ini diarahkan pada pengembangan sistem manajemen jaringan nirkabel berbasis Cloud Gateway, yang mendukung QoS dan penguatan *firewall*.

2.2 Konsep Dasar Jaringan

Wibowo [11] Jaringan komputer merupakan suatu sistem yang menghubungkan dua atau lebih perangkat komputer untuk memungkinkan pertukaran data melalui media komunikasi tertentu. Jaringan ini dapat dibentuk dengan minimal dua perangkat atau terminal, seperti komputer, laptop, gadget, atau perangkat elektronik lainnya yang mendukung fungsi jaringan. Tujuan utama dari pengaturan jaringan komputer adalah untuk memungkinkan *transfer* dan komunikasi data antar perangkat. Data yang ditransmisikan dapat berupa *teks*, *audio*, *video*, maupun kombinasi dari ketiganya.

Jaringan komputer merupakan sebuah sistem yang dirancang untuk menghubungkan dua atau lebih perangkat komputer, sehingga memungkinkan terjadinya pertukaran data, informasi, dan sumber daya seperti printer atau koneksi internet secara efisien. Dengan adanya jaringan, komunikasi antarperangkat menjadi lebih mudah, cepat, dan terkoordinasi, baik dalam skala kecil maupun skala besar. [12]

A. Topologi Jaringan

Topologi jaringan adalah teknologi yang mempelajari cara menghubungkan komputer satu sama lain. Ini juga dapat menggabungkan dua komputer dengan menggunakan kabel UTP, fiber optik ataupun nirkabel.

Dalam sebuah jaringan komunikasi, setiap perangkat yang menjadi bagian dari jaringan serta mampu menerima, membuat, menyimpan, atau mengirimkan data melalui berbagai rute disebut sebagai node. Dalam konteks komunikasi data, node dapat berupa perangkat seperti *modem*, *hub*, *bridge*, *switch*, *router*, telepon digital, printer, komputer maupun *server*. Sementara itu, topologi jaringan secara fisik menggambarkan metode pengkabelan fisik dari suatu jaringan, yaitu struktur atau desain jaringan yang menunjukkan bagaimana berbagai komponen jaringan, seperti perangkat dan kabel, diposisikan dan dihubungkan satu sama lain [12].

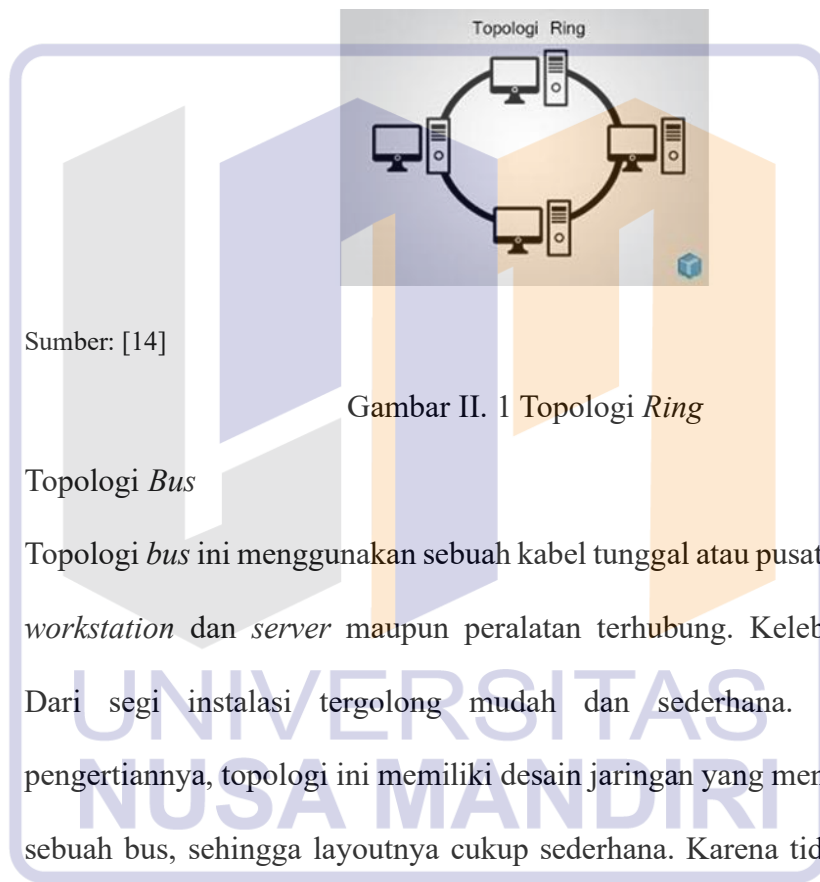
Beberapa topologi yang digunakan secara umum adalah

1. Topologi *Ring*

Semua *workstation* dan *server* dihubungkan sehingga terbentuk suatu pola lingkaran atau cincin. Topologi *ring* merupakan topologi dimana setiap perangkat dihubungkan sehingga berbentuk ring atau lingkaran. Kelebihan Topologi *Ring* adalah lebih murah, tidak diperlukannya *host*, kecepatan dalam pengirimannya yang tinggi, mudah dalam perancangan, pengaksesan data yang optimal, penggunaan kabel yang sedikit, komunikasi antar terminal mudah,

mampu melayani *traffic* yang padat. Sedangkan Kelurangnya adalah pengiriman suara, *video*, dan data yang buruk, kerusakan pada salah satu komputer dapat menyebabkan jaringan lumpuh, memerlukan penanganan dan pengelolaan khusus *bundles*, perubahan jumlah perangkat yang sulit, kinerja komunikasi bergantung dari banyaknya node yang terdapat pada jaringan. [13]

