

## BAB II

### LANDASAN TEORI

#### 2.1. Tinjauan Jurnal

Sebagai landasan untuk mendukung penelitian ini, penulis menyajikan sejumlah jurnal ilmiah yang memiliki relevansi dengan topik yang dikaji.

1. Pada tinjauan jurnal yang pertama, Frihadi et al. membahas performa metode Per Connection Classifier (PCC) yang diterapkan pada perangkat MikroTik Router. Dalam penelitian tersebut, para penulis melakukan pengujian melalui simulasi menggunakan aplikasi Winbox untuk mengukur parameter performa jaringan seperti throughput, latency, jitter, dan packet loss. Hasil pengujian menunjukkan bahwa metode PCC mampu memberikan peningkatan performa yang signifikan, dengan capaian throughput sebesar 26,4 Mbps, latency rata-rata 18,2 ms, jitter 7,4 ms, serta tingkat packet loss sebesar 0,82%. Selain itu, penelitian ini juga menerapkan mekanisme failover otomatis menggunakan fitur Netwatch, yang terbukti menjaga kontinuitas layanan ketika jalur utama mengalami gangguan. Implementasi PCC dan Netwatch dalam penelitian tersebut menghasilkan distribusi trafik yang lebih seimbang dan koneksi yang lebih stabil dibandingkan kondisi sebelum konfigurasi diterapkan [4], yang menjadi fokus utama dalam implementasi manajemen jaringan di PT. ABB Sakti Industri.

2. Pada tinjauan jurnal yang kedua, “Mustofa dan Ramayanti membahas konfigurasi failover menggunakan fitur Netwatch pada Mikrotik RouterOS, dengan

tujuan menjaga konektivitas internet tetap aktif meskipun salah satu jalur ISP mengalami gangguan. Penelitian dilakukan melalui pendekatan studi kasus dan konfigurasi langsung pada perangkat Mikrotik, di mana Netwatch digunakan untuk memantau koneksi ke alamat IP tertentu dan mengeksekusi skrip failover ketika koneksi utama terdeteksi gagal. Hasil penelitian menunjukkan bahwa sistem failover dapat berfungsi dengan baik dan mampu mengalihkan koneksi secara otomatis dengan waktu eksekusi kurang dari lima detik, sehingga meningkatkan ketersediaan layanan internet secara signifikan.” [5], yang akan diterapkan dalam jaringan PT. ABB Sakti Industri untuk menjaga konektivitas saat terjadi gangguan.

3. Pada tinjauan jurnal yang ketiga, penelitian oleh Magfa et al. mengulas penerapan kombinasi Penerapan metode load balancing dan failover dalam infrastruktur jaringan korporasi menggunakan router Mikrotik sebagai solusi optimasi. Penelitian ini menggunakan metode eksperimen dengan pengujian parameter latency, throughput, dan uptime. Konfigurasi dilakukan dengan PCC untuk load balancing dan recursive routing untuk failover. Temuan penelitian menunjukkan adanya peningkatan kinerja jaringan yang signifikan, ditandai dengan penurunan nilai latency, peningkatan throughput, serta tingkat uptime yang mendekati 99% [6]. Temuan ini menunjukkan bahwa kombinasi metode load balancing dan failover terbukti meningkatkan keandalan jaringan, yang menjadi tujuan utama dalam implementasi sistem di PT. ABB Sakti Industri

## 2.2. Konsep Dasar Jaringan

### 2.2.1. Jaringan Komputer

Jaringan komputer merupakan sistem telekomunikasi yang memungkinkan komputer saling berinteraksi dan melakukan pertukaran data. Hal ini sejalan dengan pendapat MADCOMS (2015:2) yang menyatakan bahwa “jaringan komputer adalah sebuah sistem yang terdiri atas beberapa unit komputer yang didesain sedemikian rupa sebagaimana tujuan utamanya yakni untuk dapat berbagi sumber daya, berkomunikasi, dan dapat mengakses informasi”[7]. “Jaringan atau biasa disebut dengan *network* merupakan sistem pengoperasian yang menghubungkan beberapa perangkat komputer atau perangkat lain yang bisa terkoneksi dengan komputer. Jaringan komputer sendiri terdiri dari beberapa tipe, berbentuk fisik ada yang berbentuk nirkabel. Jaringan fisik artinya jaringan yang masih menggunakan benda fisik seperti kabel untuk melakukan koneksi. Contoh jaringan fisik adalah *Local Area Network* atau yang biasa disebut LAN. Selain LAN ada *Wide Area Network* atau WAN, WAN bisa mengcover lebih besar daerah namun biasanya kecepatannya lebih lambat karena jarak yang dibutuhkan untuk mengirim data sangat jauh.”[8]. Dalam model layanan jaringan, entitas yang mengajukan permintaan atau memperoleh layanan disebut sebagai *client*, dalam arsitektur jaringan, pihak yang memberikan atau mengirimkan layanan disebut *server*. Arsitektur ini dikenal sebagai sistem *client-server* dan diterapkan secara luas pada hampir seluruh aplikasi jaringan komputer.

“Jaringan atau biasa disebut dengan *network* merupakan sistem pengoperasian yang menghubungkan beberapa perangkat komputer atau perangkat lain yang bisa terkoneksi dengan komputer. Jaringan komputer sendiri terdiri dari beberapa tipe, berbentuk fisik ada yang berbentuk nirkabel”[9].

Awal mula jaringan komputer terjadi pada 1940-an di Amerika Serikat, ditandai dengan pengembangan komputer MODEL I oleh Bell Labs dan riset Universitas Harvard yang dipimpin Howard Aiken. Konsep tersebut dirancang untuk memungkinkan pemrosesan bersama pada satu komputer, yang dikenal sebagai *Batch Processing*. Memasuki era 1950-an, seiring perkembangan teknologi komputer hingga terciptanya superkomputer, muncul konsep distribusi proses berbasis waktu yang disebut *Time Sharing System (TSS)*, yang memungkinkan satu komputer melayani banyak terminal secara simultan. Perkembangan ini menjadi tonggak awal penerapan jaringan komputer.

### 2.2.2. Skala Jaringan Komputer

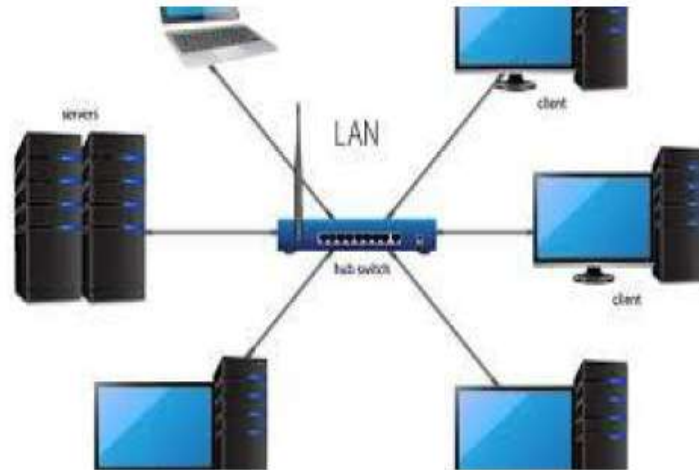
Konsep skala jaringan komputer merujuk pada ukuran atau cakupan jaringan, mulai dari skala kecil seperti jaringan lokal hingga skala besar seperti jaringan global yang meliputi wilayah geografis yang luas[10]. Secara umum, terdapat beberapa kategori skala jaringan komputer, antara lain:

#### 1. LAN (*Local Area Network*)

*Local Area Network (LAN)* merupakan jaringan komputer yang menghubungkan sejumlah perangkat dalam area terbatas seperti kantor atau gedung. Menurut modul resmi Laboratorium Komputer Fakultas Teknik Universitas Pancasila, "*Local Area Network (LAN)* adalah sejumlah komputer yang saling dihubungkan bersama di dalam satu areal tertentu yang tidak begitu luas, seperti di dalam satu kantor atau gedung. Secara garis besar terdapat dua tipe jaringan atau LAN, yaitu jaringan Peer to Peer dan jaringan *Client-Server*." [11]. Pada LAN tipe *Peer-to-Peer*, setiap komputer dapat berfungsi sebagai *server* sekaligus *workstation*, sedangkan pada tipe *Client-Server*, satu komputer bertindak sebagai *server* dan perangkat lain berperan sebagai

