

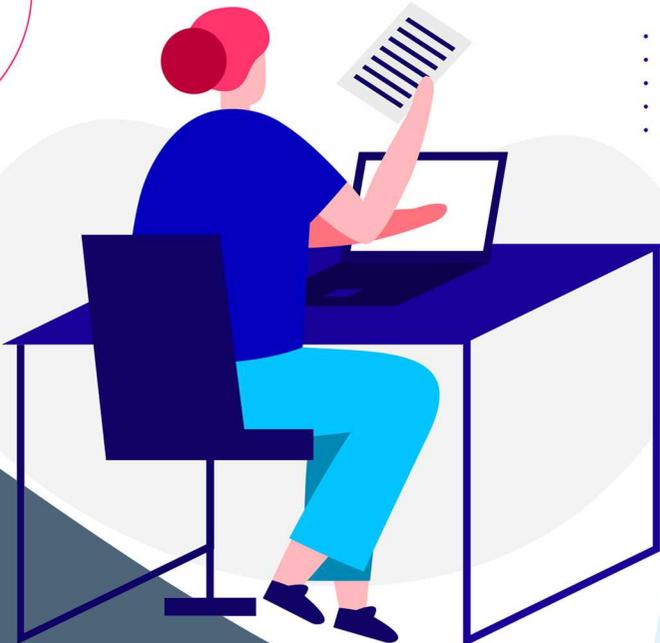


CV REY MEDIA GRAFIKA



PENGENALAN DASAR JARINGAN KOMPUTER

Nono Heryana, M.Kom - Moh. Erkamim, S.Kom., M.Kom
Afif Zuhri Arfianto, S.T. M.T - Ir. Dahlan Susilo, M.Kom
Firdhaus Hari S A H, ST., M.Eng - Farid Fitriyadi, S.Kom., M.kom
Wartono, S.Kom, M.Kom - Iwan Adhichandra, ST, MSc
Muhammad Hidayat, M.Kom - Dr. Irmawati, S.Kom., MMSI



PENGENALAN DASAR JARINGAN KOMPUTER

Disusun Oleh

Nono Heryana, M.Kom

Moh. Erkamim, S.Kom., M.Kom

Afif Zuhri Arfianto, S.T. M.T

Ir. Dahlan Susilo, M.Kom

Firdhaus Hari S A H, ST., M.Eng

Farid Fitriyadi, S.Kom., M.kom

Wartono, S.Kom, M.Kom

Iwan Adhicandra, ST, MSc

Muhammad Hidayat, M.Kom

Dr. Irmawati, S.Kom., MMSI



CV.REY MEDIA GRAFIKA

PUBLISHER

PENGENALAN DASAR JARINGAN KOMPUTER

Penulis:

Nono Heryana, M.Kom
Moh. Erkamim, S.Kom., M.Kom
Afif Zuhri Arfianto, S.T. M.T
Ir. Dahlan Susilo, M.Kom
Firdhaus Hari S A H, ST., M.Eng
Farid Fitriyadi, S.Kom., M.kom
Wartono, S.Kom, M.Kom
Iwan Adhicandra, ST, MSc
Muhammad Hidayat, M.Kom
Dr. Irmawati, S.Kom., MMSI

Penyunting:

Paput Tri Cahyono

Ukuran:

x hal + 229 hal; 14,8cm x 21cm

Diterbitkan Oleh:



CV.REY MEDIA GRAFIKA
PUBLISHER

Jln.Melati, BKG. Palapa, Blok.T No.6
Batam-Indonesia 29432
Email:reymediagrafika.rgm@gmail.com

ISBN: 978-623-88689-3-3

IKAPI: 010/Kepri/2022

Terbitan: Oktober 2023

Hak Cipta Pada Penulis

Hak Cipta dilindungi Undang-Undang

Dilarang Keras Memperbanyak Karya Tulis Ini Dalam Bentuk Dan Dengan
Cara Apapun Tanpa Seizin Dari Penerbit

KATA PENGANTAR

Syukur *alhamdulillah* penulis haturkan kepada Allah Swt. yang senantiasa melimpahkan karunia dan berkah Nya sehingga penulis mampu merampungkan karya ini tepat pada waktunya, sehingga penulis dapat menghadirkannya dihadapan para pembaca. Kemudian, tak lupa *shalawat* dan salam semoga senantiasa tercurah limpahkan kepada Nabi Muhammad Saw, para sahabat, dan ahli keluarganya yang mulia.

Dalam era teknologi informasi yang semakin berkembang pesat, pemahaman dasar tentang jaringan komputer menjadi sangat penting. Pengetahuan mengenai bagaimana data dan informasi dapat berpindah dengan cepat antar perangkat, baik dalam skala lokal maupun global, telah menjadi bagian tak terpisahkan dari kehidupan sehari-hari.

Buku ini, "Pengenalan Dasar Jaringan Komputer," disusun dengan tujuan untuk memberikan pemahaman dasar tentang konsep jaringan komputer kepada pembaca. Buku ini akan membantu pembaca memahami bagaimana jaringan komputer bekerja, jenis-jenisnya, serta manfaat dan tantangan yang terkait dengan penggunaan jaringan komputer.

Dalam Keperluan itulah buku berjudul **Pengenalan Dasar Jaringan Komputer** ini ditulis dalam upaya memberikan konstribusi bagi pemenuhan kebutuhan referensi yang berkaitan dengan kepentingan umum dan dunia pendidikan.

Penulis menyampaikan terima kasih yang tak terhingga bagi semua pihak yang telah berpartisipasi. Terakhir seperti kata pepatah bahwa” Tiada Gading Yang Tak Retak” maka penulisan buku ini juga jauh dari kata sempurna, oleh karena itu penulis sangat berterima kasih apabila ada saran dan masukan yang dapat diberikan guna menyempurnakan buku ini di kemudian hari.

Agustus 2023

Penulis

DAFTAR ISI

KATA PENGANTAR.....	iii
DAFTAR ISI	v
BAB I PENGENALAN DASAR JARINGAN KOMPUTER 1	
1.1. Definisi Jaringan Komputer	1
1.1.1. Pengertian Jaringan Komputer	1
1.1.2. Fungsi Jaringan Komputer	3
1.1.3. Keuntungan Jaringan Komputer.....	5
1.2. Sejarah dan Perkembangan Jaringan Komputer	7
1.2.1. Awal Mula Jaringan Komputer	7
1.2.2. Perkembangan Jaringan Komputer	9
1.3. Jenis-Jenis Jaringan Komputer	11
1.3.1. Berdasarkan Luas Geografis.....	11
1.3.2. Berdasarkan Teknologi Koneksi	17
1.4. Keuntungan dan Kelemahan Jaringan Komputer	24
1.4.1. Keuntungan Jaringan Komputer.....	24
1.4.2. Kelemahan Jaringan Komputer.....	26
1.5. Peran Jaringan Komputer dalam Dunia Digital	28
1.5.1. Perkembangan Teknologi Digital.....	28
1.5.2. Pengaruh Jaringan Komputer di Berbagai Bidang.....	31
1.5.3. Masa Depan Jaringan Komputer	33

BAB II PERANGKAT JARINGAN KOMPUTER.....	35
2.1. Pengertian dan Fungsinya.....	35
2.2. Perangkat Keras <i>End Device</i>	38
2.3. Perangkat Keras Intermediary Devices	41
2.4. Media Transmisi.....	46
2.5. Ringkasan Materi	53
BAB III ARSITEKTUR KOMPUTER.....	57
3.1. Pengantar ke Arsitektur Komputer	57
3.2. Sejarah Perkembangan Arsitektur Komputer .	57
3.3. Konsep Dasar Komputer	61
3.4. Sistem Bilangan dalam Komputer	65
3.5. Model Von Neumann.....	67
3.6. Arsitektur RISC vs. CISC.....	70
BAB IV JENIS-JENIS JARINGAN KOMPUTER.....	75
4.1. Jaringan Komputer Berdasar Jangkauan Area Jaringan	75
4.2. Jaringan Komputer Berdasar Jenis Transmisinya	82
4.3. Jaringan Komputer Berdasar Fungsinya	86
BAB V MEDIA TRANSMISI JARINGAN KOMPUTER ..	93
5.1. Kegunaan Media Transmisi	94
5.2. Media Transmisi Fisik	96
5.3. Media Transmisi Non-Fisik.....	100
BAB VI TOPOLOGI JARINGAN KOMPUTER	107
6.1. Deskripsi Topology Jaringan	107
6.2. Topologi BUS.....	108

6.3. Topologi Star	111
6.4. Topologi Ring	114
6.5. Topologi Mesh.....	116
6.6. Topologi Tree	119
BAB VII KONSEP DASAR PROTOKOL TCP/IP	123
7.1. Asal Mula TCP/IP.....	123
7.2. Relevansi TCP/IP di Era Modern	126
7.3. Model TCP/IP	129
7.4. Keamanan dalam TCP/IP.....	131
7.5. Masa Depan Protokol TCP/IP.....	135
BAB VIII KEAMANAN JARINGAN KOMPUTER.....	139
8.1. Definisi Keamanan Jaringan.....	139
8.1.1. Pentingnya Keamanan Jaringan.....	139
8.1.2. Ancaman dan Serangan Jaringan	140
8.2. Jenis-Jenis Ancaman.....	140
8.3. Prinsip Dasar Keamanan Jaringan	143
8.4. Teknologi Keamanan Jaringan.....	146
8.5. Manajemen Keamanan	149
8.6. Teknik Pertahanan dan Proteksi	152
8.7. Aspek Hukum dan Kepatuhan.....	154
8.7.1. Peraturan dan Undang-undang Terkait Keamanan Jaringan.....	155
8.7.2. Pelaporan Insiden Keamanan.....	155
8.8. Tantangan dan Trend Masa Depan	156
8.8.1. Keamanan di Era IoT (Internet of Things)	156

8.8.2.	Ancaman Baru dan Perkembangan Teknik Serangan.....	157
8.8.3.	Kecerdasan Buatan dalam Keamanan Jaringan.....	158
8.9.	Kesimpulan.....	159
BAB IX APLIKASI JARINGAN KOMPUTER.....		161
9.1.	Definisi Aplikasi Jaringan Komputer.....	161
9.2.	Peran Penting Aplikasi dalam Jaringan.....	161
9.3.	Sejarah Perkembangan Aplikasi Jaringan.....	164
9.4.	Aplikasi Web dan Layanan.....	167
9.5.	Aplikasi Kolaboratif.....	171
9.6.	Aplikasi Keamanan.....	174
BAB X KONSEP DASAR INTERNET		179
10.1.	Pengenalan Internet.....	179
10.2.	Protokol Internet.....	181
10.3.	Lapisan OSI (<i>Open Systems Interconnection</i>)..	184
10.4.	Arsitektur Internet.....	186
10.4.1.	Arsitektur Klien-Server.....	189
10.4.2.	Arsitektur Peer-to-Peer.....	192
10.5.	Layanan Internet.....	194
10.6.	Keamanan dan Privasi.....	199
10.6.1.	Ancaman Internet.....	202
10.6.2.	Privasi di Internet.....	204
10.7.	Masa Depan Internet.....	207
10.8.	Internet of Things (IoT).....	211
DAFTAR PUSTAKA.....		215

BAB I

Pengenalan Dasar Jaringan Komputer

1.1. Definisi Jaringan Komputer

1.1.1. Pengertian Jaringan Komputer

Jaringan komputer adalah kumpulan dua atau lebih komputer yang saling terhubung dan dapat saling berkomunikasi untuk bertukar informasi atau sumber daya seperti file, printer, dan perangkat lainnya (Forouzan, 2007). Dalam jaringan komputer, setiap komputer yang terhubung ke jaringan dapat berfungsi sebagai sumber daya atau pengguna, tergantung pada peran yang diberikan. Dalam sebuah jaringan komputer, setiap komputer dihubungkan dengan kabel atau nirkabel dan memiliki alamat unik yang disebut dengan alamat IP (Internet Protocol) untuk memudahkan pengiriman data (Kozierok, 2005).

Menurut Liu (2020), jaringan komputer juga dapat diartikan sebagai suatu sistem yang terdiri dari beberapa komputer yang dihubungkan dengan perangkat jaringan seperti kabel atau nirkabel.

Setiap komputer dalam jaringan tersebut dapat saling berkomunikasi, bertukar data dan informasi, serta memanfaatkan sumber daya yang ada di dalam jaringan tersebut.

Sedangkan menurut Tanenbaum (2011), jaringan komputer adalah sebuah kumpulan dari dua atau lebih komputer yang saling berhubungan satu sama lain dengan tujuan untuk saling bertukar informasi dan sumber daya. Dalam jaringan tersebut, terdapat perangkat jaringan yang berfungsi sebagai perantara atau penghubung antara komputer-komputer yang terhubung.

Dari beberapa definisi di atas, dapat disimpulkan bahwa jaringan komputer adalah kumpulan dari beberapa komputer yang saling terhubung dengan perangkat jaringan seperti kabel atau nirkabel, dan dapat saling bertukar informasi dan sumber daya. Jaringan komputer memungkinkan pengguna untuk berbagi data dan sumber daya seperti printer dan hard disk, sehingga dapat meningkatkan efisiensi dan produktivitas dalam suatu organisasi atau lingkungan kerja. Sebagai contoh, di sebuah perusahaan, karyawan dapat saling berbagi file dan mencetak dokumen dengan mudah tanpa harus menggunakan flashdisk

atau memindahkan file ke komputer lain. Jaringan komputer juga memungkinkan pengguna untuk berkomunikasi satu sama lain secara langsung, baik melalui pesan instan, email, atau video conference. Hal ini sangat membantu dalam mempercepat proses pengambilan keputusan dan kerja tim yang lebih efektif.

1.1.2. Fungsi Jaringan Komputer

Fungsi jaringan komputer adalah untuk memungkinkan pengguna untuk berbagi sumber daya seperti data, informasi, dan perangkat keras. Dalam sebuah jaringan komputer, sumber daya tersebut dapat dibagi dengan cara yang berbeda-beda, seperti berbagi file, printer, atau koneksi internet. Selain itu, jaringan komputer juga dapat digunakan untuk mengoptimalkan penggunaan sumber daya, meningkatkan efisiensi kerja, dan memudahkan koordinasi antara pengguna (Comer, 2014).