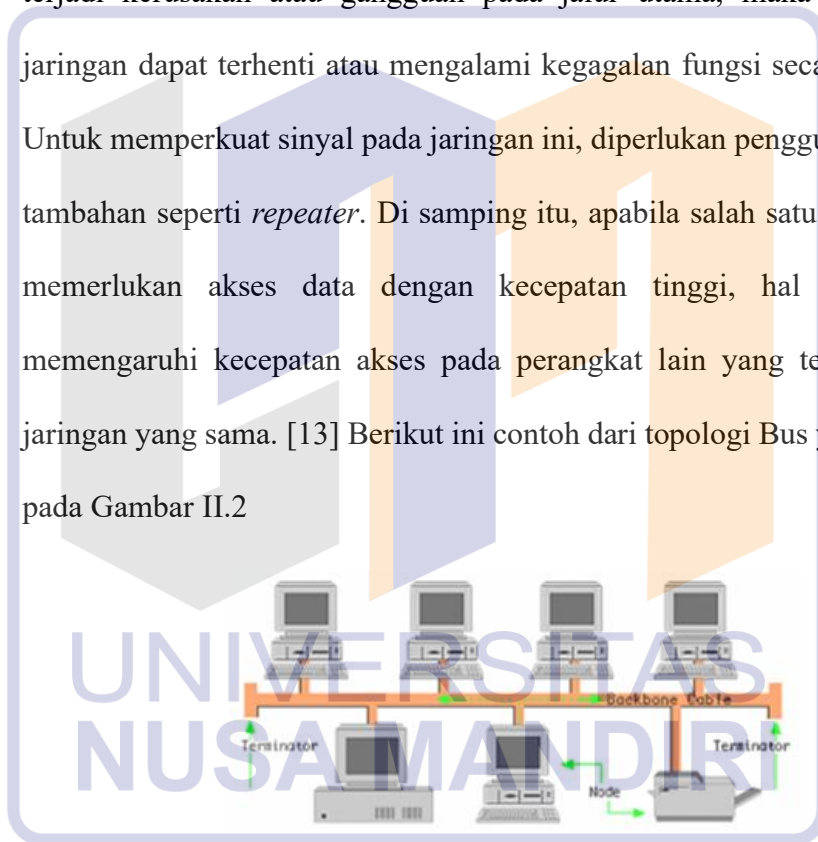
Berikut ini contoh dari topologi Ring yang ditunjukkan pada Gambar II.1



2. Topologi *Bus*

Topologi *bus* ini menggunakan sebuah kabel tunggal atau pusat dimana seluruh *workstation* dan *server* maupun peralatan terhubung. Kelebihannya adalah Dari segi instalasi tergolong mudah dan sederhana. Sesuai dengan pengertiannya, topologi ini memiliki desain jaringan yang menyerupai interior sebuah bus, sehingga layoutnya cukup sederhana. Karena tidak memerlukan banyak kabel maupun komponen tambahan, biaya pembuatannya relatif rendah dibandingkan dengan jenis topologi lainnya. Oleh karena itu, topologi *bus* sering dipilih untuk menekan pengeluaran dalam pembangunan jaringan. Selain itu, topologi ini juga mudah dikembangkan tanpa mengganggu perangkat jaringan lain yang terhubung. Jika terjadi kerusakan pada salah satu perangkat klien, hal tersebut tidak akan memengaruhi perangkat klien lainnya. Dalam implementasinya, topologi bus tidak memerlukan perangkat keras

seperti *switch* atau *hub*, sebagaimana diperlukan dalam topologi *star*. Sedangkan kekurangannya adalah apabila terjadi gangguan pada salah satu perangkat komputer, proses identifikasi letak kesalahan cenderung sulit dilakukan. Selain itu, jaringan dengan topologi ini memiliki karakteristik lalu lintas data yang semakin padat seiring bertambahnya jumlah perangkat yang terhubung, yang pada akhirnya dapat menurunkan performa jaringan. Jika terjadi kerusakan atau gangguan pada jalur utama, maka seluruh sistem jaringan dapat terhenti atau mengalami kegagalan fungsi secara menyeluruh. Untuk memperkuat sinyal pada jaringan ini, diperlukan penggunaan perangkat tambahan seperti *repeater*. Di samping itu, apabila salah satu komputer klien memerlukan akses data dengan kecepatan tinggi, hal tersebut dapat memengaruhi kecepatan akses pada perangkat lain yang terhubung dalam jaringan yang sama. [13] Berikut ini contoh dari topologi Bus yang ditunjukkan pada Gambar II.2



Sumber: [14]

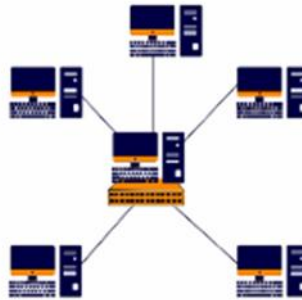
Gambar II. 2 Topologi *Bus*

3. Topologi *Star*

Pada topologi jenis *star* setiap komputer dihubungkan menggunakan *switch*, dimana fungsi *switch* adalah untuk pengatur lalu lintas seluruh komputer yang terhubung karena menggunakan proses pengiriman dan penerimaan informasi secara langsung. Keunggulan yang menjadikannya banyak digunakan dalam

implementasi jaringan komputer. Topologi ini bersifat *fleksibel* karena memungkinkan penambahan atau pengurangan perangkat tanpa mengganggu kinerja jaringan secara keseluruhan. Dari segi keamanan, topologi star menawarkan tingkat perlindungan data yang relatif tinggi karena setiap perangkat terhubung secara terpusat melalui *switch*. Selain itu, proses deteksi dan penanganan gangguan pada jaringan ini tergolong mudah dilakukan, karena kerusakan pada satu perangkat tidak akan memengaruhi perangkat lainnya. Instalasi dan pengelolaan jaringan dengan bentuk topologi ini sederhana, serta memudahkan dalam proses pemeliharaan dan pemecahan masalah jaringan. Sedangkan kekurangannya biaya implementasinya yang relatif tinggi karena memerlukan perangkat tambahan seperti *switch*. Selain itu, topologi ini memiliki ketergantungan yang besar terhadap perangkat pusat tersebut. Jika *switch* mengalami kerusakan, maka seluruh jaringan dapat terganggu atau bahkan lumpuh. Kapasitas koneksi pada *switch* juga bersifat terbatas, sehingga jumlah perangkat yang dapat dihubungkan memiliki batasan tertentu. Di sisi lain, apabila terjadi kemacetan lalu lintas data, kinerja jaringan secara keseluruhan dapat menurun dan menyebabkan keterlambatan dalam proses transmisi data. [13]

Berikut ini contoh dari topologi *star* yang ditunjukkan pada Gambar II.3



Sumber: [14]