*workstation*. [11] LAN merupakan jaringan komputer yang beroperasi dalam area terbatas untuk memungkinkan komunikasi antar perangkat. Area cakupan LAN dapat berupa satu ruangan, antar ruangan dalam satu gedung, atau antar gedung dalam wilayah tertentu. LAN juga didefinisikan sebagai sistem komunikasi komputer dengan jangkauan terbatas (tidak melebihi satu mil) yang memanfaatkan koneksi berkecepatan tinggi, berkisar antara 2 hingga 100 megabit per detik. Jenis jaringan LAN merupakan yang paling umum digunakan di lingkungan perkantoran, baik pada perusahaan berskala kecil maupun besar. Ini disebabkan karena jaringan jenis ini tidak terlalu sulit untuk diterapkan dan tidak terlalu mahal. LAN mendukung transmisi data berkecepatan tinggi dan umumnya digunakan dalam lingkup terbatas pada satu organisasi, dengan jarak yang relatif pendek serta menggunakan teknologi komunikasi yang seragam. Karena jaraknya pendek, kecepatan transmisi dapat lebih tinggi dibandingkan jaringan berbasis *circuit-switched*, meskipun perbedaan ini semakin berkurang. Adapun karakteristik utama LAN adalah sebagai berikut:

- a. Jarak antar terminal berada dalam lingkup yang relatif dekat.
- b. Biasanya dimiliki dan dikelola oleh satu entitas atau organisasi.
- c. Tidak menggunakan fasilitas jaringan telepon, sehingga kecepatan transmisi data tidak bergantung pada jaringan telekomunikasi tersebut.
- d. Memanfaatkan media kabel khusus untuk komunikasi berkecepatan tinggi (1 Mbps hingga 10 Mbps), dan saat ini banyak organisasi yang telah beralih ke teknologi transmisi nirkabel (Wireless LAN).



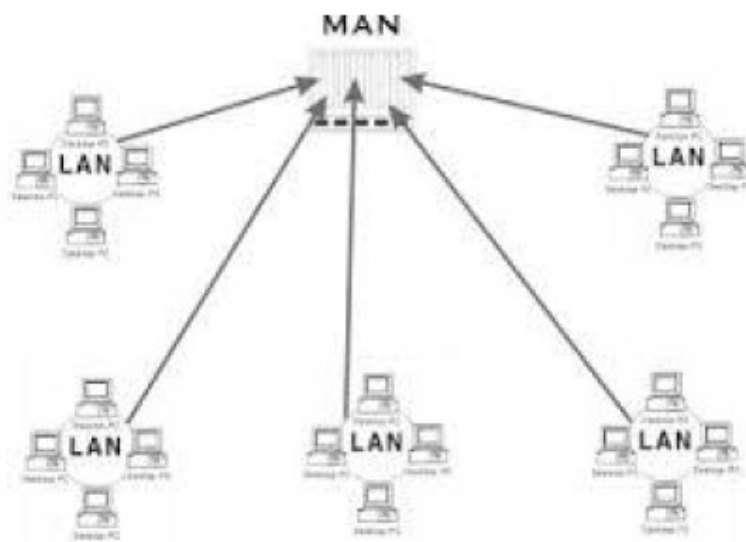
Sumber: [12]

Gambar II.1 Jaringan LAN

## 2. MAN (*Metropolitan Area Network*)

“MAN adalah jenis jaringan komputer yang memiliki cakupan area operasi dalam satu wilayah metropolitan, biasanya satu kota. Jaringan komputer MAN tersusun dengan menghubungkan sejumlah jaringan LAN yang berada dalam satu wilayah besar...” Dengan demikian, MAN memungkinkan koneksi antar lokasi seperti perkantoran, kampus, atau instansi pemerintah dalam satu kota menggunakan media transmisi berkecepatan tinggi seperti serat optik, koneksi koaksial, atau teknologi nirkabel [13]. MAN merupakan jaringan komputer yang beroperasi pada skala metropolitan, bertujuan untuk mengonsolidasi beberapa LAN menjadi jaringan yang lebih komprehensif. MAN dirancang untuk mengintegrasikan jaringan di area metropolitan, seperti perkantoran, instansi, atau kampus dalam satu kota. Dengan memanfaatkan MAN, berbagai sumber daya seperti server, printer,

dan koneksi internet dapat digunakan bersama, sehingga meningkatkan efektivitas komunikasi data. Umumnya, jaringan ini mengandalkan teknologi berkecepatan tinggi, seperti serat optik atau koneksi nirkabel, guna menjamin kecepatan transmisi. Konsep MAN dapat digambarkan seperti hubungan jaringan antara kantor pusat dan kantor cabang yang berada dalam satu kota, di mana MAN berperan sebagai penghubung utama dan LAN sebagai jaringan lokal di masing-masing cabang. MAN memungkinkan integrasi dan pertukaran data antar LAN melalui koneksi nirkabel atau kabel serat optik. Contoh penerapan MAN dapat ditemukan pada lingkungan kampus yang memiliki beberapa gedung terpisah dalam satu kota, di mana setiap gedung memiliki LAN yang saling terhubung untuk berbagi sumber daya. Penerapan serupa juga terdapat pada institusi perbankan yang menghubungkan kantor pusat dengan sejumlah kantor cabang dalam satu wilayah metropolitan. Dengan menggunakan jaringan MAN, kantor pusat dapat terhubung dengan kantor cabang, memungkinkan transmisi data yang mudah dan efisien antara mereka.



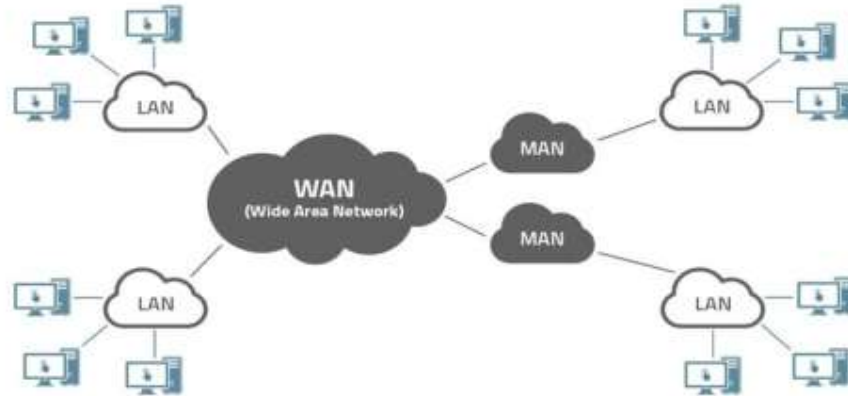
Sumber: [12]

Gambar II.2 Jaringan MAN

### 3. WAN (*Wide Area Network*)

“*Wide Area Network* atau WAN adalah jaringan komputer yang beroperasi dengan cakupan area yang luas. Jaringan WAN biasanya menghubungkan beberapa jaringan dengan cakupan area yang lebih kecil seperti *Local Area Network* (LAN).

WAN bisa mencakup wilayah yang lebih luas, seperti koneksi ke kantor pusat perusahaan, kantor cabang, layanan *cloud*, dan lainnya. WAN memungkinkan pengguna untuk mengakses berbagai sumber daya, seperti aplikasi, layanan penyimpanan, internet, dan sumber daya lain yang berlokasi jauh seperti dari kantor cabang ke kantor pusat.”[14]. *Wide Area Network* (WAN) merupakan infrastruktur jaringan area luas yang mengintegrasikan sejumlah *Local Area Network* (LAN) yang terpisah secara geografis dengan memanfaatkan media transmisi seperti serat optik, satelit, dan teknologi nirkabel. WAN memfasilitasi komunikasi antara pengguna atau perangkat yang berada di lokasi yang terpisah, termasuk antar kantor cabang, antara kota, negara, atau bahkan benua. Ini memungkinkan perusahaan atau organisasi untuk berbagi informasi, aplikasi, dan sumber daya komputasi di seluruh lokasi mereka dengan efisien. Salah satu contoh paling umum dari WAN adalah internet, yang menghubungkan jaringan dan perangkat di seluruh dunia.