Secara umum, jaringan komputer memiliki beberapa fungsi yang sangat penting dalam mempermudah aktivitas sehari-hari dalam penggunaan teknologi informasi. Beberapa fungsi

jaringan komputer antara lain adalah sebagai berikut:

1. Berbagi Sumber Daya

Salah satu fungsi utama jaringan komputer adalah berbagi sumber daya antar komputer yang terhubung dalam jaringan. Sumber daya tersebut dapat berupa printer, scanner, hard disk, atau perangkat lain yang dapat diakses oleh seluruh pengguna dalam jaringan.

2. Komunikasi Data

Jaringan komputer juga berfungsi sebagai media komunikasi data yang memungkinkan pengguna untuk bertukar informasi antara satu sama lain dalam jaringan. Komunikasi data dalam jaringan komputer dapat dilakukan dengan menggunakan berbagai macam protokol, seperti TCP/IP, FTP, HTTP, dan lain-lain.

3. Akses Internet

Dengan adanya jaringan komputer, pengguna dalam jaringan dapat mengakses internet secara bersama-sama melalui satu koneksi internet yang terhubung ke jaringan. Dengan demikian, pengguna dalam jaringan dapat

saling berbagi informasi dan sumber daya yang diperoleh dari internet.

4. Peningkatan Keamanan

Jaringan komputer dapat digunakan untuk meningkatkan keamanan informasi dalam sebuah organisasi atau perusahaan. Dengan adanya jaringan komputer, perusahaan dapat mengimplementasikan berbagai teknologi keamanan, seperti firewall, VPN, dan IDS untuk melindungi informasi penting yang tersimpan dalam jaringan.

1.1.3. Keuntungan Jaringan Komputer

Keuntungan penggunaan jaringan komputer adalah terciptanya koneksi antarperangkat yang memungkinkan terjadinya pertukaran data dan informasi secara cepat dan efisien. Selain itu, jaringan komputer juga memberikan manfaat lain seperti:

1. Lebih efisien dalam penggunaan sumber daya seperti printer dan ruang penyimpanan data karena dapat digunakan bersama oleh semua perangkat yang terhubung ke jaringan.

2. Memungkinkan adanya komunikasi dan kolaborasi yang lebih baik antar anggota tim atau pengguna jaringan, baik secara lokal maupun jarak jauh.
3. Memudahkan akses ke sumber daya informasi dan aplikasi yang terpusat, seperti database dan program aplikasi yang dihosting di server jaringan.
4. Menyediakan akses internet yang terhubung ke dunia luar, sehingga memungkinkan pengguna jaringan untuk berinteraksi dan berkomunikasi dengan pengguna jaringan lain di seluruh dunia.
5. Meningkatkan keamanan dan privasi data karena dapat diatur pengaturan hak akses dan kontrol akses pada jaringan.
6. Lebih efisien dalam manajemen dan pemeliharaan infrastruktur jaringan karena dapat dilakukan secara terpusat dan otomatis.

Menurut Byrnes, dkk (2021), keuntungan utama dari penggunaan jaringan komputer adalah efisiensi dalam penggunaan sumber daya seperti printer dan penyimpanan data, serta memudahkan

komunikasi dan kolaborasi antar pengguna jaringan. Selain itu, Yigit, dkk (2014) menyatakan bahwa penggunaan jaringan komputer dapat meningkatkan produktivitas dan efektivitas bisnis karena memungkinkan akses terhadap sumber daya dan informasi yang terpusat.

1.2. Sejarah dan Perkembangan Jaringan Komputer

1.2.1. Awal Mula Jaringan Komputer

Jaringan komputer pertama kali muncul pada tahun 1960-an ketika para ilmuwan komputer di Amerika Serikat mulai mengembangkan jaringan yang terhubung antar komputer. Kantrowitz dan Rogers (1994) menjelaskan bahwa jaringan komputer pertama kali muncul pada tahun 1960-an ketika para ilmuwan komputer di Amerika Serikat mulai mengembangkan jaringan yang terhubung antar komputer. Pada awalnya, jaringan komputer dibuat untuk memudahkan pertukaran data antar para ilmuwan di lembaga-lembaga riset dan universitas yang terpisah geografis. Salah satu jaringan pertama yang dikembangkan adalah jaringan komputer ARPANET (Advanced Research Projects Agency Network) oleh Departemen Pertahanan AS pada tahun 1969.

Leiner et al. (1997) menjelaskan bahwa dengan adanya Internet, jaringan komputer menjadi semakin luas dan global. Berbagai teknologi dan standar jaringan seperti Ethernet, Wi-Fi, dan Bluetooth juga mulai dikembangkan untuk memungkinkan penggunaan jaringan secara nirkabel dan mudah diakses. Pada tahun 2000-an, jaringan komputer semakin berkembang pesat dengan adanya teknologi broadband yang memungkinkan transfer data yang lebih cepat dan stabil. Selain itu, pengembangan aplikasi dan layanan internet juga semakin meluas, seperti aplikasi media sosial, layanan streaming, dan e-commerce.

Stark (1997) menjelaskan bahwa dalam sejarah perkembangan jaringan komputer, terdapat beberapa tokoh yang berperan penting dalam mengembangkan teknologi jaringan, antara lain Bob Kahn dan Vint Cerf dalam pengembangan protokol TCP/IP, dan Tim Berners-Lee dalam pengembangan World Wide Web (WWW) pada tahun 1989. Dalam teknologi jaringan nirkabel, terdapat tokoh Guglielmo Marconi yang memperkenalkan teknologi radio pada awal abad ke-20, dan Martin Cooper yang menciptakan ponsel pertama pada

tahun 1973. Tahun 2000-an, jaringan komputer semakin berkembang pesat dengan adanya teknologi broadband yang memungkinkan transfer data yang lebih cepat dan stabil. Selain itu, pengembangan aplikasi dan layanan internet juga semakin meluas, seperti aplikasi media sosial, layanan streaming, dan e-commerce.

1.2.2. Perkembangan Jaringan Komputer

Perkembangan jaringan komputer telah mengalami evolusi yang signifikan selama beberapa dekade terakhir. Pada awalnya, jaringan komputer hanya digunakan secara terbatas dalam lingkup militer dan lembaga pemerintahan. Namun, seiring dengan perkembangan teknologi, jaringan komputer semakin populer dan digunakan secara luas di berbagai bidang.

Pada tahun 1960-an, jaringan komputer pertama kali digunakan oleh militer Amerika Serikat dengan tujuan untuk meningkatkan efisiensi komunikasi dan memperkuat pertahanan negara. Pada masa itu, jaringan komputer masih terbatas pada penggunaan kabel koaksial dan tidak dapat diakses oleh masyarakat umum.

Pada tahun 1970-an, ARPANET (Advanced Research Projects Agency Network) yang merupakan salah satu jaringan komputer awal mulai berkembang dan digunakan oleh lembaga akademik dan penelitian. ARPANET kemudian menjadi cikal bakal dari internet yang kita kenal saat ini.

Pada tahun 1980-an, jaringan komputer mulai digunakan oleh perusahaan dan industri dalam rangka meningkatkan efisiensi dan produktivitas. Pada masa ini, terjadi perkembangan teknologi jaringan komputer yang lebih cepat dan efisien seperti penggunaan protokol TCP/IP, penggunaan fiber optic, dan teknologi nirkabel.

Pada tahun 1990-an, internet mulai populer di masyarakat umum dan menjadi sarana komunikasi, informasi, dan bisnis yang sangat penting. Kemudian pada awal abad ke-21, jaringan komputer semakin berkembang dengan adanya teknologi cloud computing dan internet of things (IoT) yang memungkinkan pengguna untuk mengakses informasi dan layanan secara lebih mudah dan efisien.

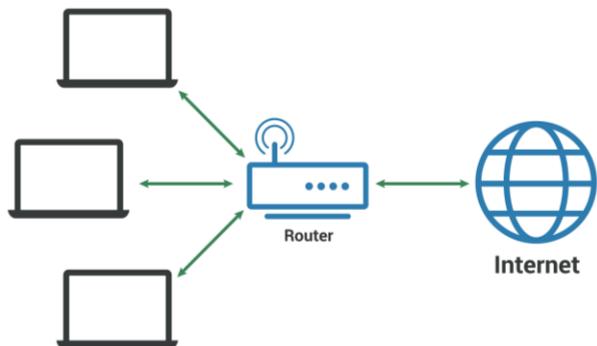
1.3. Jenis-Jenis Jaringan Komputer

1.3.1. Berdasarkan Luas Geografis

Dalam klasifikasi berdasarkan luas geografis, terdapat empat jenis jaringan komputer yang umum, yaitu Local Area Network (LAN), Wide Area Network (WAN), Metropolitan Area Network (MAN), dan Virtual Private Network (VPN).

a. Local Area Network (LAN)

Local Area Network (LAN) adalah jenis jaringan komputer yang mencakup area yang relatif kecil, seperti di dalam suatu gedung atau kampus universitas. LAN biasanya digunakan untuk menghubungkan beberapa komputer dalam satu area geografis yang sama sehingga memungkinkan komunikasi dan berbagi sumber daya antar komputer.



Gambar 1.1 Local Area Network (LAN)

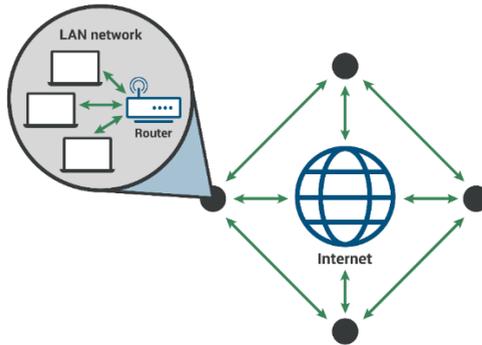
Menurut Nuaymi (2007), LAN adalah jaringan komputer yang mencakup area yang relatif kecil, biasanya di dalam satu gedung atau kampus universitas. Jaringan ini umumnya menggunakan kabel atau nirkabel untuk menghubungkan beberapa komputer dalam satu jaringan yang sama.

Komponen utama dalam sebuah LAN adalah komputer-komputer yang terhubung dalam jaringan tersebut dan perangkat jaringan seperti router dan switch yang digunakan untuk mengatur aliran data di dalam jaringan. LAN biasanya memiliki kecepatan transfer data yang lebih cepat dibandingkan dengan jaringan yang lebih luas seperti WAN (Wide Area Network).

Penggunaan LAN dapat meningkatkan efisiensi kerja dan produktivitas di lingkungan perkantoran karena memungkinkan berbagi sumber daya dan komunikasi antar komputer yang lebih mudah. Selain itu, LAN juga memungkinkan akses internet yang lebih cepat dan stabil bagi pengguna di dalam jaringan.

b. Wide Area Network (WAN)

Wide Area Network (WAN) adalah jenis jaringan komputer yang mencakup area yang sangat luas, biasanya mencakup area yang melintasi wilayah yang sangat besar seperti negara atau bahkan benua yang terhubung melalui jaringan publik. WAN dapat terdiri dari jaringan komputer yang terpisah dan terhubung melalui perangkat jembatan atau router.



Gambar 1.2 Wide Area Network (WAN)

Menurut Stallings (2016), WAN adalah jaringan yang terdiri dari dua atau lebih jaringan LAN yang terhubung dan terletak pada lokasi geografis yang berbeda. Salah satu contoh dari WAN adalah jaringan telepon yang digunakan untuk menghubungkan lokasi

yang berbeda melalui kabel telepon atau sinyal nirkabel.

WAN memiliki keuntungan yang signifikan dalam menghubungkan lokasi yang jauh secara geografis, yang memungkinkan perusahaan untuk beroperasi secara efisien di seluruh wilayah. Namun, WAN juga memiliki kelemahan, diantaranya biaya instalasi dan pemeliharaan yang tinggi, keamanan yang kurang dan juga ketergantungan pada kualitas jaringan publik.

c. Metropolitan Area Network (MAN)

Metropolitan Area Network (MAN) adalah jenis jaringan komputer yang meliputi area geografis yang lebih besar dari Local Area Network (LAN), namun lebih kecil dari Wide Area Network (WAN). MAN umumnya digunakan untuk menghubungkan beberapa LAN di area yang lebih luas, seperti kampus universitas atau perkantoran di sebuah kota. MAN memiliki kecepatan transfer data yang lebih cepat daripada WAN karena jarak antara komputer-komputer yang terhubung di MAN lebih dekat, dan menggunakan teknologi koneksi yang lebih canggih seperti serat optik.

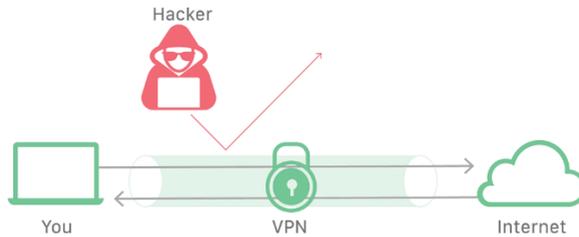
Sebagai contoh, sebuah MAN yang terdiri dari beberapa LAN di sebuah kampus universitas dapat memberikan kecepatan transfer data hingga ratusan gigabit per detik.

Salah satu contoh implementasi MAN adalah jaringan komputer yang menghubungkan kampus-kampus sebuah universitas. Sebuah studi yang dilakukan oleh Hernandez, dkk (2018) menunjukkan bahwa penggunaan MAN dalam sebuah universitas dapat meningkatkan efisiensi dan efektivitas sistem informasi universitas secara keseluruhan. Dengan adanya MAN, informasi dan data dapat dipertukarkan dengan cepat dan mudah antara berbagai fakultas dan departemen di universitas tersebut.

d. Virtual Private Network (VPN)

Virtual Private Network (VPN) merupakan salah satu jenis jaringan komputer yang saat ini semakin populer digunakan. VPN adalah jaringan yang memungkinkan pengguna untuk terhubung ke jaringan publik atau internet dengan cara yang aman dan terenkripsi. Dalam VPN, data yang ditransmisikan antara pengguna dan jaringan

publik akan dienkripsi, sehingga lebih sulit untuk diakses oleh pihak yang tidak berwenang.