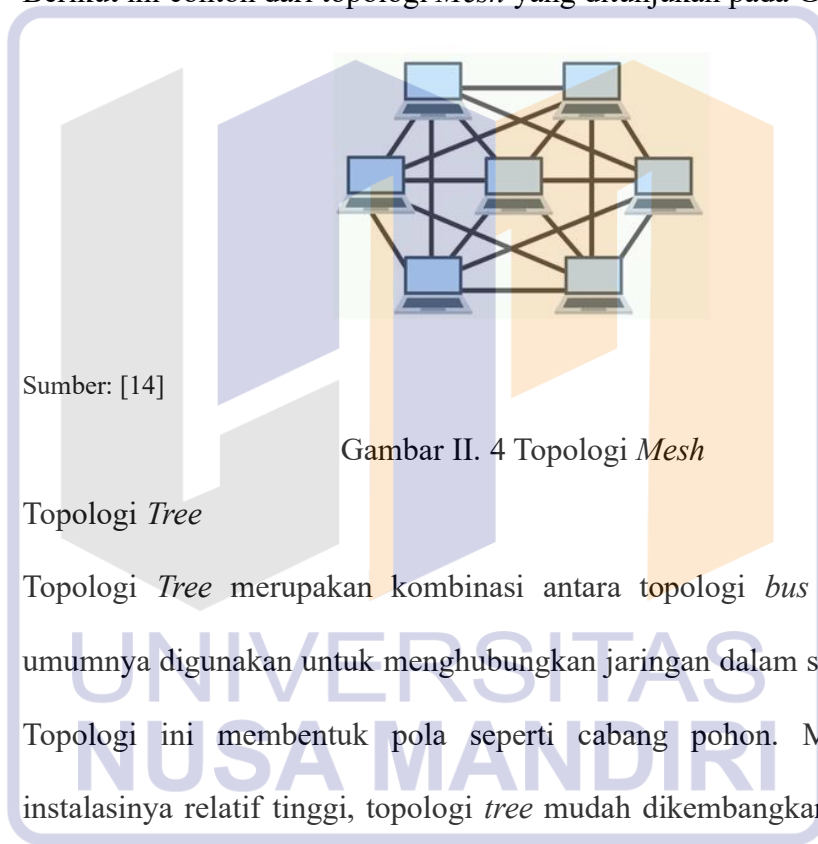
Gambar II. 3 Topologi *Star*

4. Topologi *Mesh*

Jenis topologi jaringan yang menghubungkan setiap perangkat secara langsung satu sama lain melalui koneksi *point-to-point*. Dengan demikian, setiap komputer dalam jaringan memiliki jalur komunikasi khusus dengan komputer lainnya, sehingga kecil kemungkinan terjadinya gangguan akibat putusnya satu jalur komunikasi. Namun, seiring bertambahnya jumlah perangkat yang terhubung, proses instalasi jaringan menjadi semakin kompleks. Hal ini disebabkan oleh kebutuhan jumlah kabel yang meningkat secara signifikan, yang dapat menyulitkan dalam proses pemasangan dan pemeliharaan jaringan. Kelebihannya adalah tingkat keamanan data yang baik, karena setiap perangkat terhubung secara langsung dan independen. Selain itu, topologi ini menawarkan *bandwidth* yang relatif besar, sehingga mampu mendukung lalu lintas data yang tinggi. Risiko terjadinya tabrakan data juga sangat minim karena data dikirimkan melalui jalur khusus antar perangkat. Dengan jalur komunikasi yang terdedikasi, proses pengiriman dan pemrosesan data dapat berlangsung dengan cepat dan efisien. Sedangkan Kekurangannya adalah terutama dari segi biaya dan kompleksitas. Biaya pemasangan topologi ini

tergolong tinggi karena memerlukan sejumlah besar kabel dan port untuk menghubungkan setiap perangkat secara langsung. Selain itu, proses instalasi dan konfigurasi jaringan dengan topologi mesh bersifat rumit dan memerlukan keahlian teknis yang memadai, sehingga tidak selalu efisien untuk diterapkan pada skala jaringan yang besar atau dalam lingkungan dengan sumber daya terbatas. [13]

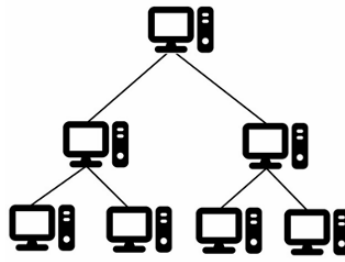
Berikut ini contoh dari topologi *Mesh* yang ditunjukkan pada Gambar II.4



5. Topologi *Tree*

Topologi *Tree* merupakan kombinasi antara topologi *bus* dan *star* yang umumnya digunakan untuk menghubungkan jaringan dalam struktur hierarki. Topologi ini membentuk pola seperti cabang pohon. Meskipun biaya instalasinya relatif tinggi, topologi *tree* mudah dikembangkan sesuai dengan kebutuhan dan skala bisnis yang ada. [15]

Berikut ini contoh dari topologi *Tree* yang ditunjukkan pada Gambar II.5



Sumber: [14]

Gambar II. 5 Topologi *Tree*

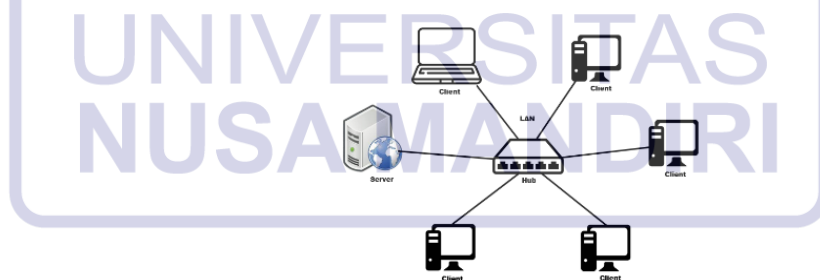
B. Jenis Jaringan Komputer

Berdasarkan cakupan geografisnya, jaringan komputer diklasifikasikan ke dalam tiga jenis utama, yaitu:

1. *Local Area Network (LAN)*

Jaringan LAN berfungsi untuk menghubungkan komputer, laptop, server, dan perangkat lainnya dalam jangkauan yang terbatas atau jarak dekat. Dengan cakupan tersebut, jaringan LAN umumnya digunakan pada lingkungan kampus, gedung perkantoran, rumah, sekolah, serta area terbatas lainnya. [7]