Sumber: [12]

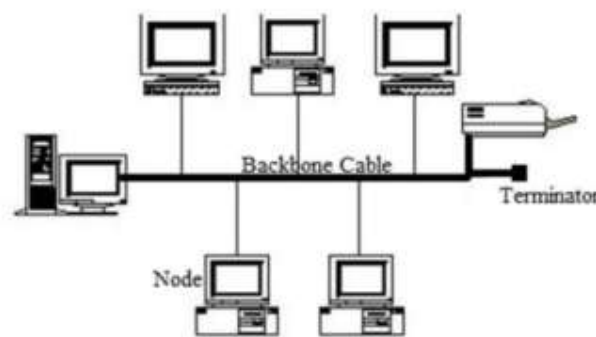
Gambar II.3 Jaringan WAN

### 2.2.3. Topologi Jaringan

“Topologi jaringan adalah pola hubungan antara *periferal-periferal* dalam suatu jaringan... Arus data yang mengalir juga sangat ditentukan kecepatan serta efisiensinya berdasarkan pola jaringan yang digunakan...” Dengan demikian, topologi jaringan berperan penting dalam menentukan bagaimana *node-node* seperti komputer, switch, maupun perangkat lainnya saling terkoneksi melalui media transmisi baik kabel (misalnya UTP atau serat optik) maupun nirkabel[15]. Topologi jaringan mengacu pada susunan fisik maupun logis dari perangkat dan koneksi dalam suatu jaringan komputer, yang mencakup cara perangkat saling terhubung serta aliran data di antara mereka. Topologi ini menentukan struktur keseluruhan jaringan dan mekanisme pengiriman data antar perangkat. Jenis-jenis topologi yang lazim diterapkan dalam perancangan jaringan meliputi bus, *star* (bintang), *ring* (cincin), *mesh* (jala), *tree* (pohon), serta konfigurasi *hybrid*, berikut variannya yang bersifat hierarkis seperti *extended star*. Setiap topologi memiliki keunggulan dan keterbatasan masing-masing, yang disesuaikan dengan kebutuhan spesifik jaringan.

## 1. Topologi *Bus*

Pada topologi ini, setiap simpul memiliki peluang yang sama untuk berkomunikasi dengan simpul lainnya. Ketiadaan simpul pusat sebagai titik kegagalan tunggal (*single point of failure*) menjadikan jaringan toleran gangguan; kerusakan pada satu simpul tidak menghentikan operasional jaringan secara keseluruhan. Namun, topologi ini memerlukan perangkat lunak yang lebih kompleks untuk mengelola kondisi ketika dua atau lebih simpul melakukan komunikasi secara bersamaan[16].



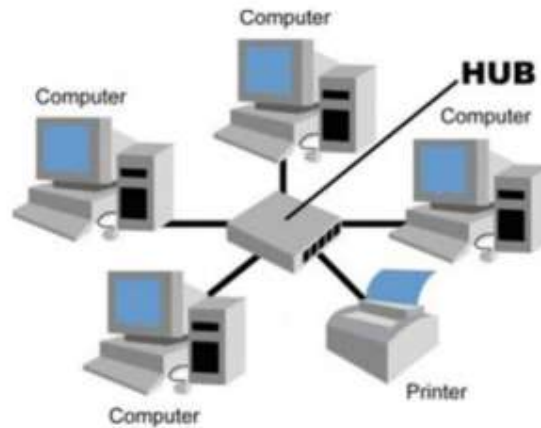
Sumber: [16]

Gambar II.4 Topologi *Bus*

## 2. Topologi *Star*

Topologi ini merepresentasikan susunan jaringan di mana sejumlah simpul (*node*) terhubung ke satu simpul pusat (*central/host node*), sehingga membentuk konfigurasi berbentuk bintang (*star topology*). Seluruh komunikasi dikendalikan oleh *node* pusat yang bertanggung jawab mengatur aliran informasi antar *node* lainnya. Apabila satu *node* ingin berkomunikasi dengan *node* lain, proses tersebut

harus melalui *node* pusat. *Node* pusat umumnya berupa komputer yang berfungsi sebagai terminal, komputer mini, atau komputer mikro yang terhubung melalui satu jalur[16].



Sumber: [8]

Gambar II.5 Topologi *Star*

Kelebihan topologi *star* terletak pada kemudahan pengelolaan dan pengendalian jaringan karena bersifat terpusat (*sentralisasi*). Namun, kelemahannya adalah apabila *node* pusat mengalami kerusakan, maka seluruh koneksi antar komputer tidak dapat berfungsi. Adapun beberapa kelebihan lain dari *topologi star* yang dapat memenuhi kebutuhan-kebutuhan pada suatu perusahaan pada saat ini dan sesuai dengan kondisi sistem yang sedang berjalan *diantaranya* :

- a. Kemampuan pengembangan yang tinggi

*Topologi star* merupakan topologi yang tidak kaku terhadap pengembangan jaringan dimasa yang akan datang, tanpa harus merusak atau mengganti sistem yang sedang berjalan.

b. Keandalan jaringan yang tinggi

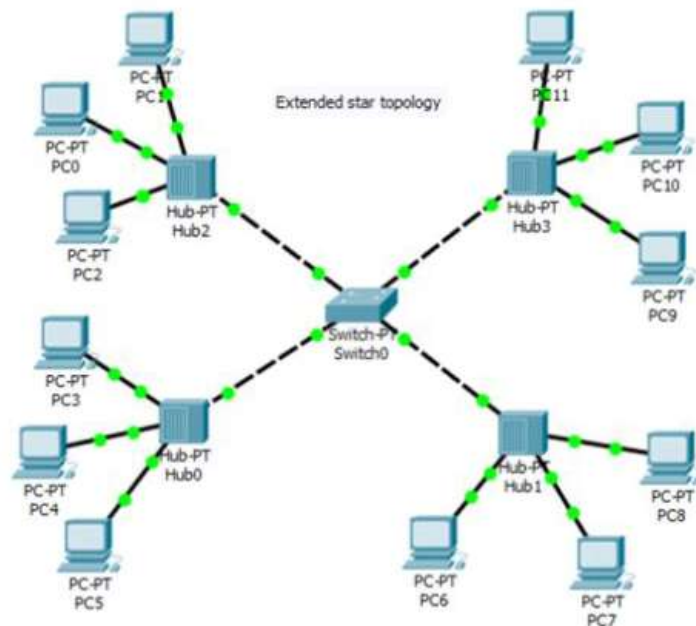
Topologi star memiliki tingkat keandalan yang tinggi, misalnya ketika terjadi gangguan pada salah satu *workstation*, hal tersebut tidak akan memengaruhi operasional *workstation* lainnya.

c. Keamanan data yang tinggi

Keamanan data akan terjaga karena yang mengetahui komunikasi antara dua *workstation* hanya komputer server, sedangkan *workstation* yang lainnya tidak mengetahui komunikasi antara dua terminal tersebut.

3. Topologi *Extended Star*

Topologi *extended star* merupakan varian hierarkis dari topologi *star*, yang memungkinkan penggunaan lebih banyak *hub* dan perangkat, bahkan hingga dua kali lipat dibandingkan topologi *star*. Karakteristiknya sepadan dengan topologi *star*: setiap *node* berkomunikasi langsung dengan *sub-node* pada tingkat di bawahnya, sementara *sub-node* meneruskan trafik menuju *central node*[16].