Gambar 1.3 Virtual Private Network (VPN)

Menurut Khanvilkar dan Khokhar (2004), VPN merupakan solusi yang efektif dalam mengamankan transmisi data melalui internet, terutama bagi organisasi yang mengoperasikan jaringan di beberapa lokasi yang tersebar geografis. Dengan menggunakan VPN, organisasi dapat membuat jaringan pribadi virtual yang terhubung dengan internet, sehingga karyawan atau pengguna di lokasi yang berbeda dapat terhubung ke jaringan tersebut dengan cara yang aman dan terenkripsi.

Selain itu, penggunaan VPN juga dapat membantu melindungi privasi dan anonimitas pengguna saat berselancar di

internet. Sebagaimana yang dijelaskan oleh Pavlicek dan Sudzina (2018), dengan menggunakan VPN, pengguna dapat menyembunyikan alamat IP asli mereka dan memalsukan alamat IP dari lokasi lain, sehingga pengguna dapat mengakses konten yang dibatasi oleh geografis atau negara tertentu.

Namun, perlu diingat bahwa penggunaan VPN juga dapat memiliki kelemahan. Salah satunya adalah penggunaan VPN yang tidak tepat dapat mengurangi kecepatan akses internet. Selain itu, VPN juga rentan terhadap serangan DDoS (Distributed Denial of Service) yang dapat mengganggu koneksi internet dan aktivitas online pengguna (Kaur, dkk, 2019).

1.3.2. Berdasarkan Teknologi Koneksi

Dalam klasifikasi berdasarkan teknologi koneksi, jaringan komputer dapat diklasifikasikan menjadi tiga jenis, yaitu kabel (wired), nirkabel (wireless), dan media serat optik. Kabel atau jaringan kabel adalah jenis jaringan komputer yang menggunakan kabel tembaga atau kabel serat optik untuk menghubungkan antara satu perangkat

dengan perangkat lainnya. Jenis jaringan kabel yang umum digunakan adalah Ethernet. Nirkabel atau jaringan nirkabel, di sisi lain, menggunakan gelombang elektromagnetik untuk mengirimkan data antara perangkat. Contoh dari jenis jaringan nirkabel adalah Wi-Fi. Terakhir, media serat optik adalah jenis jaringan komputer yang menggunakan kabel serat optik sebagai media transmisi datanya.

a. Kabel (wired)

Kabel atau jaringan kabel merupakan salah satu teknologi koneksi jaringan komputer yang paling umum digunakan. Kabel digunakan untuk menghubungkan berbagai perangkat dalam jaringan komputer sehingga dapat saling berkomunikasi dan berbagi sumber daya. Berdasarkan jenis kabelnya, kabel jaringan komputer dapat dibagi menjadi beberapa jenis, antara lain:

1. Kabel Koaksial

Kabel koaksial adalah kabel jaringan yang memiliki inti tembaga yang dilapisi oleh isolator dan pelindung berupa anyaman logam. Kabel ini biasanya digunakan untuk menghubungkan perangkat dalam jaringan LAN dan memiliki kecepatan

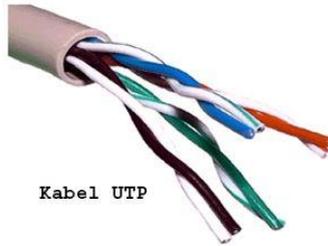
transfer data yang cukup tinggi. Keuntungan dari kabel koaksial adalah tahan terhadap gangguan elektromagnetik sehingga dapat meminimalkan kebisingan dalam transmisi data.



Gambar 1.4 Kabel Koaksial

2. Kabel UTP (Unshielded Twisted Pair)

Kabel UTP adalah jenis kabel jaringan yang terdiri dari dua hingga delapan pasang kawat yang dilapisi oleh isolator. Kabel UTP biasanya digunakan untuk menghubungkan perangkat dalam jaringan LAN dan memiliki kecepatan transfer data yang cukup tinggi. Keuntungan dari kabel UTP adalah mudah dalam penggunaannya dan memiliki harga yang relatif murah.



Gambar 1.5 Kabel UTP (Unshielded Twisted Pair)

3. Kabel STP (Shielded Twisted Pair)

Kabel STP memiliki karakteristik yang sama dengan kabel UTP, namun dengan pelindung berupa foil logam yang dilapisi pada setiap pasang kabel. Pelindung tersebut berfungsi untuk mengurangi kebisingan pada transmisi data dan meningkatkan keamanan jaringan. Kabel STP umumnya digunakan untuk menghubungkan perangkat dalam jaringan LAN dan memiliki kecepatan transfer data yang cukup tinggi.

Shielded twisted pair (STP)



Gambar 1.6 Kabel STP (Shielded Twisted Pair)

b. Nirkabel (wireless)

Nirkabel atau yang juga dikenal sebagai jaringan tanpa kabel adalah salah satu teknologi koneksi jaringan komputer yang semakin populer dan banyak digunakan dalam beberapa tahun terakhir. Teknologi nirkabel memungkinkan pengguna untuk terhubung ke jaringan komputer tanpa harus menggunakan kabel.

Menurut Mahendran (2016), teknologi nirkabel menggunakan gelombang elektromagnetik untuk mengirimkan data antara perangkat. Beberapa jenis teknologi nirkabel yang umum digunakan adalah Wi-Fi, Bluetooth, dan satelit. Teknologi Wi-Fi merupakan teknologi nirkabel yang paling populer dan biasa digunakan pada jaringan LAN di rumah atau kantor. Sedangkan teknologi Bluetooth biasanya digunakan untuk menghubungkan perangkat-perangkat seluler seperti smartphone dengan speaker atau headphone. Teknologi satelit digunakan untuk menghubungkan jaringan komputer di lokasi yang sulit dijangkau seperti di laut atau di pegunungan.

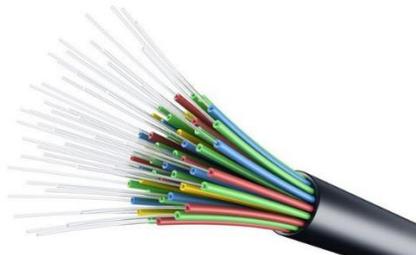
Penggunaan teknologi nirkabel memberikan beberapa keuntungan, antara lain kemudahan dalam menghubungkan perangkat, fleksibilitas dalam penggunaan perangkat, serta kepraktisan dan mobilitas yang tinggi (Zorzi, 2010). Menurut Hua dan Shunwaritu (2021), Teknologi nirkabel memungkinkan pengguna untuk mengakses jaringan dari mana saja dan kapan saja tanpa terbatas oleh kabel. Selain itu, teknologi ini juga memungkinkan pengguna untuk menghubungkan perangkat secara mudah dan cepat tanpa harus menginstal kabel yang rumit. Namun, teknologi nirkabel juga memiliki beberapa kelemahan seperti keamanan yang kurang terjamin dan kecepatan transfer data yang lebih lambat dibandingkan dengan teknologi kabel.

Dalam perkembangannya, teknologi nirkabel terus mengalami peningkatan kualitas dan kecepatan transfer data. Hal ini membuat teknologi nirkabel semakin populer dan digunakan dalam berbagai aplikasi seperti pengawasan lingkungan, sistem transportasi, serta aplikasi kesehatan (Khanh, dkk., 2022).

Namun, teknologi nirkabel juga memiliki beberapa kelemahan, seperti keamanan yang kurang dan rentan terhadap gangguan. Menurut Li dan Liu (2021), teknologi nirkabel rentan terhadap serangan cyber, seperti serangan hacker dan virus. Oleh karena itu, perlu adanya tindakan pencegahan dan perlindungan yang tepat untuk meminimalkan risiko keamanan.

c. Media Serat Optik

Media Serat Optik adalah salah satu teknologi koneksi jaringan komputer yang menggunakan kabel serat optik untuk mengirimkan sinyal data. Kabel serat optik terdiri dari serat optik yang sangat tipis dan fleksibel, yang terbuat dari bahan kaca atau plastik. Sinyal data dihasilkan dari cahaya yang dipancarkan melalui serat optik dengan menggunakan laser atau LED.



Gambar 1.7 Media Serat Optik

Keuntungan penggunaan media serat optik adalah kapasitas transmisi data yang sangat besar dan jangkauan yang lebih jauh dibandingkan dengan kabel tembaga. Selain itu, kabel serat optik juga lebih aman dan tahan terhadap interferensi elektromagnetik sehingga dapat mengurangi gangguan yang sering terjadi pada koneksi kabel tembaga.

Menurut Liu dan Deng (2020), penggunaan media serat optik dapat memberikan kecepatan transmisi data yang sangat tinggi dan dapat mengatasi masalah jangkauan dan keamanan pada koneksi jaringan. Namun, biaya pengadaan dan pemasangan kabel serat optik yang relatif mahal masih menjadi kendala utama dalam penggunaannya.

1.4. Keuntungan dan Kelemahan Jaringan

Komputer

1.4.1. Keuntungan Jaringan Komputer

Beberapa keuntungan jaringan komputer adalah kemampuan untuk saling berbagi sumber daya, informasi, dan data secara efektif dan efisien antara komputer-komputer yang terhubung dalam

jaringan. Keuntungan jaringan komputer secara detail sebagai berikut:

1. Kemampuan berbagi sumber daya

Jaringan komputer memungkinkan berbagai perangkat keras dan perangkat lunak, seperti printer, scanner, dan perangkat penyimpanan data (hard disk), dapat digunakan secara bersama-sama oleh banyak pengguna di dalam jaringan. Hal ini membantu menghemat biaya karena perangkat keras dan perangkat lunak tidak perlu dibeli dan dipasang pada setiap komputer secara terpisah.

2. Kemampuan berbagi informasi dan data

Dalam jaringan komputer, informasi dan data dapat dengan mudah dibagikan antara pengguna di dalam jaringan. Hal ini memungkinkan pengguna untuk berkolaborasi dan bekerja bersama-sama dalam pengembangan proyek atau tugas tertentu.

3. Kemampuan untuk meningkatkan efisiensi dan produktivitas

Dengan jaringan komputer, pengguna dapat mengakses dan menggunakan sumber daya

dan informasi secara lebih cepat dan mudah. Misalnya, pengguna dapat mencetak dokumen dari printer yang terhubung ke jaringan tanpa harus pindah-pindah ke setiap komputer. Hal ini dapat meningkatkan efisiensi dan produktivitas kerja.

4. Kemampuan untuk meningkatkan keamanan
Dalam jaringan komputer, administrator jaringan dapat mengelola dan memonitor penggunaan jaringan secara lebih efektif. Hal ini memungkinkan untuk meningkatkan keamanan dan mencegah akses tidak sah ke sumber daya dan informasi penting.

1.4.2. Kelemahan Jaringan Komputer

Kelemahan jaringan komputer dapat menjadi salah satu faktor yang mempengaruhi kinerja dan keamanan jaringan. Beberapa kelemahan jaringan komputer yang sering terjadi antara lain:

1. Keamanan: Jaringan komputer rentan terhadap serangan virus, worm, dan malware. Keamanan jaringan menjadi sangat penting untuk mencegah serangan tersebut dan melindungi data yang tersimpan di dalamnya (Graham, dkk, 2016).

2. Ketergantungan: Jaringan komputer membutuhkan perangkat keras dan perangkat lunak yang memadai. Ketergantungan pada perangkat keras dan perangkat lunak tersebut dapat menyebabkan gangguan jika ada kerusakan atau pembaruan sistem yang tidak dilakukan dengan benar (Buhagiar, 2018).
3. Kecepatan: Kecepatan jaringan sangat penting untuk memastikan transfer data yang cepat dan efisien. Namun, jaringan komputer dapat mengalami kecepatan rendah atau bahkan terputus jika ada gangguan pada kabel atau perangkat keras lainnya (Peterson & Davie, 2007).
4. Pengelolaan: Jaringan komputer yang kompleks membutuhkan pengelolaan yang baik dan terus-menerus. Jika pengelolaan tidak dilakukan dengan benar, jaringan komputer dapat mengalami masalah seperti kegagalan sistem dan kinerja yang buruk (Kizza, 2017).

Mengatasi kelemahan jaringan komputer membutuhkan upaya yang terus-menerus dan

harus dilakukan dengan baik. Keamanan jaringan dapat ditingkatkan dengan menggunakan perangkat lunak antivirus yang mutakhir dan teknologi firewall yang dapat mengawasi lalu lintas jaringan. Selain itu, perangkat keras yang berkualitas dan pengelolaan yang baik juga dapat membantu mengatasi kelemahan jaringan komputer (Buhagiar, 2018).

1.5. Peran Jaringan Komputer dalam Dunia Digital

Jaringan komputer memiliki peran penting dalam dunia digital. Perkembangan teknologi digital dan penggunaan internet telah mengubah cara orang berkomunikasi, bekerja, dan berinteraksi dengan dunia. Di bawah ini, akan dibahas lebih detail mengenai peran jaringan komputer dalam dunia digital, termasuk perkembangan teknologi digital, pengaruh jaringan komputer di berbagai bidang, dan masa depan jaringan komputer.

1.5.1. Perkembangan Teknologi Digital

Perkembangan teknologi digital sangat berpengaruh terhadap perkembangan jaringan komputer. Teknologi digital memungkinkan pengiriman dan penerimaan data secara lebih cepat

dan efisien melalui jaringan komputer. Selain itu, teknologi digital juga memungkinkan adanya inovasi baru dalam pengembangan jaringan komputer, seperti penggunaan teknologi nirkabel yang semakin populer.

Menurut Javaid, dkk. (2022), perkembangan teknologi digital telah memungkinkan terciptanya teknologi jaringan komputer yang semakin canggih dan efisien. Teknologi digital juga memungkinkan adanya penggunaan jaringan komputer yang lebih luas dan terintegrasi, seperti penggunaan internet dalam berbagai bidang seperti bisnis, pendidikan, dan hiburan. Menurut Evans dan Wurster (1997), perkembangan teknologi digital juga memungkinkan terciptanya bisnis baru yang berbasis pada jaringan komputer. Contohnya adalah bisnis online yang semakin berkembang dengan adanya teknologi e-commerce.

Internet adalah salah satu inovasi teknologi digital yang paling penting. Internet memungkinkan orang untuk berkomunikasi dan berbagi informasi di seluruh dunia dengan cepat dan mudah. Selain itu, internet juga telah mengubah cara orang bekerja, belajar, dan berbelanja. Menurut laporan yang diterbitkan oleh We Are Social dan Hootsuite

pada tahun 2021, ada sekitar 4,9 miliar pengguna internet di seluruh dunia, dan penggunaan internet terus meningkat setiap tahunnya (Fitriani, 2021).