Berikut ini contoh dari jaringan LAN yang ditunjukkan pada Gambar II.6



Sumber: [16]

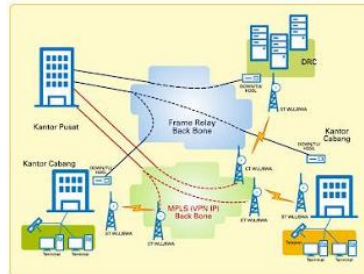
Gambar II. 6 Jaringan LAN

2. *Metropolitan Area Network (MAN)*

Jaringan MAN merupakan jenis jaringan yang mencakup area dalam satu kota dan memiliki kemampuan transfer data berkecepatan tinggi. Jaringan ini menghubungkan berbagai lokasi seperti kampus, perkantoran, instansi

pemerintahan, dan lokasi-lokasi lain dalam satu wilayah metropolitan. [13]

Berikut ini contoh dari jaringan MAN yang ditunjukkan pada Gambar II.7



Sumber: [16]

Gambar II. 7 Jaringan MAN

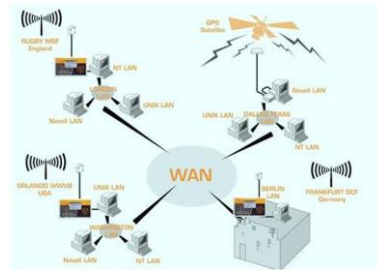
3. *Wide Area Network (WAN)*

WAN merupakan jenis jaringan komputer yang mencakup area geografis yang luas. WAN digunakan untuk menghubungkan jaringan di berbagai wilayah, bahkan antar negara, sehingga memungkinkan pertukaran data dalam skala besar dan lintas lokasi. [17]

Dalam konteks perusahaan, WAN biasanya mencakup koneksi antara kantor pusat, kantor cabang, dan fasilitas lain yang dimiliki perusahaan. Untuk menghubungkan LAN ke WAN atau sebaliknya, umumnya digunakan perangkat seperti *router* atau perangkat jaringan multifungsi lainnya. Adapun jaringan LAN sendiri merupakan jaringan milik pribadi yang digunakan dalam satu gedung atau area terbatas dengan jangkauan sekitar 1 hingga 10 kilometer.

[13]

Berikut ini contoh dari jaringan WAN yang ditunjukkan pada Gambar II.8



Sumber: [16]

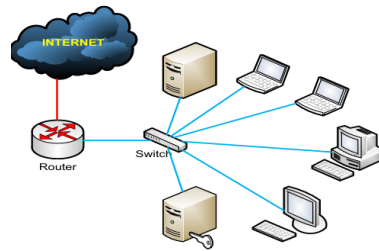
Gambar II. 8 Jaringan WAN

Selain berdasarkan cakupan geografis, jaringan komputer juga dapat diklasifikasikan berdasarkan media transmisi yang digunakan. Dalam konteks lingkungan perkantoran, terdapat dua jenis utama jaringan komputer berdasarkan media fisiknya, yaitu:

a. Jaringan Kabel (*Wired Network*)

Jaringan Kabel merupakan metode pendistribusian informasi yang menggunakan kabel sebagai media penghubung antarperangkat. Jenis jaringan ini umumnya digunakan pada lingkungan dengan cakupan jaringan tetap atau infrastruktur yang stabil. Beberapa jenis kabel yang sering digunakan antara lain *coaxial cable*, *Unshielded Twisted Pair (UTP)*, dan *Fiber Optic (FO)*. Agar dua perangkat dapat saling berkomunikasi, keduanya harus terhubung secara fisik melalui kabel, sehingga menjadikan jaringan kabel kurang fleksibel dibandingkan jaringan nirkabel. Kabel yang digunakan biasanya terdiri dari untaian logam atau serat optik yang bertugas menghantarkan data dari satu titik ke titik lainnya. [18]

Berikut ini contoh dari jaringan Kabel yang ditunjukkan pada Gambar II.9



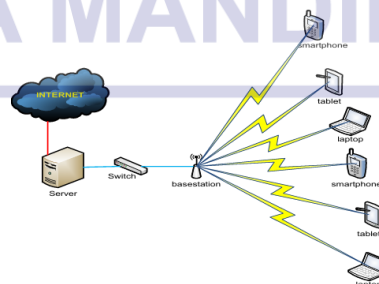
Sumber: [11]

Gambar II. 9 Jaringan Kabel

b. Jaringan Nirkabel (*Wireless Network*)

Jaringan nirkabel merupakan jenis jaringan yang tidak menggunakan media kabel sebagai sarana transmisi, melainkan memanfaatkan gelombang radio untuk melakukan komunikasi antar perangkat yang mendukung koneksi nirkabel. Teknologi ini umumnya beroperasi pada frekuensi 2,4 GHz (802.11 b/g/n/ac) atau 5 GHz (802.11 a/n/ac). Meskipun bersifat nirkabel pada sisi pengguna, infrastruktur inti (*backbone*) dari jaringan nirkabel umumnya tetap menggunakan media kabel dan didukung oleh satu atau lebih titik akses point sebagai penghubung antar perangkat dan jaringan utama. [11]

Berikut ini contoh dari jaringan nirkabel yang ditunjukkan pada Gambar II.10



Sumber: [11]

Gambar II. 10 Jaringan Nirkabel

C. Perangkat Keras Jaringan Komputer

Perangkat keras jaringan komputer secara umum merupakan kumpulan komponen fisik yang memiliki fungsi dan peran yang berbeda-beda, yang digunakan sebagai sarana untuk menghubungkan beberapa komputer dalam suatu jaringan. Melalui koneksi yang terbentuk antar komputer tersebut, dimungkinkan terjadinya berbagai aktivitas seperti pertukaran data, berbagi informasi, pemanfaatan sumber daya bersama (*resource sharing*), serta pelaksanaan fungsi-fungsi jaringan lainnya.

Azhar [19] perangkat keras jaringan ialah perangkat yang dipakai untuk menghubungkan setidaknya dua PC dalam satu jaringan, sehingga setiap PC terkait dapat berbagi informasi, catatan, dan aset yang berbeda lainnya.