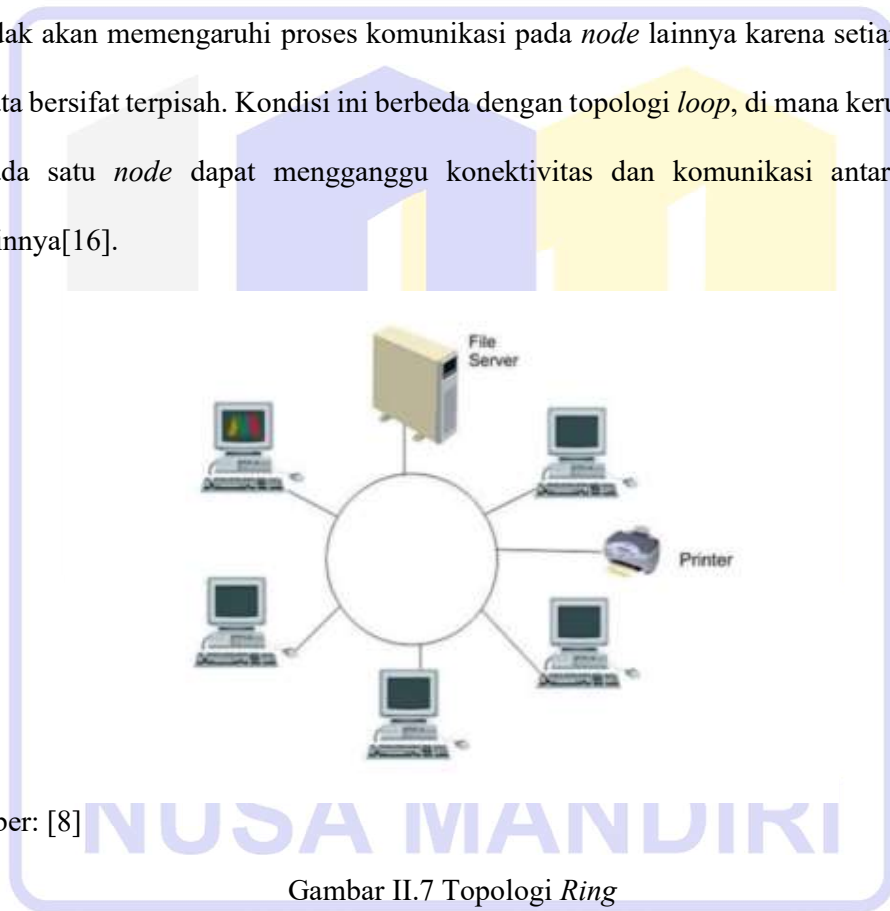


Sumber :[8]

Gambar II.6 Topologi *Extended Star*

#### 4. Topologi *Ring*

Topologi ini merupakan hibrida yang memadukan karakteristik *loop (ring)* dan *bus*. Jika salah satu node penghubung mengalami kegagalan atau kerusakan, hal tersebut tidak akan memengaruhi proses komunikasi pada *node* lainnya karena setiap jalur data bersifat terpisah. Kondisi ini berbeda dengan topologi *loop*, di mana kerusakan pada satu *node* dapat mengganggu konektivitas dan komunikasi antar *node* lainnya[16].



Sumber: [8]

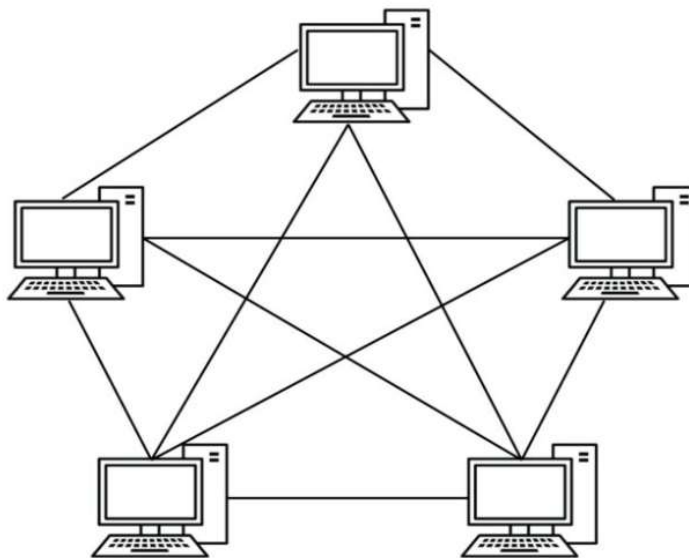
Gambar II.7 Topologi *Ring*

Kelebihan topologi *ring* terletak pada kemampuannya menjaga konektivitas antar *node*; apabila salah satu *node* mengalami kerusakan, hal tersebut tidak langsung mengganggu *node* lainnya karena setiap *node* terhubung melalui media transmisi bersama (*bus*) dan bukan secara langsung. Namun, kelemahan topologi ini adalah

apabila terjadi kerusakan pada *link* utama, seluruh *node* akan kehilangan fungsi komunikasi. Selain itu, pengelolaan kontrol jaringan menjadi lebih kompleks karena mekanisme pengendalian bersifat tersentralisasi.

#### 5. Topologi *Mesh*

Topologi *mesh* merupakan bentuk jaringan di mana setiap perangkat (*node*) memiliki koneksi langsung dengan seluruh perangkat lainnya dalam jaringan, sehingga membentuk struktur yang saling terhubung penuh (*full connectivity*). Tidak ada perangkat pusat yang mengatur aliran data, sehingga setiap perangkat memiliki koneksi langsung ke semua yang lain. Ini memungkinkan rute alternatif untuk mentransfer data jika ada masalah dengan jalur utama. Walaupun topologi *mesh* memberikan tingkat keandalan yang tinggi berkat adanya *redundansi* jalur komunikasi, biaya implementasinya relatif besar karena setiap perangkat harus memiliki koneksi langsung dengan seluruh perangkat lainnya. Topologi ini umumnya diterapkan pada jaringan yang menuntut keandalan tinggi, seperti pada sistem militer atau infrastruktur perbankan[16].

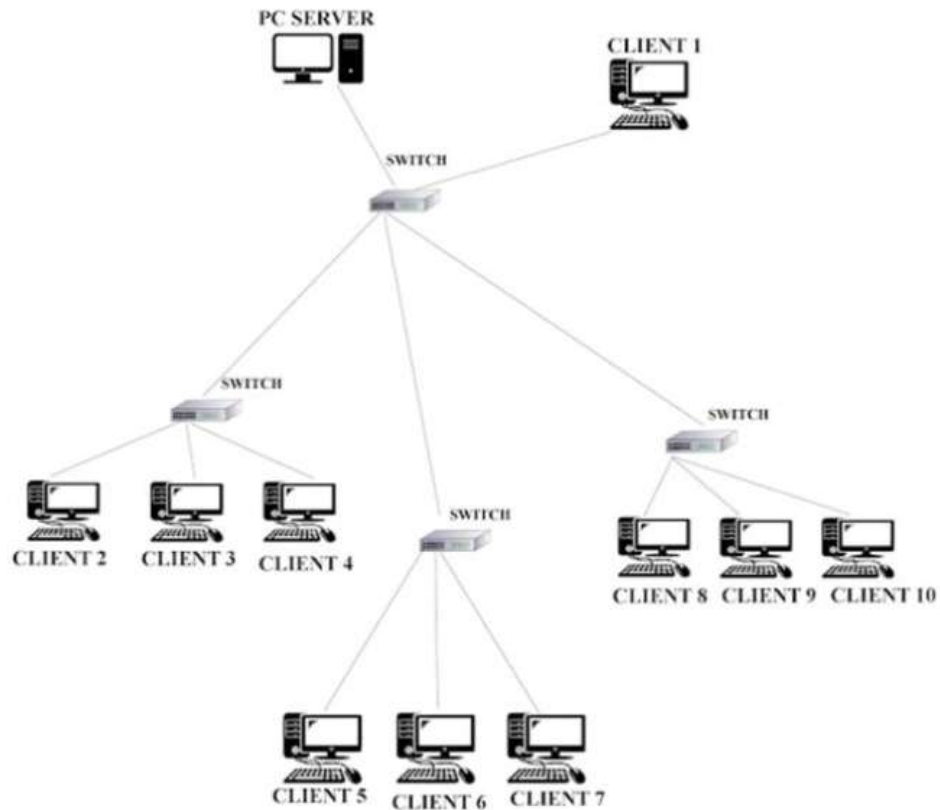


Sumber: [8]

Gambar II.8 Topologi Mesh

## 6. Topologi Tree

Topologi ini juga dikenal sebagai topologi pohon bercabang (*branched tree topology*), yang tersusun secara hierarkis dengan sebuah *central node* terhubung ke *node* lainnya secara berjenjang. *Central node* umumnya berupa komputer berkapasitas besar, seperti *mainframe*, yang berperan sebagai *host* pada tingkat hierarki tertinggi. Fungsinya sebagai simpul kendali yang mengoordinasikan dan mengendalikan node pada lapisan subordinat, yang dapat berwujud komputer mini (*minicomputer*) maupun komputer makro/*mainframe*[16].