Cloud computing juga telah mempengaruhi cara bisnis dan organisasi menyimpan, mengelola, dan mengakses data mereka. Dengan cloud computing, data dapat disimpan di server jarak jauh dan diakses dari mana saja dengan koneksi internet. Hal ini memungkinkan bisnis dan organisasi untuk bekerja secara efisien dan menghemat biaya infrastruktur IT.

Internet of Things (IoT) adalah konsep yang mengacu pada konektivitas antara objek-objek di dunia fisik dengan jaringan internet. Contoh dari aplikasi IoT termasuk kendaraan pintar, rumah pintar, dan kesehatan pintar. Dalam sistem IoT, objek-objek di dunia fisik dikumpulkan, dianalisis, dan diolah oleh jaringan komputer untuk memberikan informasi yang lebih baik dan meningkatkan efisiensi dalam pengambilan keputusan.

1.5.2. Pengaruh Jaringan Komputer di Berbagai Bidang

Jaringan komputer memiliki pengaruh yang sangat besar di berbagai bidang, seperti bisnis, pendidikan, hiburan, dan lain sebagainya. Dalam bidang bisnis, jaringan komputer memungkinkan perusahaan untuk berkomunikasi secara efektif dan efisien, baik dalam hal pertukaran informasi maupun transaksi bisnis. Dalam bidang pendidikan, jaringan komputer memungkinkan siswa dan guru untuk berinteraksi dan berbagi informasi dengan mudah melalui internet. Dalam bidang hiburan, jaringan komputer memungkinkan pengguna untuk mengakses berbagai jenis konten seperti musik, film, dan game dengan cepat dan mudah.

Salah satu contoh pengaruh jaringan komputer di bidang pendidikan adalah penggunaan Learning Management System (LMS) atau Sistem Manajemen Pembelajaran. LMS memungkinkan guru dan siswa untuk mengakses materi pelajaran, tugas, dan ujian secara online. Sebuah studi menunjukkan bahwa penggunaan LMS dapat meningkatkan keterlibatan siswa dan memudahkan guru dalam mengelola kelas (Nurakun Kizy, dkk., 2018).

Di bidang bisnis, penggunaan jaringan komputer juga memberikan banyak manfaat. Sebuah penelitian menunjukkan bahwa perusahaan yang mengadopsi teknologi jaringan komputer cenderung lebih inovatif dan memiliki tingkat produktivitas yang lebih tinggi (Cucculelli dan Bettinelli, 2015).

Dalam bidang hiburan, jaringan komputer memungkinkan pengguna untuk mengakses berbagai jenis konten dengan cepat dan mudah, termasuk film, musik, dan game (Roberts dan Foehr, 2008). Contohnya adalah platform game online seperti Steam yang memungkinkan pengguna untuk mengunduh dan memainkan game dari berbagai genre dengan mudah.

Di bidang kesehatan, jaringan komputer memungkinkan dokter dan tenaga medis untuk berkomunikasi dan berkolaborasi dengan mudah. Dengan jaringan komputer, data medis dapat diakses dari mana saja, sehingga memungkinkan para profesional medis untuk memberikan perawatan yang lebih baik dan lebih cepat kepada pasien (Porumb, 2010).

1.5.3. Masa Depan Jaringan Komputer

Masa depan jaringan komputer sangat menjanjikan dan terus berkembang seiring dengan perkembangan teknologi. Beberapa tren teknologi yang diperkirakan akan mempengaruhi jaringan komputer di masa depan antara lain adalah Internet of Things (IoT), 5G, dan teknologi jaringan yang lebih cepat dan handal.

Internet of Things (IoT) adalah konsep yang mengacu pada koneksi perangkat-perangkat elektronik yang dapat berkomunikasi satu sama lain melalui jaringan internet. Dalam konteks jaringan komputer, IoT akan memungkinkan banyak perangkat terhubung ke jaringan, sehingga membutuhkan jaringan yang lebih kuat dan handal. Menurut Diechmann, dkk (2018), perkembangan IoT akan mempercepat pertumbuhan dan adopsi teknologi jaringan nirkabel.

Sementara itu, teknologi jaringan 5G diprediksi akan mengubah cara kita mengakses dan menggunakan jaringan. Dengan kecepatan dan kapasitas yang lebih tinggi, jaringan 5G dapat memungkinkan penggunaan aplikasi yang lebih canggih dan kompleks, seperti Augmented Reality

(AR) dan Virtual Reality (VR) (Rao dan Prasad, 2018).

Selain itu, terdapat beberapa teknologi jaringan lain yang sedang dikembangkan untuk mengatasi masalah kecepatan dan kehandalan jaringan, seperti teknologi jaringan Mesh dan teknologi WiGig. Teknologi jaringan Mesh memungkinkan jaringan terdiri dari beberapa perangkat yang terhubung tanpa memerlukan titik akses pusat (central access point), sehingga meningkatkan keandalan jaringan (Karthika, 2016). Sedangkan teknologi WiGig adalah teknologi jaringan nirkabel dengan kecepatan tinggi yang dapat digunakan untuk aplikasi streaming video dan VR (Rodrigues, dkk., 2023). Teknologi 5G sedang berkembang dan dianggap sebagai teknologi yang akan mempercepat koneksi internet dan meningkatkan kinerja jaringan komputer secara keseluruhan. Teknologi 5G diharapkan dapat mengubah cara kita berinteraksi dengan teknologi digital dan memberikan pengalaman yang lebih cepat dan lebih mulus.

BAB II

PERANGKAT JARINGAN KOMPUTER

2.1. Pengertian dan Fungsinya

Perangkat jaringan komputer merupakan perangkat keras maupun lunak yang digunakan untuk menghubungkan, mengelola, dan memfasilitasi komunikasi antara komputer atau perangkat lain di dalam suatu jaringan komputer. Perangkat jaringan ini meliputi berbagai macam perangkat seperti *router*, *switch*, *hub*, *modem*, *firewall*, *gateway* dan perangkat lunak seperti protokol jaringan dan aplikasi jaringan. Penggunaan perangkat jaringan komputer sangat penting untuk memfasilitasi pengiriman dan transformasi data sehingga perangkat tersebut dapat beroperasi secara optimal. Seperti yang kita ketahui, perangkat komputer memiliki beberapa jaringan yang digunakan untuk meningkatkan kinerjanya. Sebuah perangkat komputer tidak akan dapat berfungsi dengan optimal jika tidak terdapat jaringan yang menghubungkan antara komponen yang ada.

Fungsi utama dari perangkat jaringan komputer adalah untuk memastikan bahwa pengiriman data dapat berjalan dengan efisien, cepat, dan aman dalam

komunikasi antar komputer atau perangkat di dalam jaringan. Dalam rangka mencapai tujuan ini, perangkat keras jaringan digunakan untuk memfasilitasi pengiriman data dari satu perangkat ke perangkat lain sehingga perangkat tersebut dapat terhubung dalam sebuah jaringan.

Jaringan komputer adalah perangkat komputasi yang saling terhubung serta dapat saling berbagi data serta sumber daya satu sama lain. Perangkat jaringan ini menggunakan protokol komunikasi yang mengatur aturan dalam teknologi transmisi atau pengiriman data baik secara fisik maupun nirkabel. Media transmisi yang digunakan dalam jaringan komputer dapat berupa kabel, gelombang radio, *infrared*, atau satelit. Agar dapat dikategorikan sebagai jaringan komputer, terdapat beberapa syarat yang harus terpenuhi:

- 1) Terdapat minimal 2 perangkat komputer yang saling terhubung, tidak terbatas hanya pada *desktop*, dan koneksi dapat menggunakan kabel, nirkabel, atau kombinasi dari keduanya.
- 2) Terdapat pengguna yang menggunakan jaringan untuk bertukar data dan informasi.
- 3) Terdapat data atau informasi yang ditukar antara perangkat dalam jaringan.

- 4) Terdapat penggunaan bersama perangkat lunak dan perangkat keras dalam jaringan.

Dalam pemanfaatan teknologi jaringan, terdapat 3 jenis perangkat yang dibutuhkan agar dapat terhubung dengan internet, yaitu: *End Devices*, *Intermediary Devices* dan *Network Media* seperti pada gambar 2.1. bagian dari struktur organisasi perangkat jaringan komputer tersebut.

Device Category	Function	Representation
End Devices	Provides an interface between the human network and the communication network.	   IP Phone Wireless Tablet Laptop
		   Desktop Computer Printer TelePresence Endpoint
Intermediary Devices	Provides a connection for a host to the network and can connect multiple networks to form an internetwork.	   Wireless Router LAN Switch Firewall Appliance
		  Router Multilayer Switch
Network Media	Provides a channel for messages to travel from source to destination.	   WAN Media Wireless Media LAN Media

Gambar 2.1. Struktur organisasi perangkat jaringan komputer (Sumber : Cisco Network Academy)

2.2. Perangkat Keras *End Device*

End devices adalah perangkat yang populer dalam dunia jaringan karena memberikan *interface* antara pengguna dan jaringan komunikasi dasar. *End devices* perangkat jaringan yang umum dan sering digunakan dalam kehidupan sehari-hari. Perangkat ini berfungsi sebagai antarmuka atau *interface* antara pengguna dan jaringan komunikasi. Sebuah perangkat *host*, baik yang menjadi sumber atau tujuan dari sebuah pesan, dikirimkan melalui suatu jaringan. Supaya dapat membedakan antara satu *host* dengan *host* lainnya, setiap *host* diberikan sebuah alamat atau *address*. Pada saat sebuah *host* memulai komunikasi, *host* tersebut menggunakan alamat dari *host* tujuan untuk menentukan ke mana tujuan pesan tersebut. Beberapa contoh perangkat end devices adalah *server*, komputer, laptop, handphone, dan tablet seperti pada gambar 2.2. bagian perangkat keras *end devices*.

Device Category	Function	Representation
End Devices	Provides an interface between the human network and the communication network.	 IP Phone  Wireless Tablet  Laptop  Desktop Computer  Printer  TelePresence Endpoint

Gambar 2.2. Perangkat keras *end devices* (Sumber: Cisco Network Academy)

Beberapa contoh *end devices* meliputi komputer seperti *workstation*, laptop, *file server*, dan *web server*, printer jaringan, telepon VoIP, *endpoint TelePresence*, Kamera Pengawas (IP Camera) serta perangkat genggam seperti *smartphone*, tablet, PDA, *wireless debit/credit card reader*, dan *barcode scanner*. Berikut ini beberapa contoh *end device* yang sering kita gunakan yaitu:

1) Komputer (*web server*)

Web server adalah sebuah jaringan komputer yang berfungsi untuk melayani permintaan HTTP dan HTTPS. Situs seperti *search engine*, blog, dan *website*, memerlukan *web server* untuk memproses *file web* seperti .html .php .asp sebelum dikirimkan ke *client*. Fungsi utama dari *web server* adalah untuk mengirimkan berkas yang diminta oleh pengguna melalui browser dengan protokol tertentu. Dengan demikian, pengguna dapat mengakses berbagai jenis informasi seperti teks, gambar, video, dan sebagainya melalui *browser*.

2) Printer Jaringan

Perangkat printer jaringan didesain agar dapat terkoneksi langsung dengan jaringan komputer. Untuk penggunaan skala besar seperti di kantor, printer yang dapat terintegrasi dengan jaringan.

Tujuan dari penggunaan printer jaringan adalah agar dapat menggunakan printer secara bersama-sama.

3) Telepon VoIP

VoIP adalah teknologi yang memungkinkan pengguna untuk melakukan komunikasi jarak jauh dengan menggunakan jaringan internet. Dalam penggunaannya, VoIP menggunakan protokol jaringan seperti H.323, MGCP, SIP, RTP, SDP, atau IAX. Dengan VoIP, koneksi suara yang dikirim melalui jaringan internet bisa sangat jernih dan terjaga kualitasnya selama koneksi internet stabil.

4) *TelePresence endpoint*

TelePresence adalah teknologi yang menggunakan standar IP dan beroperasi di dalam jaringan suara, video dan data dengan menggunakan koneksi internet.

5) Kamera Pengawas (*IP Camera*)

IP Camera adalah sebuah kamera video digital yang menggunakan jaringan komputer untuk mengirimkan gambar dan video melalui protokol *Internet Protocol* (IP). Dalam penggunaannya, IP Camera dapat diakses dan dikendalikan dari jarak jauh melalui jaringan internet, sehingga

memungkinkan pengguna untuk memantau dan merekam video dari lokasi yang berbeda secara *real-time*.

6) Perangkat *Mobile (Smartphone)*

Smartphone adalah jenis ponsel yang dirancang untuk terhubung ke internet melalui jaringan seluler atau nirkabel, sehingga memungkinkan penggunaannya untuk berkomunikasi dan mengakses berbagai aplikasi dan layanan *online*. Dengan menggunakan frekuensi sinyal atau teknologi nirkabel, *smartphone* dapat terhubung ke jaringan dan melakukan *transfer* data secara efisien dan cepat.

Semua perangkat *host* memiliki alamat atau *address* yang digunakan untuk membedakan satu perangkat *host* dengan perangkat *host* lainnya. Ketika perangkat *host* memulai komunikasi, alamat *host* tujuan digunakan untuk menentukan tujuan pesan tersebut.

2.3. Perangkat Keras Intermediary Devices

Intermediary Devices adalah perangkat keras yang berfungsi untuk menghubungkan antara end devices seperti *router*, *switch*, *multilayer switch* dan *firewall appliance*. Contohnya *router* adalah alat yang

mengirimkan paket data melalui jaringan atau internet menuju tujuannya, melalui sebuah proses yang disebut *routing*. *Router* digunakan untuk menghubungkan dua atau lebih jaringan dan meneruskan data dari satu jaringan ke jaringan lainnya. Berbeda dengan *switch*, yang hanya menghubungkan perangkat dalam satu *Local Area Network* (LAN). Sebagai contoh, *switch* dapat diibaratkan sebagai jalanan, sedangkan *router* adalah penghubung antara jalanan tersebut. Masing-masing perangkat *end devices* berada pada jalanan yang memiliki alamat tertentu yang dikenal sebagai IP Address dalam sebuah LAN.