Berikut perangkat keras komputer serta fungsinya:

1. *Modem*

Modem (*Modulator Demodulator*) merupakan perangkat keras yang berfungsi untuk mengubah sinyal digital menjadi sinyal analog dan sebaliknya, agar data dapat ditransmisikan melalui media komunikasi seperti saluran telepon atau kabel. Ketika *modem* menerima sinyal analog dari penyedia layanan internet, perangkat ini akan mengubahnya menjadi sinyal digital yang dapat diproses oleh komputer. Dengan demikian, modem berperan sebagai penghubung antara komputer dengan jaringan internet, memungkinkan perangkat pengguna untuk terhubung dan melakukan komunikasi data secara daring. [13]

Berikut ini contoh dari modem yang ditunjukkan pada Gambar II.11



Sumber: [20]

Gambar II. 11 Modem

2. Router

Router adalah perangkat jaringan yang berperan dalam menghubungkan dua atau lebih jaringan yang berbeda, sehingga memungkinkan pertukaran data dan komunikasi antar jaringan tersebut. Keberadaan *router* sangat penting, karena tanpa perangkat ini, interkoneksi antar jaringan tidak dapat terwujud. [21]

Router memiliki beberapa fungsi utama dalam jaringan, yaitu: menghubungkan jaringan, mengarahkan paket data, mengelola akses, mengoptimalkan kinerja. [14]

Router juga berfungsi untuk membagi sebuah jaringan besar menjadi beberapa *subnetwork* yang lebih kecil. Setiap *subnetwork* tersebut bekerja seolah-olah terpisah atau terisolasi dari jaringan lainnya. Pemisahan ini memungkinkan pengelolaan lalu lintas data (*traffic*) yang lebih efisien, sehingga dapat meningkatkan performa dan stabilitas jaringan secara keseluruhan.

Berikut ini contoh dari router yang ditunjukkan pada Gambar II.12



Sumber: [12]

Gambar II. 12 Router

3. *Switch*

Switch merupakan perangkat keras jaringan yang berfungsi menghubungkan berbagai perangkat dalam suatu jaringan lokal. Perangkat ini berperan dalam mengatur lalu lintas data, sehingga data dikirim secara efisien ke perangkat tujuan yang tepat. Dengan penggunaan *switch*, komunikasi antar perangkat dalam jaringan menjadi lebih cepat dan terorganisir. [14]

Kapasitas sebuah *switch* ditentukan berdasarkan jumlah port yang dimilikinya, seperti 8, 16, atau 24 port. Semakin banyak jumlah port pada *switch*, maka semakin banyak perangkat atau komputer yang dapat terhubung ke dalam jaringan melalui perangkat tersebut. Dari segi fungsi dasarnya, *switch* dibedakan menjadi dua jenis yaitu *Unmanaged Switch* dan *Managed Switch*. *Unmanaged Switch* merupakan jenis *switch* yang dapat langsung digunakan tanpa memerlukan proses konfigurasi atau instalasi yang kompleks. Namun, kemudahan ini diimbangi dengan keterbatasan dalam fitur dan kapasitas jaringan, sehingga umumnya digunakan pada skala jaringan kecil.

Sedangkan *Managed Switch* menawarkan fleksibilitas yang lebih tinggi karena dapat dikonfigurasi secara menyeluruh, baik secara lokal maupun jarak jauh (*remote access*). Selain itu, *Managed Switch* juga mendukung kapasitas jaringan yang lebih besar serta memiliki fitur keamanan dan monitoring yang lebih lengkap, sehingga cocok digunakan pada lingkungan jaringan yang lebih kompleks dan berskala besar. [21]

Berikut ini contoh dari *Managed Switch* yang ditunjukkan pada Gambar II.13



Sumber : [12]

Gambar II. 13 *Managed Switch*

Berikut ini contoh dari *Unmanaged Switch* yang ditunjukkan pada Gambar II.14



Sumber : [20]

Gambar II. 14 *Unmanaged Switch*

4. *Access Point*

Dalam jaringan nirkabel, *Access Point* (AP) berfungsi sebagai titik sentral yang mengatur lalu lintas data antara perangkat klien dan jaringan utama melalui transmisi frekuensi radio. AP memungkinkan konektivitas *multipoint* dengan menampung sejumlah klien dalam satu segmen jaringan *wireless*, sehingga secara fungsional berperan layaknya *switch* atau *hub* pada jaringan berbasis kabel [7].

Berikut ini contoh dari *Access Point* yang ditunjukkan pada Gambar II.15



Sumber : [20]

Gambar II. 15 *Access Point*

5. *Network Interface Card* (NIC)

NIC adalah perangkat yang menghubungkan komputer ke jaringan. NIC terbagi menjadi dua jenis, yaitu fisik (seperti *Ethernet* dan *Token Ring*) dan logis (seperti *Loopback* dan *Dial-up Adapter* atau *network adapter*). [22]

Berikut ini contoh dari NIC yang ditunjukkan pada Gambar II.16



Sumber: [20]

Gambar II. 16 Network Interface Card (NIC)