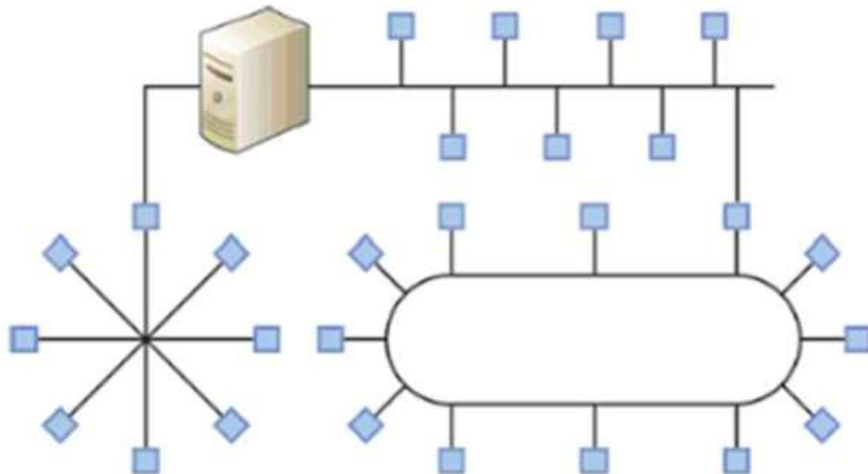
Sumber: [8]

Gambar II.9 Topologi *Tree*

Kelebihan topologi ini terletak pada kemudahan pengelolaan kontrol jaringan karena struktur hierarkis yang terpusat. Kelemahannya, bila terjadi kegagalan pada salah satu tautan/penghubung, maka seluruh node pada tingkat hierarki di bawahnya (*downstream*) akan kehilangan konektivitas/fungsi komunikasi.

### 7. Topologi *Hybrid*

Topologi hibrida (*hybrid*) adalah arsitektur jaringan yang mengombinasikan dua atau lebih jenis topologi yang berbeda. Contohnya, segmen ber-topologi *ring* diintegrasikan dengan segmen lain ber-topologi *star*, sehingga terbentuk struktur komposit hasil integrasi keduanya. Sebaliknya, penggabungan segmen dengan topologi yang sama tidak diklasifikasikan sebagai hibrida; misalnya, penggabungan dua segmen *bus* tetap disebut topologi *bus*[16].



Sumber: [8]

Gambar II.10 Topologi *Hybrid*

#### 2.2.4. Perangkat Pendukung Jaringan Komputer

“Perangkat Keras (*Hardware*) Jaringan Komputer adalah perangkat yang secara fisik dapat dilihat dan diraba, yang membentuk suatu kesatuan, sehingga dapat membangun sebuah jaringan komputer. Untuk dapat membangun sebuah jaringan komputer, ada beberapa perangkat keras jaringan komputer yang harus diketahui seperti NIC, Kabel Jaringan, Konektor, dan lain sebagainya.”[17]. Dalam proses pembangunan jaringan komputer, diperlukan sejumlah perangkat yang harus dipilih sesuai dengan kebutuhan dan skala jaringan yang akan diterapkan. Perangkat jaringan tersebut berperan menjamin konektivitas, menyelenggarakan pengelolaan data, serta mengoptimalkan efisiensi komunikasi antar *node* dalam jaringan. Secara umum, komponen yang digunakan untuk membangun jaringan komputer mencakup:

##### 1. Kabel Jaringan

Kabel jaringan merupakan media transmisi yang berfungsi sebagai media penghubung fisik antar alat dalam jaringan, misalnya komputer ke komputer, *hub* ke *hub*, maupun ke komputer. Peran utamanya adalah sebagai jalur lalu lintas data dalam jaringan. Selain itu, kabel jaringan juga menjadi indikator adanya koneksi fisik antara perangkat, khususnya antara PC (*Personal Computer*) dengan infrastruktur jaringan komputer.

Jenis kabel jaringan yang lazim digunakan dalam implementasi jaringan komputer meliputi beberapa kategori berikut:

##### a. Kabel *Twisted Pair*

Kabel *Twisted Pair* terdiri dari dua pasang kabel (total empat kabel, dan dapat lebih sesuai kebutuhan tertentu). Kabel ini terbagi menjadi dua jenis, yaitu *Shielded Twisted Pair* (STP) dan *Unshielded Twisted Pair* (UTP). STP

dilengkapi lapisan pelindung berbahan aluminium untuk mengurangi gangguan elektromagnetik (*Electromagnetic Interference* atau EMI), sehingga cocok digunakan pada jaringan dengan kinerja tinggi, seperti IBM *Token Ring*. Sebaliknya, UTP menggunakan konektor modular tipe telepon dan lebih rentan terhadap gangguan EMI. Untuk menjaga konsistensi impedansi dan resistansi serta meminimalkan interferensi, kabel UTP dijalin dengan pola enam lilitan per inci. Perlu dicatat bahwa jenis *Network Interface Card* (NIC) yang digunakan akan menentukan jenis kabel dan konektor yang sesuai.



Sumber: [12]

Gambar II.11 Kabel Twisted Pair

Untuk mempermudah pemakaian dan kebutuhan pemakai kabel UTP terbagi dalam beberapa kategori. Seperti diperlihatkan pada tabel II.1.

Tabel II.1 Kategori Kabel twisted Pair

Kategori	Kecepatan maksimal	Jarak Maksimal	Penggunaan Umum
CAT1	Hingga 1 Mbps	-	<i>Plain Old Telephone Service (POTS)</i>
CAT2	Hingga 4 Mbps	-	<i>10BASE-T Ethernet</i>
CAT3	Hingga 10 Mbps	100m	<i>10BASE-T Ethernet</i>
CAT4	Hingga 16 Mbps	100m	<i>10BASE-T Ethernet</i>
CAT5	Hingga 100 Mbps	100m	<i>Ethernet, Fast Ethernet</i>
CAT5e	Hingga 1 Gbps	100m	<i>Ethernet, Fast Ethernet &amp; Gigabit Ethernet</i>
CAT6	Hingga 10 Gbps	100m	<i>Gigabit Ethernet &amp; 10G Ethernet (55m)</i>
CAT6a	Hingga 10 Gbps	100m	<i>Gigabit Ethernet &amp; 10G Ethernet (55m)</i>
CAT7	Hingga 10 Gbps	100m	<i>Gigabit Ethernet &amp; 10G Ethernet (100m)</i>

Sumber: [12]

Kabel *Unshielded Twisted Pair* (UTP) terdiri atas delapan konduktor yang dipilin menjadi empat pasangan. Terminasi/penyusunan kabelnya umumnya mengikuti dua skema utama, yakni *straight-through* dan *cross-over*. Pola *straight-through* digunakan untuk menghubungkan perangkat berlainan jenis (mis. komputer ke *switch/router*), sedangkan pola *cross-over* dipakai untuk perangkat sejenis (mis. komputer-ke-komputer atau *switch-ke-switch*).

Konfigurasi *straight-through* diterapkan saat kabel digunakan untuk menghubungkan perangkat berlainan jenis, misalnya komputer (*host*) ke *hub* atau *switch*. Standar internasional untuk susunan *pin* pada konektor mengikuti pola lurus, yaitu: 1-1, 2-2, 3-3, 4-4, 5-5, 6-6, 7-7, dan 8-8. Dengan kata lain, setiap *pin* pada ujung pertama terhubung langsung ke *pin* yang sama pada ujung kedua.

Tabel II.2. Jenis Kabel UTP Fungsi *Straight*

<i>No</i>	Ujung 1 (Warna Kabel)	<i>No</i>	Ujung 2 (Warna Kabel)
1	Putih Orange	1	Putih Orange
2	Orange	2	Orange
3	Putih Hijau	3	Putih Hijau
4	Biru	4	Biru
5	Putih Biru	5	Putih Biru
6	Hijau	6	Hijau
7	Putih Coklat	7	Putih Coklat
8	Coklat	8	Coklat

Sumber: [12]

Konfigurasi *Cross-Over* menggunakan kabel *Unshielded Twisted Pair* (UTP) yang dilengkapi konektor RJ-45, dan berfungsi untuk menghubungkan perangkat sejenis, seperti komputer ke komputer atau *hub* ke *hub*. Standar internasional untuk susunan *pin* pada pola ini adalah: 1-3, 2-6, 3-1, dan 6-2,

sedangkan *pin* lainnya (4-4, 5-5, 7-7, 8-8) tetap terhubung lurus. Dengan demikian, pasangan kabel transmisi dan penerima ditukar untuk memungkinkan komunikasi dua arah.