Intermediary Devices berfungsi sebagai penghubung antara *end device* dalam jaringan komputer. Perangkat ini bertanggung jawab untuk menyediakan konektivitas dan memastikan aliran data yang melalui jaringan. Selain menghubungkan *host* secara individual ke jaringan, perangkat *intermediary* juga dapat menghubungkan beberapa jaringan individu untuk membentuk *internetwork*. Beberapa contoh perangkat *intermediary* meliputi *switch* dan *wireless access point* untuk *network access*, *router* untuk *Internetworking*, serta *firewall* untuk *security*.

Intermediary Devices juga bertugas untuk mengatur aliran data melalui jaringan dan menggunakan alamat

host tujuan untuk menentukan jalur yang harus ditempuh oleh pesan. Proses yang berjalan dalam perangkat *intermediary* mencakup pembangkitan dan pengiriman sinyal data, manajemen informasi mengenai jalur yang tersedia di jaringan dan *internetwork*, notifikasi adanya kesalahan dan kegagalan komunikasi, pengalihan data melalui jalur alternatif pada saat terjadi kegagalan sambungan, klasifikasi dan pengarahan pesan berdasarkan prioritas *Quality of Service (QoS)*, serta persetujuan atau penolakan aliran data berdasarkan pengaturan keamanannya.

Device Category	Function	Representation
Intermediary Devices	Provides a connection for a host to the network and can connect multiple networks to form an internetwork.	   Wireless Router LAN Switch Firewall Appliance   Router Multilayer Switch

Gambar 2.3. Perangkat keras *intermediary devices*
(Sumber: Cisco Network Academy)

Beberapa contoh perangkat keras *intermediary devices* meliputi:

- 1) *Network Access* (switch, hub dan wireless access point)

Switch adalah perangkat keras yang memiliki fungsi serupa dengan hub, yaitu membagikan jaringan lokal ke banyak perangkat komputer.

Namun, fungsi utama *switch* adalah menerima sinyal dan mengirimkan data jaringan dari *server* ke perangkat lain di dalam jaringan dengan lebih efisien dan akurat.

Hub digunakan untuk membagi server ke jaringan lain, tetapi memiliki kelemahan jika mengalami kerusakan maka transmisi jaringan ke komputer juga terganggu. Hub juga tidak dapat mengatur kecepatan data yang dikirimkan ke komputer lainnya. Prinsip kerja hub adalah menyalin paket data dari sebuah sumber yang terhubung dengan *port* pada hub dan membagikannya ke seluruh *port* yang terhubung dengan hub tersebut.

Wireless Access Point memiliki fungsi untuk menghubungkan perangkat nirkabel ke jaringan kabel dengan memancarkan sinyal Wi-Fi. Meskipun memiliki fungsi yang mirip dengan *router*, tetapi fungsi utama *Access point* adalah untuk memperluas jangkauan jaringan nirkabel yang dipancarkan oleh *router*. *Access point* dapat terhubung ke *broadband* atau *router* melalui kabel jaringan.

2) *Internetworking (router)*

Router adalah perangkat yang bertujuan untuk menghubungkan dua atau lebih jaringan agar dapat saling berkomunikasi dan bertukar data. *Router* mampu mengintegrasikan berbagai jenis topologi jaringan seperti *bus*, *star*, dan *ring* dalam proses pengirimannya. Sehingga, data yang dikirimkan dari satu perangkat ke perangkat lain dapat diterima dengan baik. Dalam penggunaannya, *router* dapat berfungsi tidak hanya untuk menghubungkan dua atau lebih jaringan, tetapi juga untuk membuat koneksi antara jaringan LAN dengan layanan telekomunikasi seperti *Leased Line* atau *Digital Subscriber Line (DSL)*. *Router* yang digunakan untuk tujuan tersebut sering disebut sebagai *access server*. Contoh lain dari *router* adalah *DSL router* yang digunakan untuk menghubungkan jaringan lokal ke koneksi jaringan DSL.

3) *Security (firewall)*

Firewall adalah sistem keamanan untuk melindungi jaringan komputer dari serangan yang berasal dari luar. *Firewall* dapat diimplementasikan dalam bentuk *software* dan *hardware* atau kombinasi dari keduanya. Instalasi *firewall* sangat penting untuk

memastikan keamanan komputer saat terhubung ke internet dan melindungi dari serangan berbahaya.

Intermediary Devices bertanggung jawab dalam mengatur aliran data melalui jaringan dan juga menggunakan alamat *host* tujuan untuk menentukan jalur yang harus dilalui oleh pesan. Selain itu, perangkat ini juga memiliki beberapa fungsi, antara lain:

- 1) Menghasilkan dan mengirimkan sinyal data
- 2) Mengatur informasi tentang jalur yang tersedia di jaringan dan *internetwork*
- 3) Memberi tahu perangkat lain tentang adanya kesalahan dan kegagalan komunikasi
- 4) Mengarahkan data melalui jalur alternatif ketika terjadi kegagalan koneksi
- 5) Mengelompokkan dan mengarahkan pesan berdasarkan prioritas *Quality of Service* (QoS)
- 6) Memvalidasi aliran data berdasarkan pengaturan keamanannya.

2.4. Media Transmisi

Media transmisi merupakan saluran fisik yang menghubungkan pengirim dan penerima dalam sistem komunikasi. Media transmisi digunakan untuk

mengirimkan pesan melalui jaringan dengan memberikan jalur bagi pesan dari sumber ke tujuannya. Terdapat tiga jenis media transmisi yang umum digunakan dalam jaringan modern. Jenis media tersebut adalah kabel tembaga, kabel serat optik, dan transmisi nirkabel. Setiap jenis media transmisi memiliki metode *encoding* sinyal yang berbeda. Kabel tembaga menggunakan impuls listrik untuk membentuk pola khusus, kabel serat optik mengirimkan pesan dengan menggunakan pulsa cahaya, dan transmisi nirkabel menggunakan pola gelombang elektromagnetik.

Media transmisi memiliki karakteristik dan keunggulan yang berbeda, sehingga tidak semua media cocok untuk setiap tujuan. Ada beberapa kriteria yang dapat digunakan untuk menentukan media transmisi yang tepat, seperti jarak yang dapat dicapai oleh media, lingkungan tempat media digunakan, jumlah data dan kecepatan yang harus dikirimkan, serta biaya media dan instalasinya.

Device Category	Function	Representation		
Network Media	Provides a channel for messages to travel from source to destination.			

Gambar 2.4. Perangkat keras *Network Media* (Sumber: Cisco Network Academy)

Beberapa jenis media perangkat *Network Media devices* meliputi:

1) WAN Media

Sekumpulan LAN atau *workgroup* yang dihubungkan dengan modem komunikasi dari jaringan internet, yang terhubung ke server pusat. Bedanya dengan LAN, WAN memiliki area cakupan yang lebih luas, seperti jaringan komputer antar kota, bahkan negara. Media komunikasi yang digunakan untuk WAN adalah PSTN atau Satellite Link, dibutuhkan alat khusus yang berfungsi sebagai pusat layanan, seperti satelit VSAT. VSAT adalah sistem komunikasi satelit yang terdiri dari beberapa stasiun remote dengan menggunakan antena parabola berdiameter lebih kecil daripada komunikasi satelit lainnya, dengan menggunakan *transponder* satelit sebagai pengulang sinyal, didukung oleh peralatan di stasiun dan sebuah stasiun bumi utama. Dengan VSAT, jaringan LAN dapat digabungkan menjadi satu jaringan baru, dan VSAT bertindak sebagai media penghubung antara satu jaringan LAN dengan jaringan LAN lainnya.

Infrastruktur WAN Media melibatkan beberapa perangkat yang bertugas mengalirkan informasi data. Seperti halnya pada LAN (*Local Area Network*), penggabungan perangkat ini menciptakan infrastruktur WAN media yang meliputi:

a) *Router*

Perangkat *router* memiliki kemampuan lebih dari *bridge*, karena mampu menunjukkan jalur *route* dan memfilter informasi pada jaringan yang berbeda. *Router* juga dapat mendeteksi masalah dan mengalihkan jalur informasi secara otomatis dari area yang bermasalah.

b) Switch ATM

Perangkat switch ATM menyediakan transfer data antara LAN dan WAN dengan kecepatan tinggi.

c) Modem dan CSU/DSU

Modem dapat mengkonversi sinyal *digital* dan analog, mengubahnya ke dalam bentuk yang sesuai dengan teknologi transmisi untuk dilewatkan melalui jaringan telepon analog atau *digital*. Sedangkan CSU/DSU mengirim data dalam format digital melalui jaringan

telepon digital dan biasanya berupa kotak fisik yang terdiri dari dua unit terpisah, yaitu CSU atau DSU.

d) *Communication Server*

Merupakan server khusus yang memungkinkan pengguna melakukan koneksi dial-*in* atau dial-*out* dari lokasi *remote* ke LAN.

e) Multiplexer

Perangkat *Multiplexer* dapat mentransmisikan beberapa sinyal melalui sebuah sirkuit, sehingga dapat mentransfer beberapa data secara simultan seperti video, suara, dan teks.

f) *X.25/Frame Relay Switches*

Switch X.25 dan *Frame Relay* menghubungkan data lokal atau pribadi melalui jaringan data dengan menggunakan sinyal digital. Perangkat ini mirip dengan *switch ATM*, namun kecepatan transfer datanya lebih rendah dibandingkan dengan ATM.

2) *Wireless Media*

Media transmisi wireless atau tanpa kabel yang menggunakan sistem gelombang dikenal sebagai media transmisi tidak terpandu (*unguided*). Beberapa jenis media transmisi tidak terpandu

yang umum digunakan termasuk inframerah, gelombang radio, gelombang mikro, dan satelit.

- a) Inframerah digunakan untuk komunikasi jarak dekat dengan kecepatan transmisi sekitar 4 Mbps. Contoh penggunaannya adalah sebagai pengontrol jarak jauh seperti *remote control* untuk televisi dan perangkat elektronik lainnya.
 - b) Gelombang radio merupakan media transmisi yang dapat digunakan untuk mengirim suara dan data.
 - c) Gelombang mikro (*microwave*) adalah bentuk radio dengan frekuensi yang tinggi (dalam satuan gigahertz) yang mencakup rentang UHF, SHF, dan EHF. Gelombang mikro sering digunakan dalam jaringan MAN, warnet, dan penyedia layanan internet (ISP).
 - d) Satelit adalah media transmisi yang menerima sinyal dari stasiun bumi dan meneruskannya ke stasiun bumi lain.
- 3) LAN Media

Media transmisi yang berpemandu adalah jenis media yang digunakan untuk mengirimkan gelombang elektromagnetik atau data dengan menggunakan media konduktor fisik seperti

serat optik atau kabel. Kabel atau serat optik pada media transmisi yang terarah digunakan untuk menghantarkan sinyal dari pengirim ke penerima dengan kecepatan yang tinggi dan minim gangguan interferensi.



Gambar 2.5. Kabel dan konektor media transmisi berpemandu (*guided*)
(Sumber: wikipedia.org)

a) Kabel Koaksial (*Coaxial Cable*)

Kabel Koaksial memiliki lapisan luar plastik yang menampung 2 konduktor paralel yang dilindungi oleh lapisan insulasi yang terpisah. Kabel koaksial dapat mentransmisikan informasi dalam dua mode: *Mode Baseband* (*bandwidth* kabel khusus) dan *Mode Broadband* (*bandwidth* kabel dibagi menjadi rentang yang terpisah). Kabel jenis ini sering

digunakan dalam koneksi televisi kabel dan jaringan televisi analog.

b) Kabel Twisted Pair (UTP)

Kabel Twisted Pair terdiri dari dua kawat konduktor terisolasi yang dipisahkan satu sama lain. Beberapa pasangan kawat tersebut sering digabungkan bersama dalam lapisan pelindung. Kabel jenis ini adalah media transmisi yang paling umum digunakan dalam jaringan LAN. Terdapat dua jenis kabel *Twisted Pair*

c) Kabel Serat Optik (*Fiber Optic Cable*)

Kabel serat optik memanfaatkan pantulan cahaya melalui inti yang terbuat dari kaca atau plastik. Inti ini dilapisi oleh kaca atau penutup plastik yang lebih tipis yang disebut *kelongsong*. Kabel ini digunakan untuk mentransmisikan data dengan kapasitas besar.

2.5. Ringkasan Materi

Komunikasi dianggap sama pentingnya dengan kebutuhan dasar seperti udara, air, makanan, dan tempat tinggal. Dengan adanya teknologi digital, manusia dapat terhubung satu sama lain dengan cara

yang lebih efektif dan efisien. Teknologi jaringan mengalami kemajuan teknologi yang sangat membantu dalam berkomunikasi, terutama untuk komunikasi dua arah yang jaraknya jauh. Pemanfaatan teknologi jaringan, banyak orang dapat saling terhubung dan berkomunikasi melalui perangkat jaringan dengan koneksi internet.

Perangkat jaringan komputer memiliki peran penting dalam menghubungkan, mengelola, dan memfasilitasi komunikasi antara perangkat di dalam suatu jaringan. Ada beberapa jenis perangkat jaringan seperti *router, switch, hub, modem, firewall, gateway* dan perangkat lunak seperti protokol jaringan dan aplikasi jaringan. Tujuan utama dari penggunaan perangkat jaringan komputer adalah untuk memfasilitasi pengiriman data sehingga perangkat tersebut dapat beroperasi secara optimal. Jaringan komputer memungkinkan perangkat saling terhubung dan berbagi data serta sumber daya satu sama lain. Untuk mencapai tujuan ini, perangkat keras jaringan digunakan untuk memfasilitasi pengiriman data dari satu perangkat ke perangkat lain melalui media transmisi seperti kabel, gelombang radio, infrared, atau satelit. Protokol jaringan juga digunakan untuk mengatur aturan dalam teknologi

transmisi atau pengiriman data secara fisik maupun nirkabel.