6. Kabel

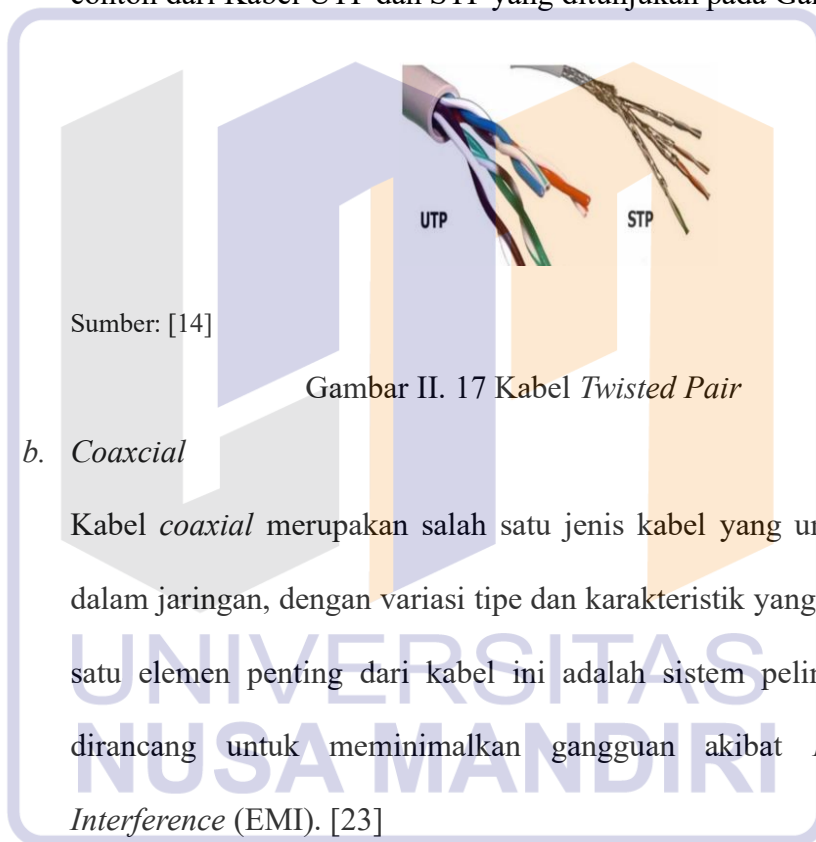
Dalam jaringan komputer, kabel berfungsi sebagai media transmisi yang penting untuk menghubungkan perangkat satu dengan lainnya, sehingga memungkinkan komputer untuk mengakses perangkat seperti printer atau scanner yang terhubung pada komputer lain dalam jaringan tersebut. [22]

Terdapat berbagai jenis kabel yang umum digunakan dalam pembangunan jaringan komputer, antara lain:

a. *Twisted Pair*

Kabel *Twisted Pair* merupakan jenis kabel yang terdiri dari beberapa pasang kabel yang saling terpilin satu sama lain. Pelintiran pada kabel ini bertujuan untuk mengurangi interferensi elektromagnetik, *noise*, serta gangguan sinyal yang dapat memengaruhi kualitas transmisi data. Terdapat dua jenis utama dari kabel twisted pair, yaitu *Unshielded Twisted Pair* (UTP) dan *Shielded Twisted Pair* (STP).

Kabel UTP tidak memiliki lapisan pelindung tambahan, sehingga lebih ringan dan fleksibel, sementara kabel STP dilengkapi dengan lapisan pelindung berupa *aluminium foil* untuk memberikan perlindungan ekstra terhadap interferensi. Kedua jenis kabel ini banyak digunakan dalam pembangunan jaringan lokal atau LAN, dengan pemilihan jenis kabel yang disesuaikan berdasarkan kebutuhan lingkungan jaringan. Berikut ini contoh dari Kabel UTP dan STP yang ditunjukkan pada Gambar II.17



Kabel *coaxial* merupakan salah satu jenis kabel yang umum digunakan dalam jaringan, dengan variasi tipe dan karakteristik yang beragam. Salah satu elemen penting dari kabel ini adalah sistem pelindungnya, yang dirancang untuk meminimalkan gangguan akibat *Electromagnetic Interference* (EMI). [23]

Kabel *coaxial* memiliki struktur yang terdiri dari dua konduktor yang dipisahkan oleh dua lapisan isolasi. Lapisan isolasi pertama membungkus inti tembaga sebagai konduktor utama, sementara lapisan kedua berupa anyaman serabut konduktor yang berfungsi sebagai pelindung terhadap gangguan elektromagnetik. [12]

Kabel *coaxial* memiliki struktur fisik berlapis, terdiri dari konduktor inti berbahan tembaga sebagai media utama penghantar data. Konduktor ini

dilapisi oleh *dielectric insulator* yang berfungsi sebagai penyangga dan penebat antara konduktor dengan lapisan pelindung logam (*metal shielding*). Lapisan pelindung tersebut, yang juga berfungsi sebagai *grounding*, membantu mengurangi interferensi sinyal dari luar. Seluruh komponen ini kemudian dibungkus oleh lapisan isolator luar guna memberikan perlindungan tambahan terhadap gangguan fisik dan lingkungan. Struktur berlapis ini memungkinkan kabel *coaxial* menghantarkan data dengan lebih stabil dan tahan terhadap gangguan elektromagnetik. Secara fisik, kabel *coaxial* memiliki kemiripan dengan kabel antena televisi, meskipun keduanya memiliki fungsi yang berbeda dalam penggunaannya. Pada ujung kabel *coaxial* biasanya dipasang konektor yang disebut *Bayonet Neill–Concelman* (BNC) untuk mendukung proses penyambungan ke perangkat jaringan. Berikut ini contoh dari kabel *coaxial* yang ditunjukkan pada Gambar II.18



Sumber: [14]

Gambar II. 18 Kabel *Coaxcial*

c. Fiber Optik

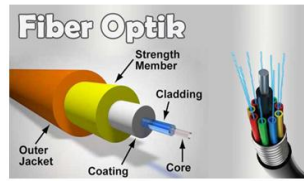
Menurut Silalahi [24] Kabel fiber optik merupakan jenis kabel terbaru dalam teknologi jaringan, yang menawarkan keunggulan dibandingkan jenis kabel lainnya. Kabel ini tersusun dari serat kaca yang mampu mentransmisikan data dengan kecepatan sangat tinggi serta menjangkau jarak transmisi yang luas, mulai dari lebih dari 500 meter hingga ratusan kilometer.

Komunikasi optik memiliki keunggulan dalam kemampuannya mengubah informasi menjadi sinyal listrik, kemudian dikonversi kembali menjadi sinyal optik atau cahaya. Sinyal ini ditransmisikan melalui serat optik, lalu diubah kembali menjadi sinyal listrik dan diterjemahkan menjadi informasi yang dapat dipahami. Berbeda dengan sistem komunikasi konvensional, di mana informasi langsung diubah menjadi sinyal listrik dan dikirim melalui kabel tembaga, sebelum akhirnya dikonversi kembali menjadi informasi di sisi penerima. [25]

Kabel ini sangat cocok digunakan pada lingkungan dengan tingkat interferensi tinggi dan untuk transmisi data jarak jauh. Fiber optik mampu mendukung kecepatan transmisi yang sangat tinggi, menjadikannya ideal untuk aplikasi yang memerlukan bandwidth besar, seperti video konferensi. Beberapa standar *Ethernet* yang menggunakan fiber optik antara lain *10BaseF*, *100BaseF*, dan *1000BaseF*. Konektor yang umum digunakan meliputi *ST connector* dan *SC connector*, dengan *SC* menjadi lebih populer karena kemudahan penggunaannya. Kabel ini umumnya digunakan pada jaringan skala besar dan sebagai tulang punggung (*backbone*) jaringan. Berdasarkan jalur transmisi cahaya, fiber optik dibedakan menjadi dua

jenis, yaitu *Single Mode* dan *Multi Mode*. Meskipun biaya instalasi dan perangkat pendukungnya relatif tinggi, tren penggunaan fiber optik terus meningkat seiring dengan menurunnya harga dan tingginya kebutuhan akan kecepatan akses data.