Tabel II.3 Jenis Kabel UTP Fungsi *Cross*

<i>No</i>	<b>Ujung 1 (Warna Kabel)</b>	<i>No</i>	<b>Ujung 2 (Warna Kabel)</b>
1	Putih <i>Orange</i>	1	Putih Hijau
2	<i>Orange</i>	2	Hijau
3	Putih Hijau	3	Putih <i>Orange</i>
4	Biru	4	Biru
5	Putih Biru	5	Putih Biru
6	Hijau	6	<i>Orange</i>
7	Putih Coklat	7	Putih Coklat
8	Coklat	8	Coklat

Sumber: [12]

Dalam memasang kabel *Twisted Pair* dengan cara memasukkan kabel *Unshilded Twisted Pair* (UTP) lalu ditekan dengan menggunakan tang tersebut. Dalam proses instalasi kabel UTP pada konektor RJ 45, aspek yang harus diperhatikan adalah urutan kabel sesuai standar (lihat Tabel II.2 dan II.3), serta ketepatan saat melakukan penekanan menggunakan *crimping tool*. Penekanan yang tidak presisi dapat menyebabkan koneksi tidak optimal atau bahkan gagal berfungsi. Oleh karena itu, pastikan setiap kabel berada pada posisi yang benar sebelum proses *crimping* dilakukan.



Sumber: [12]

Gambar II.12 Tang Crimping

b. Kabel *Coaxial*

Kabel ini memiliki konduktor pusat berbahan tembaga, yang dipisahkan dari lapisan pelindung berupa anyaman tembaga oleh bahan dielektrik sebagai isolator. Dibandingkan kabel twisted pair, media ini berbiaya lebih tinggi, namun memberikan kualitas transmisi data yang secara signifikan lebih unggul. Kabel ini mampu mendukung kecepatan transfer data yang tinggi, serta dapat digunakan untuk sinyal analog dengan frekuensi tinggi. Selain itu, kabel ini memiliki *bandwidth* yang cukup besar sehingga ideal untuk transmisi data berkecepatan tinggi maupun sinyal video.



Sumber: [12]

Gambar II.13 Kabel *Coaxial*

Tabel II.4. Jenis Kabel *Coaxial* dan Penggunaannya

NO	JENIS KABEL	DIGUNAKAN	IMPEDANSI
1	RG-8 dan RG-11	<i>Thick Ethernet</i> (10 base 5)	50 $\Omega$
2	RG-58	<i>Thick Ethernet</i> (10 base 2)	50 $\Omega$
3	RG-59	Kabel Antena TV dan <i>Broadband Ethernet</i>	75 $\Omega$
4	RG-62	<i>ARCnet</i> dan IBM SNA Network	93 $\Omega$

Sumber: [12]

Keuntungan menggunakan kabel *coaxial* :

- 1) Sangat tahan terhadap EMI (*Elektromagnetik Interference*).
- 2) Mendukung *Bandwith* yang besar.
- 3) Banyak pembuat teknologi jaringan menggunakan jenis kabel ini sehingga dapat memilih *Network Interface Card* (NIC) yang ada jika jika mempergunakan kabel ini.

Kerugian menggunakan kabel *coaxial* :

- 1) Meskipun cukup tahan terhadap EMI (*Elektromagnetik Interference*) akan tetapi tidak pada kondisi yang berat seperti di pabrik.
- 2) Karena ukuran yang sangat besar menjadi sulit untuk memasangnya.

c. Kabel serat optik (*Fiber Optic Cable*)

Saat ini terdapat upaya pemanfaatan cahaya sebagai media transmisi data, yang didorong oleh kemampuan pengiriman data dengan kualitas sangat tinggi serta kapasitas besar dalam satu kali transmisi, menggunakan media berukuran serupa dengan kabel *Twisted Pair* maupun kabel koaksial. Dari sisi teknologi, penerapan

ini tergolong berhasil, namun dari perspektif biaya, kabel jenis ini relatif mahal dan kurang ekonomis dibandingkan media lainnya. Sebagai media ber-*bandwidth* besar, kabel ini mampu menyalurkan *bit-rate* tinggi dan umum digunakan untuk telemetri suara, distribusi video, serta trafik data.

Kelebihan kabel serat optik (*fiber optic*) antara lain :

- 1) Memiliki *bandwidth* yang sangat besar, sehingga mampu mendukung transmisi data berkecepatan tinggi.
- 2) Tahan terhadap EMI (*Elektromagnetik Interference*).
- 3) Tidak mengeluarkan frekuensi radio, sinyal pada kabel *fiber optic* tidak akan mengganggu peralatan elektronik yang terdekat.

Kelemahan kabel serat optik (*fiber optic*) meliputi :

- 1) Biaya relatif tinggi, sehingga kurang ekonomis dibandingkan media transmisi lainnya.
- 2) Proses instalasi memerlukan peralatan khusus serta tenaga kerja yang berpengalaman dan terlatih, karena sifat kabel yang sensitif dan teknologi yang kompleks.
- 3) Tidak mendukung beberapa konfigurasi data tertentu, sehingga penerapannya terbatas pada sistem yang kompatibel dengan teknologi serat optik.

## 2. Modem

Modem (*modulator-demodulator*) merupakan perangkat yang berfungsi untuk mengonversi sinyal, baik sinyal listrik maupun sinyal lainnya, sehingga dapat digunakan dalam komunikasi data. Modem mampu menerjemahkan berbagai jenis

sinyal, seperti sinyal DC, sinyal analog, frekuensi radio, dan gelombang cahaya. Setiap modem menjalankan dua fungsi pokok, yakni modulasi dan demodulasi. Dalam sistem komunikasi data, diperlukan sepasang modem yang ditempatkan masing-masing pada sisi pemancar dan sisi penerima. Salah satu skema modulasi yang lazim diterapkan adalah modulasi frekuensi berbasis *Frequency Shift Keying* (FSK), di mana informasi biner dimetakan ke sinyal analog melalui penggeseran frekuensi pembawa pada nilai-nilai diskret. Sebagai contoh, jika frekuensi pembawa adalah 1700 Hz, maka bit biner “1” dikirim dengan frekuensi 1200 Hz, sedangkan bit biner “0” dikirim dengan frekuensi 2200 Hz. Proses demodulasi memetakan komponen frekuensi 1200 Hz sebagai simbol biner “1” dan 2200 Hz sebagai simbol biner “0”. Perlu ditekankan bahwa modem tidak menghasilkan data itu sendiri, melainkan berfungsi sebagai perangkat konversi yang mengubah sinyal biner dari komputer menjadi sinyal analog dan sebaliknya.



Sumber: [12]

Gambar II.14 Modem

### 3. *Switch*

*Switch* merupakan perangkat jaringan yang berfungsi untuk menghubungkan beberapa node dalam suatu jaringan. Berdasarkan arsitektur dasarnya, *switch*

diklasifikasikan menjadi dua, yakni *cut-through* dan *store-and-forward*. Pada mode *cut-through*, *switch* meneruskan *frame* segera setelah membaca alamat tujuan pada *header*, sehingga unggul dalam kecepatan (latensi rendah). Sebaliknya, *switch store-and-forward* melakukan pemeriksaan terhadap seluruh isi paket data sebelum diteruskan, sehingga membutuhkan waktu lebih lama. Namun, penggunaan *switch store-and-forward* memberikan keuntungan berupa alokasi *bandwidth* penuh (misalnya 10 Mbps) untuk setiap segmen jaringan.



Sumber: [12]

Gambar II.15.Switch

#### 4. HUB

Sebagai perangkat konsentrator, *hub* menghubungkan beberapa *node* pada satu titik pusat, sehingga struktur fisik jaringan terwujud sebagai topologi bintang. Dalam jaringan sederhana berbasis *hub*, satu *port* dialokasikan untuk komputer/server, sedangkan *port-port* lainnya digunakan untuk menghubungkan *client* atau *workstation*.



Sumber: [12]

Gambar II.16.Hub

Berdasarkan cara pengelolaannya, *Hub* diklasifikasikan menjadi dua kategori, yakni *Manageable Hub* dan *Unmanageable Hub*. *Manageable Hub* mendukung konfigurasi/pengelolaan melalui perangkat lunak khusus yang umumnya disediakan oleh pabrikan. Sebaliknya, *Unmanageable Hub* tidak menyediakan fitur manajemen berbasis perangkat lunak, sehingga pengaturan bersifat manual dan terbatas.