End devices digunakan dalam jaringan karena memberikan antarmuka antara pengguna dan jaringan komunikasi dasar. *Host* diberi alamat untuk membedakannya dari *host* lain dalam jaringan, dan mereka menggunakan alamat tujuan untuk menentukan tempat mengirim pesan. Perangkat perantara, seperti *router*, *switch*, *multilayer switch*, dan perangkat *firewall*, menghubungkan *end device* dan bertanggung jawab untuk memberikan konektivitas dan memastikan aliran data melalui jaringan. Jenis media transmisi yang berbeda seperti kabel tembaga, kabel serat optik dan transmisi nirkabel, digunakan untuk mengirimkan pesan melalui jaringan. Setiap media memiliki metode *encoding* dan karakteristik unik, seperti jarak yang dapat dicapai, faktor lingkungan, kecepatan data, dan biaya, yang perlu dipertimbangkan saat memilih media yang tepat untuk tujuan tertentu.

BAB III

ARSITEKTUR KOMPUTER

3.1. Pengantar ke Arsitektur Komputer

Arsitektur komputer merujuk pada struktur dasar, organisasi, dan komponen yang membentuk suatu sistem komputer atau perangkat komputasi. Ini adalah konsep inti dalam ilmu komputer yang memungkinkan perancang sistem untuk merancang, mengembangkan, dan memahami cara kerja komputer atau perangkat komputasi tertentu.

Arsitektur komputer adalah dasar bagi pemahaman dan pengembangan teknologi komputer. Ini memungkinkan para insinyur dan ilmuwan komputer untuk merancang sistem yang sesuai dengan kebutuhan dan mengoptimalkan kinerja komputasi. Selain itu, pemahaman tentang arsitektur komputer juga penting bagi pengembang perangkat lunak untuk menulis program yang efisien dan kompatibel dengan berbagai platform komputer.

3.2. Sejarah Perkembangan Arsitektur Komputer

Sejarah perkembangan arsitektur komputer adalah cerita panjang tentang evolusi perangkat keras

komputer dari zaman awal hingga era modern. Berikut adalah beberapa tonggak sejarah dalam perkembangan arsitektur komputer:

1. Zaman Mesir Kuno (sekitar 2700 SM - 1070 SM):
Penggunaan alat perhitungan seperti papan tulis dan penghitung bulat di Mesir Kuno adalah contoh awal perangkat komputasi sederhana.
2. Abakus (sekitar 300 SM):
Abakus adalah salah satu alat perhitungan pertama yang dikenal manusia. Ini adalah alat mekanis yang digunakan untuk melakukan perhitungan aritmetika dasar.
3. Mesin Analitik Charles Babbage (1837):
Charles Babbage dikenal sebagai "Bapak Komputer" karena ia merancang mesin analitik pertama yang dapat diprogram. Ini adalah perangkat mekanis yang menggunakan kartu punch untuk memasukkan instruksi.
4. Tabulating Machine IBM (1889):
Perusahaan IBM, yang saat itu dikenal sebagai Tabulating Machine Company, memperkenalkan mesin yang menggunakan kartu punch untuk menghitung dan menyimpan data.
5. Komputer Elektronik Pertama, ENIAC (1945):

ENIAC (Electronic Numerical Integrator and Computer) adalah komputer elektronik pertama yang dapat diprogram. Ini digunakan untuk menghitung tabel tembakau untuk proyek penelitian atom selama Perang Dunia II.

6. Komputer Generasi Pertama (1940-an - 1950-an):

Komputer generasi pertama adalah komputer besar yang menggunakan tabung vakum untuk pemrosesan data. Contohnya adalah UNIVAC dan IBM 701.

7. Transistor (1947):

Penemuan transistor oleh Bell Labs membawa revolusi dalam desain komputer. Transistor lebih kecil, lebih efisien, dan lebih andal daripada tabung vakum.

8. Komputer Generasi Kedua (akhir 1950-an - awal 1960-an):

Komputer generasi kedua menggunakan transistor sebagai komponen utama. Mereka lebih kecil, lebih cepat, dan lebih efisien daripada komputer generasi pertama.

9. Mikroprosesor (1971):

Intel memperkenalkan mikroprosesor 4004, yang merupakan komponen dasar dari komputer pribadi pertama.

10. Komputer Pribadi (awal 1980-an):

IBM memperkenalkan IBM PC pada tahun 1981, yang membuka jalan bagi komputer pribadi. Ini adalah awal dari era komputasi pribadi yang populer.

11. Komputer Paralel dan Superkomputer (1980-an - sekarang):

Pengembangan komputer paralel dan superkomputer telah meningkatkan kemampuan pemrosesan data dan aplikasi seperti simulasi ilmiah dan pemodelan cuaca.

12. Perkembangan GPU (Graphics Processing Unit):

GPU awalnya dikembangkan untuk pengolahan grafis, tetapi kemudian digunakan dalam komputasi paralel, yang berkontribusi pada percepatan pemrosesan berbagai jenis data.

13. Komputasi Kuantum (Mulai dari 1990-an):

Penelitian dalam komputasi kuantum telah membawa perkembangan baru dalam pemrosesan informasi dan berjanji untuk mengubah cara kita memecahkan masalah yang sangat kompleks.

Perkembangan arsitektur komputer adalah cermin dari kemajuan teknologi dan ilmu pengetahuan komputer. Setiap generasi baru komputer membawa perbaikan dalam kinerja, efisiensi, dan aplikasi yang dapat digunakan. Perjalanan ini terus berlanjut dengan penemuan dan inovasi baru yang memacu perkembangan teknologi komputer.

3.3. Konsep Dasar Komputer

Konsep dasar komputer mencakup prinsip-prinsip fundamental yang membentuk dasar dari ilmu komputer dan arsitektur komputer. Berikut adalah beberapa konsep dasar komputer yang penting:

1. Bit (Binary Digit):

Bit adalah unit data terkecil dalam komputer, yang dapat memiliki nilai 0 atau 1. Bit digunakan untuk merepresentasikan informasi digital, dan serangkaian bit membentuk byte.

2. Byte:

Byte adalah grup delapan bit dan merupakan unit dasar untuk menyimpan dan mengirim data dalam komputer. Sebagian besar informasi dalam komputer direpresentasikan dalam bentuk byte.

3. Sistem Bilangan:

Sistem bilangan yang paling umum digunakan dalam komputer adalah sistem bilangan biner (base-2), tetapi juga ada sistem bilangan desimal (base-10), heksadesimal (base-16), dan lainnya.

4. Prosesor (CPU - Central Processing Unit):

CPU adalah otak komputer yang bertanggung jawab untuk mengeksekusi instruksi, melakukan operasi aritmetika dan logika, dan mengendalikan operasi komputer secara keseluruhan.

5. Memori:

Memori digunakan untuk menyimpan data dan instruksi yang diperlukan oleh CPU. Ini termasuk RAM (Random Access Memory) untuk penyimpanan sementara dan media penyimpanan jangka panjang seperti hard drive atau SSD.

6. Perangkat Input/Output (I/O):

Ini mencakup perangkat seperti keyboard, mouse, monitor, printer, dan perangkat lain yang memungkinkan komunikasi antara manusia dan komputer.

7. Sistem Operasi:

Sistem operasi adalah perangkat lunak yang mengelola sumber daya komputer, mengatur

eksekusi program, dan menyediakan antarmuka antara pengguna dan perangkat keras. Contoh sistem operasi termasuk Windows, macOS, dan Linux.

8. Instruksi dan Bahasa Mesin:

Bahasa mesin adalah kumpulan instruksi biner yang dipahami oleh CPU. Program-program komputer ditulis dalam bahasa pemrograman tingkat tinggi seperti C++, Java, atau Python, dan kemudian diterjemahkan menjadi bahasa mesin oleh kompiler.

9. Arsitektur Komputer Von Neumann:

Ini adalah model arsitektur komputer yang paling umum, yang memiliki konsep memori terpusat dan unit pemrosesan terpusat. CPU secara berurutan mengambil instruksi dari memori, menguraikannya, dan melakukan operasi yang sesuai.

10. Perkembangan Teknologi Komputer:

Teknologi komputer terus berkembang dengan peningkatan kecepatan, kapasitas, dan efisiensi perangkat keras. Ini termasuk peningkatan dalam CPU, memori, dan media penyimpanan.

11. Pemrograman Komputer:

Pemrograman komputer melibatkan penulisan kode komputer dalam bahasa pemrograman tertentu untuk menyelesaikan tugas atau masalah tertentu. Ini melibatkan algoritma, struktur data, dan logika pemrograman.

12. Jaringan Komputer:

Jaringan komputer adalah koneksi antara komputer yang memungkinkan berbagi data dan sumber daya. Internet adalah contoh besar dari jaringan komputer global.

13. Keamanan Komputer:

Keamanan komputer adalah perlindungan terhadap ancaman dan serangan yang mungkin memengaruhi integritas, kerahasiaan, dan ketersediaan data komputer.

14. Komputasi Kuantum (Quantum Computing):

Komputasi kuantum adalah bidang baru dalam ilmu komputer yang berjanji untuk memberikan pemrosesan yang jauh lebih cepat daripada komputer konvensional dengan menggunakan prinsip-prinsip mekanika kuantum.

Pemahaman konsep dasar komputer adalah langkah penting dalam memahami dunia komputer dan teknologi informasi. Ini membantu individu untuk

mengoperasikan komputer, memahami bagaimana perangkat keras dan perangkat lunak berinteraksi, serta berkontribusi pada pengembangan dan pemeliharaan sistem komputer yang efisien.

3.4. Sistem Bilangan dalam Komputer

Sistem bilangan dalam komputer adalah cara komputer mewakili dan memproses data numerik. Tiga sistem bilangan yang paling umum digunakan dalam komputer adalah:

1. Sistem Bilangan Desimal (Base-10):

Sistem bilangan desimal adalah sistem yang paling umum digunakan dalam kehidupan sehari-hari. Ini terdiri dari angka 0 hingga 9, dan setiap digit mewakili pangkat 10 yang berbeda. Contohnya: 1234.

2. Sistem Bilangan Biner (Base-2):

Sistem bilangan biner menggunakan hanya dua digit, yaitu 0 dan 1. Ini adalah sistem yang digunakan secara internal oleh komputer karena mudah diimplementasikan dalam sirkuit elektronik. Dalam sistem biner, setiap digit mewakili pangkat 2 yang berbeda. Contohnya: 1101 (dalam desimal, ini sama dengan 13).

3. Sistem Bilangan Heksadesimal (Base-16):

Sistem bilangan heksadesimal menggunakan 16 digit, yaitu 0-9 dan huruf A hingga F (mewakili nilai 10 hingga 15). Ini digunakan secara luas dalam pemrograman komputer, terutama saat berurusan dengan alamat memori, konfigurasi perangkat keras, dan pemrograman rendah tingkat. Setiap digit dalam heksadesimal mewakili pangkat 16 yang berbeda. Contohnya: 1A3 (dalam desimal, ini sama dengan 419).

Komputer juga dapat mengonversi antara sistem bilangan ini menggunakan perangkat lunak atau sirkuit khusus yang disebut konverter. Beberapa hal penting terkait sistem bilangan dalam komputer adalah:

1. Operasi Aritmetika: Komputer dapat melakukan operasi aritmetika seperti penjumlahan, pengurangan, perkalian, dan pembagian pada bilangan dalam sistem biner. Ini adalah dasar dari semua operasi matematika yang dilakukan oleh komputer.
2. Representasi Data: Data dalam komputer direpresentasikan dalam bentuk biner. Misalnya, teks, gambar, suara, dan video diubah menjadi kode biner sebelum disimpan dan diproses oleh komputer.

3. Representasi Memori: Alamat memori dalam komputer sering kali diwakili dalam sistem heksadesimal. Ini memudahkan pengelolaan dan debugging program.
4. Pemrograman Komputer: Bahasa pemrograman dapat digunakan untuk mengekspresikan instruksi dalam bentuk yang lebih mudah dimengerti oleh manusia, tetapi kompiler atau interpreter akan menerjemahkannya menjadi bahasa mesin dalam sistem bilangan biner.

Pemahaman sistem bilangan dalam komputer penting bagi pengembang perangkat lunak dan insinyur perangkat keras karena itu memengaruhi cara data direpresentasikan, diproses, dan disimpan dalam komputer. Selain itu, pemahaman ini juga relevan ketika berurusan dengan pemrograman rendah tingkat, debugging, dan pengoptimalan perangkat lunak.

3.5. Model Von Neumann

Model Von Neumann, dinamai dari ilmuwan komputer John von Neumann, adalah salah satu model arsitektur komputer yang paling umum digunakan dalam desain komputer modern. Model ini dikenal sebagai "von Neumann architecture" atau "von

Neumann machine." Ini adalah model dasar yang digunakan oleh sebagian besar komputer yang ada hari ini. Berikut adalah beberapa fitur utama dari Model Von Neumann:

1. Memori Terpusat: Model Von Neumann memiliki memori sentral tunggal yang digunakan untuk menyimpan instruksi (program) dan data. Ini berarti instruksi program dan data yang akan diproses oleh CPU (Central Processing Unit) semuanya disimpan dalam memori yang sama.
2. Unit Pemrosesan (CPU) Terpusat: CPU adalah bagian inti dari komputer dan bertanggung jawab untuk mengeksekusi instruksi, melakukan operasi aritmetika dan logika, dan mengendalikan operasi keseluruhan komputer. CPU bekerja secara berurutan mengambil instruksi dari memori, mengurai instruksi tersebut, mengeksekusi instruksi, dan mengambil instruksi berikutnya.
3. Bus Data: Model Von Neumann menggunakan bus data sebagai jalur komunikasi utama untuk mengirim dan menerima data antara CPU, memori, dan perangkat input/output. Bus data menghubungkan berbagai komponen dalam komputer dan memungkinkan transfer data.

4. Instruksi dan Data Dipisahkan: Instruksi program dan data yang akan diproses oleh CPU dipisahkan dalam memori. Instruksi-instruksi program diambil secara berurutan oleh CPU dan diuraikan untuk dijalankan. Data-data yang digunakan oleh program juga disimpan dalam memori yang sama.
5. Eksekusi Berurutan: Instruksi-instruksi dalam program dieksekusi secara berurutan, satu per satu. CPU mengambil instruksi, mengurai instruksi tersebut menjadi operasi yang sesuai, menjalankan operasi tersebut, dan kemudian mengambil instruksi berikutnya.
6. Program Counter (PC): PC adalah register khusus dalam CPU yang menyimpan alamat dari instruksi berikutnya yang akan diambil dan dieksekusi. PC akan diperbarui secara otomatis setiap kali instruksi dieksekusi.
7. Pemrograman dalam Bahasa Mesin: Program-program komputer ditulis dalam bahasa mesin, yang terdiri dari serangkaian instruksi biner yang dipahami oleh CPU. Program-program ini kemudian dapat dibuat menggunakan bahasa pemrograman tingkat tinggi dan diterjemahkan menjadi bahasa mesin oleh kompiler.