Berikut ini contoh dari kabel Fiber Optik yang ditunjukkan pada Gambar II.19



Sumber: [14]

Gambar II. 19 Kabel Fiber Optik

7. Konektor

Konektor berfungsi sebagai soket penghubung antara kabel UTP dengan antarmuka pada komputer, khususnya dalam jaringan komputer yang menggunakan media transmisi berbasis kabel UTP. [26]

Tanpa konektor, kabel jaringan tidak dapat terhubung dengan *network adapter* atau NIC. Pemilihan jenis konektor disesuaikan dengan tipe kabel yang digunakan. Konektor RJ45 digunakan untuk menghubungkan kabel UTP atau STP, sementara konektor BNC digunakan untuk kabel *coaxial*. Untuk kabel fiber optik, konektor yang digunakan adalah SC atau LC. Berikut ini contoh dari Konektor RJ45 yang ditunjukkan pada Gambar II.20



Sumber: [19]

Gambar II. 20 Konektor RJ45

Berikut ini contoh dari Konektor BNC yang ditunjukkan pada Gambar II.21



Sumber: [20]

Gambar II. 21 Konektor Bayonet Neill–Concelman (BNC)

Berikut ini contoh dari Konektor LC dan SC yang ditunjukkan pada

Gambar II.22



Sumber: [20]

Gambar II. 22 Konektor LC dan SC

D. IP Address

IP Address merupakan alamat logika yang diberikan kepada setiap perangkat dalam jaringan komputer agar dapat dikenali dan saling berkomunikasi. Alamat ini terdiri atas dua bagian utama, yaitu *network ID* yang menunjukkan identitas jaringan, dan *host ID* yang mengidentifikasi perangkat atau host di dalam jaringan tersebut.

Haffidz [27] alamat IP merupakan nomor identifikasi yang diberikan kepada setiap perangkat dalam jaringan yang menggunakan protokol *TCP/IP*. Setiap perangkat yang terhubung ke internet harus memiliki alamat IP yang unik agar tidak terjadi konflik dalam komunikasi data. Alamat IP versi IPv4 terdiri atas 32 bit yang dibagi menjadi empat oktet, masing-masing terdiri dari 8 bit. Dalam sistem pengalamatan *IP Address* dibagi ke dalam beberapa kelas berdasarkan ukuran jaringan dan jumlah host yang dapat ditampung. Berikut rinciannya:

1. *IP Address* kelas A diberikan untuk jaringan dengan jumlah host yang sangat besar. Range IP 1.xxx.xxx.xxx. – 126.xxx.xxx.xxx, terdapat 16.777.214 (16 juta) *IP Address* pada tiap kelas A. Pada *IP Address* kelas A, network ID ialah 8 bit pertama, sedangkan host ID ialah 24 bit berikutnya.
2. *IP Address* kelas B biasanya dialokasikan untuk jaringan berukuran sedang dan besar. Pada *IP Address* kelas B, network ID ialah 16 bit pertama,

sedangkan host ID ialah 16 bit berikutnya. Dengan panjang host ID 16 bit, network dengan *IP Address* kelas B dapat menampung sekitar 65000 host. Range IP 128.xxx.xxx – 191.255.xxx.xxx.

3. *IP Address* kelas C awalnya digunakan untuk jaringan berukuran kecil (LAN). Network ID adalah 24 bit pertama. Host ID ialah 8 bit terakhir. Dengan konfigurasi ini, bisa dibentuk sekitar 2 juta network dengan masing-masing network memiliki 255 *IP Address*. Range IP 192.0.0.xxx – 223.255.255.xxx.

Berikut ini tabel *IP Address* yang ditunjukkan pada Tabel II.2

Tabel II. 2 Tabel *IP Address*

Class	Oktet Pertama	Subnet Mask Default	Private Address
A	1-127	255.0.0.0	10.0.0.0 – 10.255.255.255
B	128-191	255.255.0.0	172.16.0.0 – 172.31.255.255
C	192-223	255.255.255.0	192.168.0.0 – 192.168.255.255

Sumber : [12]

Berikut adalah aturan-aturan dasar dalam menentukan *network ID* dan *host ID* yang digunakan:

1. *Network ID* tidak boleh sama dengan 127 *Network ID* 127 secara default digunakan sebagai alamat *loopback* yakni *IP address* yang digunakan oleh suatu komputer untuk menunjuk dirinya sendiri.
2. *Network ID* dan *host ID* tidak boleh sama dengan 255 *Network ID* atau *host ID* 255 akan diartikan sebagai alamat *broadcast*. ID ini merupakan alamat yang mewakili seluruh jaringan.

3. *Network ID* dan *host ID* tidak boleh sama dengan 0 *IP address* dengan *host ID* 0 diartikan sebagai alamat *network*. Alamat *network* digunakan untuk menunjuk suatu jaringan bukan suatu *host*.

Host ID harus unik dalam suatu *network*. Dalam suatu *network* tidak boleh ada dua *host* yang memiliki *host ID* yang sama.

2.3 Manajemen Jaringan

Manajemen jaringan (*Network Management*) merupakan serangkaian aktivitas yang bertujuan untuk mengelola, mengontrol, memantau dan mengoptimalkan infrastruktur jaringan agar tetap berjalan secara stabil dan efisien. Dalam lingkungan organisasi atau institusi pemerintahan, sistem manajemen jaringan memegang peranan penting dalam menjamin ketersediaan layanan, menjaga keamanan data dan mendukung efisiensi operasional harian.