#### 5. NIC (*Network Interface Card*)

*Network Interface Card* (NIC)—juga dikenal sebagai *LAN card* atau kartu jaringan—merupakan komponen elektronik yang dipasang pada setiap komputer (baik server maupun klien) untuk menyediakan antarmuka fisik/logis guna terhubung ke jaringan. Pemilihan kartu jaringan harus disesuaikan dengan kecepatan koneksi yang diinginkan. Seiring perkembangan teknologi jaringan, tersedia berbagai merek dan tipe NIC, seperti 3Com, D-Link, dan ProLink. Berdasarkan jenisnya, NIC terbagi menjadi tipe standar dan tipe *combo*. NIC tipe standar hanya memiliki satu *port* untuk konektor RJ-45, sedangkan tipe *combo* dilengkapi dengan port tambahan seperti konektor BNC. Sebelum membeli NIC, tiga parameter kunci yang harus diperhatikan adalah tipe NIC, protokol komunikasi yang didukung, serta kesesuaian dengan media kabel yang digunakan.



Sumber: [12]

Gambar II.17 NIC (*Network Interface Card*)

### 2.2.5. TCP/IP

Alamat IP (*Internet Protocol address*) adalah deretan bilangan biner 32 bit yang dibagi menjadi empat oktet (masing-masing 8 bit). Alamat ini berfungsi sebagai pengidentifikasi unik bagi setiap *host* pada jaringan, sehingga setiap perangkat harus memiliki alamat unik agar dapat berkomunikasi dan bertukar data. Secara umum terdapat dua versi, yakni IPv4 (format 32 bit) dan IPv6 (format 128 bit). Fungsi IP *address* mencakup identifikasi perangkat, pengaturan rute data (*routing*) di internet, komunikasi antar perangkat, serta penyediaan layanan jaringan. Alamat IP dapat diperoleh secara dinamis melalui server DHCP atau ditetapkan secara statis oleh administrator jaringan.

### 2.2.6. *Subnet Mask Default*

Setiap jaringan memerlukan parameter *subnet* yang disebut *subnet mask* (atau *address mask/netmask*) untuk menetapkan batas antara bagian jaringan (*network*) dan bagian *host*. *Subnet* merupakan partisi dari *Network ID* yang membagi prefiks jaringan menjadi beberapa subjaringan berukuran lebih kecil. Tujuan utama dari pembagian ini adalah untuk mengurangi beban kerja jaringan, meningkatkan efisiensi pengelolaan, serta mengoptimalkan penggunaan alamat IP.

*Subnet* direpresentasikan dalam bentuk bilangan biner sepanjang 32 bit, contohnya 11111111.11111111.11111111.00000000 atau dalam notasi desimal 255.255.255.0. Pada *subnet mask*, seluruh bit yang merepresentasikan *Network ID* dikonfigurasi dengan nilai 1, sedangkan bit yang merepresentasikan *Host ID* dikonfigurasi dengan nilai 0.

*Subnet mask* berfungsi menetapkan batas antara *Network ID* dan *Host ID* sekaligus menentukan lokalitas alamat (*on-link vs. off-link*), yakni apakah suatu host

berada dalam jaringan lokal atau di luar jaringan tersebut. Jika *host* berada pada jaringan non-lokal, maka pengiriman paket data harus dilakukan melalui *router*. Oleh karena itu, *subnet mask* diperlukan untuk melakukan penyaringan (*filtering*) terhadap alamat IP dan paket data yang masuk maupun keluar dari jaringan. Pemilihan *subnet mask* ditentukan oleh jumlah *host* yang akan diakomodasi dalam suatu jaringan. Untuk membedakan kapasitas *host* yang tersedia, *subnet mask* diklasifikasikan ke dalam beberapa kelas, sebagaimana ditunjukkan pada Tabel II.5 berikut.

Tabel II.5. Kelas *Subnet Mask*

Kelas	<i>Subnet Mask</i>
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Sumber: [12]

### 2.2.7. *Network Address Translation* (NAT)

“*Network Address Translation* atau NAT membuat jaringan yang menggunakan alamat lokal (*private*), alamat yang tidak boleh ada dalam tabel *routing* Internet dan dikhususkan untuk jaringan lokal/intranet, dapat berkomunikasi ke Internet dengan jalan ‘meminjam’ alamat IP Internet yang dialokasikan oleh ISP. Dengan cara ini, alamat IP *privat* dalam jaringan dapat ditranslasikan menjadi alamat IP global sehingga memungkinkan perangkat lokal mengakses jaringan publik seperti Internet.”[18].

*Network Address Translation* (NAT) adalah mekanisme pada perangkat perbatasan (*router/gateway*) yang melakukan translasi alamat IP dari satu ruang alamat ke ruang alamat lain saat paket melewati perangkat tersebut. Tujuan utama NAT

adalah memungkinkan sejumlah perangkat dalam jaringan lokal menggunakan satu alamat IP publik untuk berkomunikasi dengan jaringan eksternal, seperti internet.

Melalui mekanisme NAT, alamat IP privat dari perangkat dalam jaringan lokal dikonversi menjadi alamat IP publik sebelum data dikirim ke jaringan eksternal. Setelah data balasan diterima, alamat IP publik tersebut diterjemahkan kembali ke alamat IP privat yang sesuai, kemudian diteruskan ke perangkat tujuan di dalam jaringan lokal.

NAT memiliki sejumlah fungsi utama, di antaranya menghemat penggunaan alamat IP dengan memungkinkan satu alamat IP publik digunakan oleh banyak perangkat dalam jaringan lokal, meningkatkan keamanan dengan menyembunyikan alamat IP asli perangkat dari jaringan eksternal, memfasilitasi konektivitas internet bagi perangkat lokal, mendukung mekanisme *load balancing*, serta mengatur akses terhadap sumber daya internet tertentu. NAT merupakan komponen krusial dalam infrastruktur jaringan modern dan telah diimplementasikan secara luas pada berbagai lingkungan jaringan.

#### **2.2.8. Domain Name System (DNS)**

*Domain Name System* (DNS) adalah sistem basis data terdistribusi di internet yang menyimpan informasi nama *host* dan nama *domain*. DNS menyediakan pemetaan alamat IP untuk setiap nama *host* serta merekam server yang berasosiasi dengan tiap *domain*, sehingga permintaan nama situs dapat dikonversi menjadi alamat IP dan mempermudah penemuan layanan maupun perangkat secara global.

### **2.3. Manajemen Jaringan**

“pengertian manajemen jaringan telekomunikasi adalah suatu proses dalam ‘managing’ segenap perangkat telekomunikasi yang menghubungkan pemakainya dengan pemakai lain, sehingga kedua pemakai tersebut dapat saling bertukar informasi.”[19]. Tujuan utama manajemen jaringan adalah memastikan jaringan mampu mendukung kebutuhan operasional organisasi secara berkelanjutan. Dalam implementasinya, manajemen jaringan mengacu pada model FCAPS yang mencakup lima fungsi pokok, yaitu *Fault*, *Configuration*, *Accounting*, *Performance*, dan *Security*:

#### **2.3.1. Fault Management (Manajemen Gangguan)**

Fungsinya adalah mendeteksi, mengisolasi, dan memperbaiki gangguan atau kesalahan yang terjadi pada jaringan. Sistem manajemen jaringan harus mampu memberikan notifikasi secara *real-time* saat terjadi gangguan, serta menyimpan *log* untuk analisis lebih lanjut.

#### **2.3.2. Configuration Management (Manajemen Konfigurasi)**

Melibatkan pengaturan dan dokumentasi konfigurasi perangkat jaringan seperti *router*, *switch*, dan *firewall*. Manajemen konfigurasi juga mencakup proses *backup* dan *restore* konfigurasi untuk menghindari kehilangan data akibat kesalahan atau kerusakan perangkat.

#### **2.3.3. Accounting Management (Manajemen Akuntansi)**

Berfungsi untuk mencatat dan mengelola penggunaan sumber daya jaringan oleh pengguna atau perangkat. Informasi ini dapat digunakan untuk keperluan audit, perencanaan kapasitas, dan pengendalian biaya operasional jaringan.

#### **2.3.4. Performance Management (Manajemen Kinerja)**

Fokus pada pemantauan dan pengukuran performa jaringan, seperti *throughput*, *latency*, dan *packet loss*. Data performa ini digunakan untuk mengidentifikasi potensi *bottleneck* dan melakukan optimasi jaringan.