Model Von Neumann sangat penting dalam sejarah komputasi dan masih menjadi dasar bagi sebagian besar sistem komputer modern. Namun, ada juga variasi dan perbaikan terhadap model ini, seperti komputer paralel dan arsitektur pipelining, yang memungkinkan eksekusi beberapa instruksi secara bersamaan untuk meningkatkan kinerja. Meskipun demikian, prinsip dasar Model Von Neumann tetap menjadi dasar dari sebagian besar komputer yang digunakan sekarang.

3.6. Arsitektur RISC vs. CISC

Arsitektur komputer dapat dibagi menjadi dua kategori utama: Reduced Instruction Set Computing (RISC) dan Complex Instruction Set Computing (CISC). Kedua arsitektur ini memiliki pendekatan yang berbeda dalam merancang set instruksi dan pemrosesan. Berikut perbandingan antara RISC dan CISC:

1. Arsitektur RISC (Reduced Instruction Set Computing):
 - Set Instruksi Sederhana: Arsitektur RISC memiliki set instruksi yang sangat sederhana dan terbatas. Instruksi-instruksi ini cenderung melakukan operasi dasar seperti penambahan, pengurangan, dan pemindahan data.

- Eksekusi Instruksi Efisien: Setiap instruksi dalam arsitektur RISC diharapkan untuk dieksekusi dalam satu siklus clock, yang membuat eksekusi instruksi lebih efisien.
 - Register Banyak: RISC memiliki banyak register CPU yang dapat digunakan untuk menyimpan data sementara. Ini meminimalkan ketergantungan pada akses memori yang lambat.
 - Penggunaan Cache yang Efisien: RISC umumnya memanfaatkan cache memori dengan baik untuk mempercepat akses data.
 - Kompleksitas Perangkat Keras Rendah: Karena instruksi sederhana, perangkat keras CPU dalam arsitektur RISC cenderung lebih sederhana dan efisien.
 - Pemrosesan Paralel Lebih Mudah: Arsitektur RISC memfasilitasi pemrosesan paralel dengan instruksi-instruksi yang sederhana dan terprediksi dengan baik.
2. Arsitektur CISC (Complex Instruction Set Computing):
- Set Instruksi Kompleks: Arsitektur CISC memiliki set instruksi yang kompleks dan beragam. Instruksi-instruksi ini dapat

melakukan berbagai operasi dalam satu instruksi, termasuk operasi aritmetika, pemindahan data, dan manipulasi data.

- Eksekusi Instruksi Lebih Lama: Instruksi-instruksi CISC cenderung memerlukan lebih banyak siklus clock untuk dieksekusi, karena lebih kompleks.
- Jumlah Register Terbatas: Arsitektur CISC biasanya memiliki jumlah register CPU yang terbatas, yang berarti lebih sering harus mengakses memori utama.
- Penggunaan Cache yang Kurang Efisien: Karena instruksi yang kompleks dan beragam, manajemen cache dalam arsitektur CISC bisa lebih rumit.
- Perangkat Keras Lebih Rumit: CISC cenderung memiliki perangkat keras CPU yang lebih kompleks untuk menangani instruksi-instruksi yang beragam.
- Pemrosesan Paralel Lebih Sulit: Pemrosesan paralel dalam arsitektur CISC dapat lebih sulit karena instruksi-instruksi yang kompleks dan tidak terprediksi dengan baik.

Keputusan untuk menggunakan arsitektur RISC atau CISC tergantung pada aplikasi dan tujuan penggunaan komputer. RISC cenderung lebih cocok untuk aplikasi yang memerlukan pemrosesan cepat dan efisien, seperti komputasi ilmiah dan pemrosesan grafis. Sementara itu, CISC mungkin lebih sesuai untuk aplikasi yang membutuhkan instruksi yang kompleks dan beragam, seperti sistem operasi dan pemrosesan bahasa natural. Banyak komputer modern menggunakan campuran dari kedua arsitektur ini dalam berbagai komponen sistem mereka.

BAB IV

JENIS-JENIS JARINGAN KOMPUTER

Jaringan komputer memiliki cakupan yang sangat luas. Untuk memudahkan pemahaman mengenai jaringan komputer perlu dibahas secara spesifik jenis-jenis jaringan komputer. Secara umum jenis-jenis jaringan komputer dapat dikategorikan berdasar hal-hal berikut:

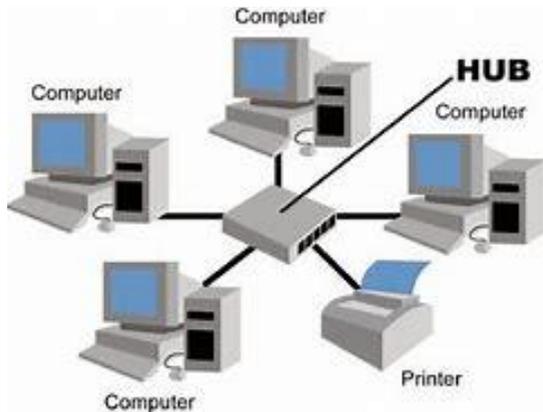
4.1. Jaringan Komputer Berdasar Jangkauan Area Jaringan

Jaringan komputer dapat dibentuk dalam area yang lokal, nasional, maupun global/internasional.

a. Jaringan Lokal (*Local Area Network*)

Pada umumnya jaringan lokal ini memiliki area terbatas, seperti jaringan dalam satu ruang, satu gedung, atau satu lokal kampus. Jaringan ini sering disebut LAN. Jaringan ini digunakan untuk menghubungkan perangkat yang umumnya digunakan untuk berbagi sumber daya seperti printer dan file, serta untuk mengakses internet. Selain secara fisik memiliki area yang sempit, LAN terbentuk atas koneksi beberapa perangkat

dengan satu identitas yang sama dalam satu jaringan. Gambaran LAN dapat dilihat pada Gambar 4.1.



Sumber: <https://www.bing.com>

Gambar 4.1. Jaringan Lokal (*Local Area Network*)

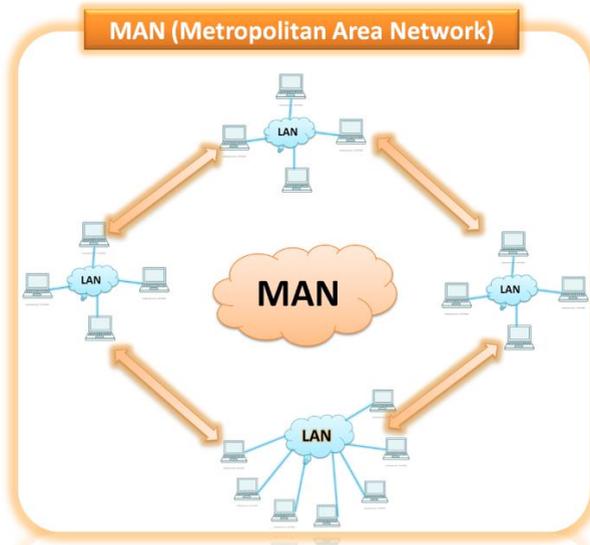
Jaringan area lokal atau LAN terdiri dari tautan fisik yang terhubung secara serial, perangkat keras antarmuka umum yang menghubungkan host ke tautan, dan protokol untuk membuat semuanya perangkat dapat bekerja sama. Dalam hal ini, setiap node LAN dapat berkomunikasi dengan setiap node LAN lainnya melalui perangkat penghubung berupa Switcch atau Hub sebagai node perantara yang bertindak sebagai sakelar atau penerus.

Keuntungan dari penggunaan LAN adalah memungkinkan pengguna untuk berbagi sumber daya seperti printer, file, dan internet dengan mudah dan cepat. Selain itu, LAN juga memungkinkan pengguna untuk berkomunikasi dengan perangkat lain dalam jaringan, seperti mengirim pesan atau melakukan panggilan suara.

LAN dapat dikonfigurasi dan dikelola secara lokal, dan tidak memerlukan biaya tambahan untuk mengakses sumber daya jaringan seperti internet. Namun, jarak jangkauan LAN terbatas, biasanya hanya beberapa ratus meter atau kurang, sehingga tidak cocok untuk menghubungkan perangkat yang berlokasi di area yang lebih luas.

b. Jaringan Kota (*Metropolitan Area Network*)

Jaringan yang biasa disebut MAN ini digunakan untuk menghubungkan beberapa LAN yang berada dalam area yang lebih besar, seperti jaringan komputer di wilayah perkotaan atau jaringan kampus yang memiliki gedung yang terpisah jauh. Jaringan kampus ini juga sering disebut CAN (*Campus Area Network*). Gambaran MAN dapat dilihat pada Gambar 4.2.



Sumber: <https://www.bing.com>

Gambar 4.2. Jaringan Kota (*Metropolitan Area Network*)

Metropolitan Area Network (MAN) adalah jenis jaringan komputer yang digunakan untuk menghubungkan beberapa jaringan LAN di area geografis yang lebih luas, biasanya pada tingkat kota atau wilayah metropolitan. MAN umumnya digunakan oleh organisasi atau lembaga pemerintah yang memerlukan jaringan yang lebih besar dari LAN tetapi lebih kecil dari WAN. MAN biasanya terdiri dari beberapa jaringan LAN yang terhubung melalui teknologi seperti

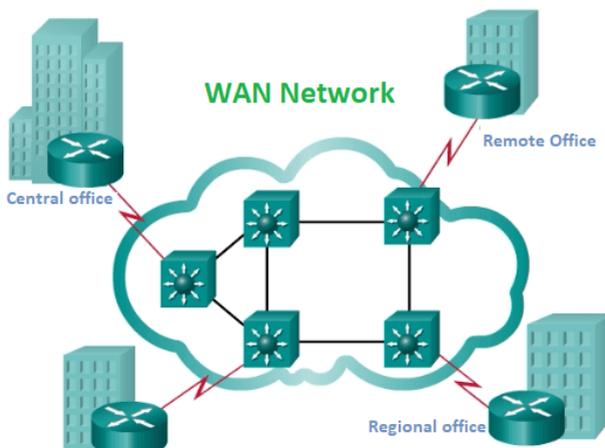
fiber optic atau kabel tembaga. MAN dapat membantu organisasi untuk memperluas jaringan mereka di seluruh kota atau wilayah metropolitan dan memungkinkan mereka untuk berbagi sumber daya seperti printer, file, dan internet dengan mudah.

Keuntungan dari penggunaan MAN adalah memungkinkan organisasi untuk mengakses sumber daya jaringan dari lokasi yang berbeda dalam area geografis yang lebih luas, memungkinkan pengguna untuk berkomunikasi dengan perangkat lain dalam jaringan dengan mudah, dan meningkatkan efisiensi dan produktivitas organisasi. Selain itu, MAN juga memungkinkan organisasi untuk menghemat biaya dengan mengurangi pengeluaran untuk biaya perjalanan dan infrastruktur jaringan yang terpisah.

Namun, MAN memiliki keterbatasan seperti biaya instalasi dan pengoperasian yang lebih tinggi dibandingkan dengan LAN, dan kecepatan transfer data yang mungkin lebih lambat karena jaringan MAN biasanya lebih besar dan kompleks.

c. Jaringan Global (*Wide Area Network*)

Wide Area Network (WAN) terdiri dari beberapa LAN dan atau MAN yang terhubung melalui perangkat jaringan seperti router dan switch. WAN umumnya digunakan untuk menghubungkan jaringan yang berlokasi di wilayah yang berbeda, bahkan di negara yang berbeda. Gambaran WAN dapat dilihat pada Gambar 4.3.



Sumber: <https://www.bing.com>

Gambar 4.3. Jaringan Global (Wide Area Network)

WAN biasanya digunakan oleh perusahaan besar, institusi pendidikan, atau organisasi yang memiliki cabang atau kantor di berbagai lokasi geografis yang berbeda. WAN memungkinkan

perangkat di berbagai lokasi untuk terhubung satu sama lain dan berkomunikasi melalui jaringan publik seperti internet, telepon, atau satelit. WAN menggunakan perangkat jaringan seperti router, switch, dan modem untuk mengirim dan menerima data antara jaringan yang berbeda.

Keuntungan dari penggunaan WAN adalah memungkinkan pengguna untuk mengakses sumber daya jaringan seperti file, aplikasi, dan printer dari lokasi yang berbeda, serta memungkinkan pengguna untuk berkomunikasi dengan perangkat lain dalam jaringan dengan mudah dan cepat. Selain itu, WAN memungkinkan organisasi untuk menghemat biaya dengan mengurangi pengeluaran untuk biaya perjalanan dan infrastruktur jaringan yang terpisah.

Namun, WAN juga memiliki kelemahan, di antaranya adalah biaya yang lebih tinggi dibandingkan dengan LAN, kecepatan transfer data yang lebih lambat, dan keamanan yang kurang dapat diandalkan karena data yang dikirim melalui jaringan publik.

4.2. Jaringan Komputer Berdasar Jenis Transmisinya

Jenis jaringan komputer juga dapat dilihat berdasarkan media transmisi yang digunakan untuk menghubungkan perangkat-perangkat jaringan yang terpasang. Berdasar media transmisi ini dapat dikelompokkan ke dalam jaringan nirkabel dan jaringan kabel.

a. Jaringan nirkabel (*Wireless Network*)

Jenis *Wireless Network* menjadi jenis jaringan komputer modern karena tidak mengandalkan kabel sebagai media transmisi informasi. Pada *Wireless Network*, proses transmisi data menggunakan gelombang elektromagnetik. Gambaran jaringan nirkabel dapat dilihat pada Gambar 4.4.



Sumber: <https://www.bing.com>

Gambar 4.4. Jaringan nirkabel (*Wireless Network*)

Wireless Local Area Network (WLAN) adalah jenis jaringan komputer nirkabel yang menghubungkan perangkat dalam area lokal seperti kantor, rumah, atau gedung. WLAN menggantikan kabel jaringan dengan teknologi nirkabel seperti Wi-Fi untuk menghubungkan perangkat ke jaringan.