Secara umum, manajemen jaringan dibagi ke dalam lima fungsi utama berdasarkan standar FCAPS (*Fault, Configuration, Accounting, Performance, and Security*) yang ditetapkan oleh ITU (*International Telecommunication Union*):

1. *Fault Management*

Tidak tersedia sistem pemantauan terpusat yang mampu mendeteksi dan memberikan notifikasi secara otomatis saat terjadi gangguan pada jaringan nirkabel. Gangguan baru disadari ketika pengguna mengalami masalah koneksi, sehingga proses penanganannya cenderung lambat.

2. *Configuration Management*

Access Point (AP) yang digunakan masih bersifat *standalone*, sehingga konfigurasi harus dilakukan satu per satu secara manual. Hal ini menyulitkan konsistensi konfigurasi antar perangkat dan memperbesar risiko kesalahan konfigurasi yang dapat berdampak pada performa jaringan.

3. *Accounting Management*

Tidak terdapat sistem pencatatan atau monitoring penggunaan jaringan oleh masing-masing pengguna. Hal ini menyulitkan dalam mengidentifikasi siapa yang menggunakan *bandwidth* berlebih atau melakukan aktivitas tidak sah di jaringan nirkabel.

4. *Performance Management*

Belum diterapkannya fitur *Quality of Service* (QoS) menyebabkan tidak adanya prioritas trafik. Akibatnya, saat terjadi lonjakan trafik, layanan penting seperti *video conference* atau akses ke aplikasi server internal dapat terganggu karena tidak adanya mekanisme pengaturan beban jaringan.

5. *Security Management*

Sistem keamanan jaringan masih bersifat dasar. Belum ada *firewall* yang terintegrasi dengan AP untuk memfilter lalu lintas, serta autentikasi pengguna hanya mengandalkan password Wifi umum yang dapat dengan mudah tersebar. Selain itu, ketika pengguna berpindah ruangan atau lantai, mereka harus memasukkan ulang kredensial, yang menunjukkan tidak adanya sistem roaming dengan manajemen keamanan yang kuat.

2.4 Konsep Penunjang Usulan

Penelitian ini bertujuan untuk penerapan *Quality of Service* (QoS) menggunakan Cloud Gateway guna meningkatkan kualitas layanan di Kantor Walikota Administrasi Jakarta Utara. Sistem ini diharapkan dapat mengoptimalkan pemanfaatan *bandwidth* yang disediakan oleh ISP untuk memenuhi kebutuhan operasional yang ada. Selain itu, penelitian ini juga bertujuan untuk mengoptimalkan penggunaan *Access Point* (AP) dengan fitur *roaming*, yang memungkinkan perangkat bergerak bebas tanpa kehilangan kualitas koneksi di seluruh area jaringan. Untuk

mendesain dan menganalisis topologi jaringan, Cisco Packet Tracer digunakan untuk mengambil dokumentasi topologi jaringan yang ada saat ini serta topologi jaringan yang diusulkan. Sementara itu, Unifi Dashboard akan digunakan untuk mensimulasikan implementasi jaringan yang baru, mengingat sebelumnya jaringan yang digunakan masih mengandalkan teknologi Wifi lama. Penelitian ini juga mencakup penguatan keamanan jaringan menggunakan *firewall* untuk memblokir akses klien ke situs web yang terlarang, sehingga menjaga integritas dan keamanan jaringan serta memastikan penggunaan internet yang sesuai dengan kebijakan yang telah ditetapkan.

A. Cisco Packet Tracer

Cisco Packet Tracer adalah sebuah media simulasi jaringan yang digunakan untuk merancang topologi jaringan berbentuk *software*. Cisco Paket Tracer adalah alat perangkat lunak jaringan komputer visualisasi dan simulasi yang kuat dapat diakses secara gratis oleh semua yang mendaftar di Cisco Network Academy.

B. Unifi Dashboard

UniFi Dashboard merupakan platform manajemen terpusat yang digunakan untuk memantau, mengelola dan mengoptimalkan infrastruktur jaringan nirkabel berbasis *Access Point*. Dalam usulan implementasi peningkatan kualitas jaringan di Kantor Walikota Administrasi Jakarta Utara, Unifi Dashboard menjadi alat penunjang utama karena kemampuannya dalam menyajikan data *real time* mengenai trafik jaringan, distribusi klien, kekuatan sinyal serta kestabilan koneksi antar titik akses.

Fitur-fitur seperti seamless roaming, pemantauan performa semua *Access Point* dan konfigurasi SSID tunggal mendukung efektivitas mobilitas pengguna di lingkungan kerja yang dinamis. Selain itu, dashboard ini juga menyediakan grafik lalu lintas jaringan dan laporan historis yang mempermudah analisis teknis dan

pengambilan keputusan berbasis data. Dengan integrasi ini, pengelolaan jaringan tidak hanya menjadi lebih efisien, tetapi juga responsif terhadap kebutuhan operasional harian di lingkungan pemerintahan.

C. Unifi Cloud Gateway

UniFi Cloud Gateway memiliki sejumlah fitur unggulan untuk pelaporan dan pengawasan aktivitas jaringan, seperti *firewall*, *Quality of Service* (QoS), serta fungsi manajemen jaringan yang terintegrasi. Kemampuan untuk melakukan konfigurasi *bandwidth* dan antarmuka pengguna yang intuitif menjadi salah satu pertimbangan utama dalam pemilihan perangkat ini untuk digunakan dalam infrastruktur jaringan. Dalam implementasinya, UniFi UDM dikolaborasikan dengan perangkat switch manageable dari Cisco, yang memiliki dukungan fitur VLAN (*Virtual Local Area Network*) guna memisahkan jaringan kabel dan jaringan nirkabel secara logis. Kombinasi ini bertujuan untuk meningkatkan efisiensi, keamanan dan keteraturan dalam pengelolaan jaringan. [28]

D. Wireshark

Dalam penelitian ini digunakan aplikasi Wireshark yang berfungsi untuk merekam lalu lintas jaringan secara real-time, termasuk mendukung analisis pada jaringan berbasis Wifi. Data hasil capture lalu lintas internet tersebut kemudian diolah dan dianalisis dengan mengacu pada standar TIPHON [29]. Standarisasi TIPHON dipilih sebagai acuan karena menyediakan parameter yang jelas untuk perhitungan, pengolahan data, serta penilaian kualitas jaringan Wifi yang ada di Kantor Walikota Jakarta Utara.