#### **2.3.5. Security Management (Manajemen Keamanan)**

Fungsinya adalah melindungi jaringan dari akses tidak sah, serangan siber, serta potensi kebocoran data. Manajemen keamanan mencakup pengaturan *firewall*, enkripsi data, serta *otentikasi* dan otorisasi pengguna. Dalam konteks penelitian ini, manajemen jaringan diterapkan untuk mengelola dua koneksi ISP yang tersedia di PT. ABB Sakti Industri. Dengan menggunakan perangkat Mikrotik, metode *load balancing* dan *failover* dikonfigurasi untuk memastikan distribusi *trafik* yang merata dan ketersediaan koneksi internet yang tinggi. Manajemen konfigurasi dilakukan melalui antarmuka *Winbox*, sedangkan *monitoring* performa dan *fault management* dilakukan dengan fitur *Netwatch* dan log sistem Mikrotik. Implementasi manajemen jaringan diharapkan mampu meningkatkan efisiensi operasional serta meminimalkan risiko *downtime* akibat gangguan konektivitas.

#### **2.4. Konsep Penunjang Usulan**

Dalam penerapan manajemen jaringan dengan metode *load balancing* dan *failover* berbasis Mikrotik, terdapat sejumlah konsep teknis yang menjadi komponen utama dalam proses perancangan dan konfigurasi sistem.

*Load balancing* merupakan mekanisme distribusi trafik internet ke berbagai jalur koneksi (*multi-ISP*) guna mengoptimalkan *utilisasi bandwidth* serta mengurangi potensi kemacetan pada satu jalur. Dengan metode ini, tidak hanya satu jalur yang

bekerja penuh, tetapi semua jalur digunakan sesuai aturan pembagian. Tujuan utama *load balancing* adalah mengoptimalkan pemakaian *bandwidth* dan mengurangi *bottleneck* atau penghalang pada satu jalur.

*Failover* adalah mekanisme otomatis yang memastikan koneksi jaringan tetap berjalan ketika salah satu jalur utama mengalami gangguan. Dalam konteks Mikrotik, *failover* dilakukan dengan memantau status koneksi (biasanya melalui ping ke IP publik seperti 8.8.8.8). Jika jalur utama *down*, trafik akan dialihkan ke jalur cadangan tanpa *intervensi manual*. Tujuan utama *failover* adalah menjamin ketersediaan layanan dan meminimalkan *downtime* akibat gangguan ISP.

Konsep-konsep ini meliputi Mikrotik *RouterOS*, *Per Connection Classifier* (PCC), *Netwatch*, *Recursive Routing*, dan *Winbox*. Berikut penjelasan masing-masing konsep:

#### **2.4.1. Mikrotik RouterOS**

“Mikrotik *server* memiliki fitur yang sangat lengkap diantaranya : *Firewall* dan *Nat*, *Routing*, *Hotspot*, *Point to Point Tunneling Protocol*, *DNS server*, *DHCP server*, Manajemen *Bandwidth*, dan keamanan...” Dengan demikian, RouterOS bertindak sebagai *platform* jaringan yang mendukung *routing*, *firewall/packet filtering*, manajemen *trafik*, *VPN*, *hotspot*, serta layanan pendukung lainnya[20].

RouterOS memberikan fleksibilitas dan efisiensi bagi *administrator* jaringan dalam mengelola lalu lintas jaringan, termasuk dalam implementasi *load balancing* dan *failover*. Hal ini diperkuat oleh penelitian Putra et al. (2024) yang menjelaskan bahwa: “Penelitian ini dengan mengkonfigurasi meliputi *ip route*, *firewall filter*, *NAT*, *Mangle* untuk penandaan paket, *Queue (manajemen bandwidth)*, *bridge wireless*, *DHCP* dan *ip cloud DDNS* pada MikroTik. Hasil analisis menunjukkan bahwa konfigurasi

tersebut dapat dilakukan dengan baik, serta mampu mengelola performa jaringan internet secara optimal, termasuk dalam hal pembagian trafik, penanganan paket, dan pengaturan *bandwidth*.”[21]. Dengan demikian, RouterOS terbukti memiliki performa stabil dalam pengaturan trafik jaringan dan menjadi solusi ekonomis serta fleksibel untuk perusahaan skala menengah

#### **2.4.2. Per Connection Classifier (PCC)**

PCC (*Per Connection Classifier*) merupakan metode pada Mikrotik yang berfungsi mengelompokkan koneksi berdasarkan atribut tertentu, seperti alamat IP sumber, alamat IP tujuan, maupun nomor *port*. Dengan mekanisme ini, distribusi trafik dilakukan berdasarkan koneksi sehingga beban dapat dibagi secara merata ke beberapa jalur ISP. Hal ini sejalan dengan penelitian Gusrion et al. (2022) yang menjelaskan bahwa: “*the load balance technique [...] one of which is PCC (Per Connection Classifier). The PCC load balance and failover method [...] classify traffic based on connection attributes so that traffic can be consistently directed through the same gateway path, enabling stable distribution and preventing overload on one of the links.*”[22]. Dengan demikian, PCC menjaga konsistensi jalur koneksi sejak awal sehingga seluruh paket dalam satu koneksi tetap melewati *gateway* yang sama, membantu mencegah *bottleneck* dan meningkatkan efisiensi load balancing.

#### **2.4.3. Netwatch**

*Netwatch* merupakan fitur *monitoring* pada Mikrotik yang berfungsi memantau status koneksi menuju alamat IP tertentu dan mengeksekusi skrip secara otomatis apabila koneksi mengalami kegagalan. Fitur ini sangat penting dalam penerapan

*failover* karena mampu merespons gangguan secara *real-time* tanpa intervensi *manual*. Hal ini ditegaskan oleh Panggabean & Kuswanto (2023) yang menyatakan bahwa: “Metode ini menggunakan 2 Jaringan *Link* ISP [...] ISP kedua sebagai *Link Backup* [...] Secara otomatis *Link Backup* ini akan naik posisi untuk menggantikan jaringan pada *Link* Utama. Penggunaan metode ini sangat mudah dan berjalan otomatis setelah melakukan konfigurasi pada tahap awal pemasangan. Setelah tahap pemasangan, diketahui sistem *failover* dengan metode Netwatch ini berjalan dengan baik dan sebagaimana mestinya, serta dapat meminimalisir terjadinya *downtime* pada koneksi internet.”[23]. Dengan demikian, Netwatch efektif digunakan untuk mendeteksi kegagalan koneksi dan mengalihkan trafik ke jalur cadangan secara otomatis.

#### **2.4.4. Recursive Routing**

*Recursive routing* merupakan teknik *routing* pada Mikrotik yang digunakan untuk menentukan jalur terbaik berdasarkan status ketersediaan *gateway*. Dalam implementasi *failover*, teknik ini memungkinkan *router* memeriksa apakah *gateway* utama masih dapat dijangkau dan secara otomatis beralih ke *gateway* cadangan apabila terjadi gangguan. Hal ini sejalan dengan penjelasan Helmud dan Novianto (2019) yang menyatakan bahwa: “*Fail over is a technique that uses more than one internet gateway [...] and the method that can be used is the recursive gateway by defining check-gateways and differentiating distance values on each routing rule. This technique ensures automatic switching when the main link experiences disruption, making the backup link active without requiring manual intervention.*”[24]. Dengan demikian, recursive routing menyediakan mekanisme otomatis untuk menjaga kontinuitas koneksi dengan memanfaatkan rute default yang hanya dapat diakses melalui *gateway* yang sedang aktif

#### 2.4.5. Winbox

Sebagai klien manajemen berbasis GUI, Winbox memudahkan *administrator* dalam melakukan *konfigurasi* dan pengelolaan router MikroTik secara *visual*. Aplikasi ini banyak digunakan untuk keperluan *konfigurasi*, *monitoring*, serta *troubleshooting* tanpa perlu menggunakan *command line*. Dalam penelitian ini, Winbox menjadi alat utama dalam proses *konfigurasi load balancing* dan *failover* pada Mikrotik RouterOS. Hal ini sejalan dengan temuan Putri et al. (2025) yang menyatakan bahwa: “Penggunaan MikroTik dengan konfigurasi melalui Winbox memberikan kemudahan dalam pengelolaan jaringan secara *visual* dan terintegrasi. Sistem ini terbukti efektif dalam menciptakan jaringan WLAN yang aman, stabil, dan sesuai kebutuhan *operasional*.” [25]. Selain itu, Mikrotik mendukung pembuatan virtual access point yang memungkinkan beberapa SSID pada satu antarmuka fisik, sehingga akses jaringan dapat dipisahkan antara jaringan publik dan internal sesuai kebutuhan operasional.



UNIVERSITAS  
NUSA MANDIRI