WLAN terdiri dari beberapa perangkat seperti router nirkabel dan adaptor nirkabel yang memungkinkan perangkat untuk terhubung ke jaringan nirkabel. Dengan WLAN, pengguna dapat mengakses internet, berbagi file, dan menggunakan aplikasi jaringan tanpa perlu menghubungkan perangkat ke jaringan melalui kabel fisik.

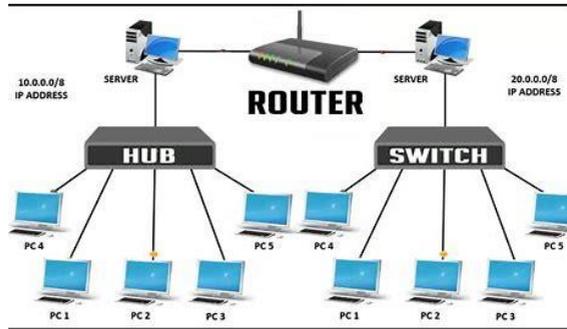
Keuntungan dari penggunaan WLAN adalah mobilitas dan fleksibilitas yang tinggi, karena pengguna dapat mengakses jaringan dari mana saja di area jangkauan nirkabel, tanpa perlu terhubung dengan kabel jaringan. Selain itu, WLAN memungkinkan pengguna untuk berbagi sumber daya seperti printer dan file dengan mudah dan cepat, dan meningkatkan produktivitas karena memungkinkan pengguna

untuk mengakses sumber daya jaringan dari lokasi yang berbeda.

Namun, WLAN juga memiliki beberapa kelemahan, seperti keamanan yang kurang karena jaringan dapat diakses dari mana saja di area jangkauan nirkabel, dan kecepatan transfer data yang lebih lambat dibandingkan dengan jaringan kabel fisik. Selain itu, jangkauan nirkabel WLAN juga terbatas, dan pengguna mungkin memerlukan perangkat tambahan seperti repeater untuk memperluas jangkauan nirkabel.

b. Jaringan Kabel (Wired Network)

Meskipun sudah banyak orang yang menggunakan jaringan nirkabel, akan tetapi jaringan kabel masih menjadi pilihan untuk beberapa pihak dalam kebutuhan transmisi data. Dalam jaringan kabel, untuk menghubungkan antar perangkat jaringan maupun antara komputer ke komputer lain membutuhkan kabel untuk menghubungkannya. Gambaran jaringan kabel dapat dilihat pada Gambar 4.5.



Sumber: <https://www.bing.com>

Gambar 4.5. Jaringan kabel (*Wired Network*)

Ada beberapa jenis kabel jaringan yang digunakan untuk menghubungkan perangkat komputer dalam jaringan, di antaranya:

- 1) Kabel Coaxial: Kabel ini terdiri dari inti tembaga yang dilapisi dengan lapisan isolator, pelindung foil, dan lapisan luar berupa bahan PVC. Kabel ini sering digunakan pada jaringan kabel TV dan Ethernet 10BASE2.
- 2) Kabel UTP (Unshielded Twisted Pair): Kabel ini terdiri dari sepasang kabel tembaga yang dililitkan satu sama lain dan dilindungi oleh bahan PVC. Kabel UTP sering digunakan pada jaringan Ethernet dan biasanya tersedia dalam beberapa jenis kategori, seperti Cat5, Cat5e, Cat6, dan Cat7.

- 3) Kabel STP (Shielded Twisted Pair): Kabel ini hampir sama dengan UTP, namun memiliki lapisan pelindung tambahan untuk mengurangi gangguan elektromagnetik. Kabel STP sering digunakan pada jaringan dengan kebutuhan keamanan yang tinggi.
- 4) Kabel Fiber Optik: Kabel ini terdiri dari serat kaca atau plastik yang sangat tipis yang dapat menghantarkan sinyal cahaya. Kabel ini sering digunakan pada jaringan jarak jauh dan sangat cepat seperti jaringan *backbone* dan Internet.

4.3. Jaringan Komputer Berdasar Fungsinya

Pengelompokan jaringan berdasar fungsinya dapat dibagi menjadi tiga kategori, yaitu intranet, ekstranet, dan internet.

a. Intranet

Intranet adalah jaringan komputer pribadi yang digunakan oleh sebuah organisasi atau perusahaan untuk berbagi informasi, sumber daya, dan aplikasi antara anggota organisasi tersebut. Intranet biasanya menggunakan protokol dan teknologi yang sama dengan Internet, seperti TCP/IP, HTTP, dan HTML, tetapi

dibatasi hanya untuk pengguna yang terdaftar dan memiliki akses ke jaringan tersebut.

Intranet dapat membantu meningkatkan efisiensi dan produktivitas organisasi dengan memfasilitasi komunikasi dan kolaborasi antara anggota tim, serta memungkinkan akses cepat dan mudah ke informasi penting dan sumber daya seperti dokumen, database, dan aplikasi bisnis. Intranet juga dapat memfasilitasi pelatihan karyawan dan berbagai aktivitas internal lainnya. Gambaran jaringan intranet dapat dilihat pada Gambar 4.6.



Sumber: <https://www.bing.com>

Gambar 4.6. Jaringan intranet

Intranet biasanya dilindungi oleh berbagai sistem keamanan, seperti *firewall*, enkripsi data, dan otorisasi akses, untuk mencegah akses tidak

sah dan kebocoran data. Beberapa organisasi bahkan mengembangkan sistem intranet khusus yang dirancang untuk memenuhi kebutuhan spesifik mereka, seperti intranet untuk riset dan pengembangan, intranet untuk manajemen kualitas, dan sebagainya.

b. Ekstranet

Ekstranet adalah jaringan komputer yang memungkinkan organisasi untuk berbagi informasi, sumber daya, dan aplikasi dengan pihak eksternal, seperti pemasok, pelanggan, atau mitra bisnis. Ekstranet menggunakan teknologi yang sama dengan Internet, seperti TCP/IP, HTTP, dan HTML, namun dibatasi hanya untuk pengguna yang memiliki hak akses yang ditentukan. Gambaran jaringan ekstranet dapat dilihat pada Gambar 4.7.



Sumber: <https://www.bing.com>

Gambar 4.7. Jaringan ekstranet

Ekstranet dapat membantu meningkatkan efisiensi dan produktivitas organisasi dengan memfasilitasi kolaborasi dan berbagi informasi dengan pihak eksternal secara aman. Misalnya, sebuah perusahaan dapat menggunakan ekstranet untuk memberikan akses ke sistem inventori dan pengiriman kepada pemasok, atau untuk memungkinkan pelanggan untuk memesan produk dan melacak pengiriman.

Ekstranet biasanya dilindungi oleh berbagai sistem keamanan, seperti *firewall*, enkripsi data, dan otorisasi akses, untuk mencegah akses tidak sah dan kebocoran data. Pengguna eksternal juga dapat diberikan hak akses yang berbeda-beda, tergantung pada jenis dan tingkat kepentingan informasi yang dibagikan.

Ekstranet juga dapat membantu meningkatkan hubungan antara organisasi dan pihak eksternal, karena memfasilitasi komunikasi dan kolaborasi yang lebih efektif dan transparan.

c. Internet

Istilah internet berasal dari kata *Interconnected Network*. Pengertian Internet adalah salah satu jenis jaringan komputer yang merupakan wadah komunikasi secara global dan menghubungkan

antara satu komputer dengan komputer lainnya. Internet adalah jaringan global yang terdiri dari jutaan jaringan komputer yang saling terhubung menggunakan protokol Internet. Internet memungkinkan komunikasi dan pertukaran informasi antara pengguna dari seluruh dunia, serta menyediakan akses ke berbagai sumber daya, seperti situs web, email, layanan pesan instan, media sosial, dan banyak lagi. Gambaran jaringan internet dapat dilihat pada Gambar 4.8.



Sumber: <https://www.bing.com>

Gambar 4.8. Jaringan internet

Internet memudahkan para pengguna dari seluruh dunia dalam mendistribusikan informasi dengan mengandalkan frekuensi dan transmisi sinyal. Internet didasarkan pada teknologi TCP/IP (*Transmission Control Protocol/Internet Protocol*), yang memungkinkan pengiriman dan penerimaan paket data antar jaringan komputer

yang berbeda-beda. Setiap jaringan dan perangkat di internet diberi alamat unik, yang disebut alamat IP, yang digunakan untuk mengirim dan menerima data.

Internet memiliki banyak manfaat, seperti memfasilitasi pertukaran informasi dan ide, meningkatkan koneksi antar manusia, memungkinkan akses ke sumber daya dan layanan global, dan mempercepat kemajuan teknologi dan inovasi.

Namun, internet juga memiliki beberapa risiko dan tantangan, seperti risiko keamanan dan privasi, penyebaran informasi palsu dan tidak akurat, kecanduan media sosial, dan sebagainya. Oleh karena itu, penting untuk menggunakan internet secara bertanggung jawab dan memperhatikan keamanan dan privasi data pribadi.

BAB V

MEDIA TRANSMISI JARINGAN KOMPUTER

Pernahkah Anda membayangkan bagaimana sebuah remote dapat mengoperasikan televisi? Atau seseorang yang bisa saling berkomunikasi dengan telepon seluler. Ternyata semua kemudahan itu bisa terjadi karena adanya media transmisi. Kami contohkan seperti saat Anda ingin mengirimkan paket ke seseorang. Maka, Anda memerlukan pengantar, bukan? Nah katakanlah itu sebagai jasa antar. Nah, jasa antar itu sama halnya dengan media atau jalur, sehingga nantinya paket bisa sampai ke penerima dengan baik. Sementara itu, remote televisi dan telepon selular dapat beroperasi karena memiliki media. Tentu saja jenis media yang digunakan yaitu gelombang. Ada banyak juga contoh perangkat lain yang memakai jalur transmisi data.

Media transmisi adalah media yang menghubungkan antara pengirim dan penerima informasi (data), karena jarak yang jauh, maka data terlebih dahulu diubah menjadi kode/ isyarat, dan isyarat inilah yang akan dimanipulasi dengan berbagai

macam cara untuk diubah kembali menjadi data. Dalam terminology jaringan komputer media transmisi adalah saluran antara pemancar atau pemberi sinyal data dan penerima data. Saluran tersebut menjadi penghubung data yang dikirim dari satu tempat ke tempat lain. Media transmisi dalam jaringan komputer mengacu pada fisik atau saluran yang digunakan untuk mentransfer data antara perangkat komputer. Media transmisi ini dapat berbeda dalam jenis, kecepatan, jarak, dan karakteristik lainnya.

5.1. Kegunaan Media Transmisi

- Media transmisi digunakan pada beberapa peralatan elektronika untuk menghubungkan antara pengirim dan penerima supaya dapat melakukan pertukaran data.
- Beberapa alat elektronika, seperti telepon, komputer, televisi, dan radio membutuhkan media transmisi untuk dapat menerima data. Seperti pada pesawat telepon, media transmisi yang digunakan untuk menghubungkan dua buah telepon adalah kabel.
- Setiap peralatan elektronika memiliki media transmisi yang berbeda-beda dalam pengiriman datanya.

Karakteristik Media Transmisi bergantung

pada:

- Jenis alat elektronika
- Data yang digunakan oleh alat elektronika tersebut
- Tingkat keefektifan dalam pengiriman data
- Ukuran data yang dikirimkan

Faktor-faktor yang berhubungan dengan media transmisi dan sinyal sebagai penentu kecepatan dan jarak:

1. Bandwidth (lebar jalur). Semakin besar bandwidth sinyal, semakin besar data yang dapat ditangani.
2. Kemampuan menghadapi gangguan listrik maupun magnetis dari luar.
3. Kemampuan dalam melayani multiple acces yaitu apakah mudah mengambil data dari padanya.
4. Keamanan data

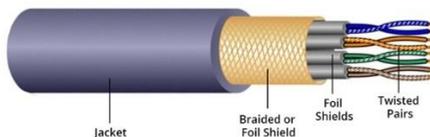
Media transmisi secara luas diklasifikasikan ke dalam 2 jenis, yaitu media transmisi fisik dan media non-fisik.

5.2. Media Transmisi Fisik

Media transmisi fisik biasa disebut juga sebagai media transmisi wired atau bounded. Sinyal data dari pengirim ditransmisikan, diarahkan, dan dibatasi dalam jalur sempit dengan menggunakan tautan fisik, berupa kabel atau bahan konduktor. Karakteristik dari media transmisi fisik adalah memiliki kecepatan transfer data yang tinggi, aman, dan umumnya untuk jarak yang relatif lebih pendek. Yang termasuk dalam media transmisi fisik pada jaringan adalah kabel twisted pair, kabel coaxial, kabel fiber optik, stripline, dan microstripline.

1. Kabel Twisted Pair

Kabel twisted pair termasuk media transmisi fisik yang paling banyak digunakan. Kabel twisted pair adalah jenis kabel yang terdiri dari 2 kabel konduktor berinsulasi terpisah yang dililitkan satu sama lain. Umumnya, beberapa pasang kabel dibundel bersama dalam selubung pelindung.



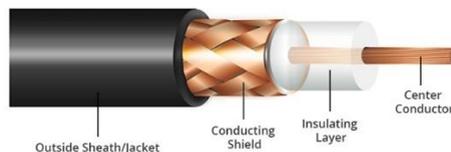
Sumber: www.community.fs.com

Twisted pair terdiri atas 2 jenis, yakni Unshielded Twisted Pair (UTP) dan Shielded Twisted Pair (STP).

- **Unshielded Twisted Pair (UTP):** UTP terdiri dari dua kabel tembaga terisolasi yang dipilin satu sama lain. Jenis kabel ini memiliki kemampuan untuk memblokir interferensi dan tidak bergantung pada pelindung fisik. Kabel ini digunakan untuk telepon.
- **Shielded Twisted Pair (STP):** Jenis kabel ini terdiri dari pelindung khusus (penutup jalinan tembaga atau pelindung foil) untuk memblokir gangguan eksternal. Kabel ini digunakan dalam Ethernet berkecepatan data tinggi. Selain itu dipakai pada saluran telepon.

2. Kabel Coaxial

Kabel coaxial adalah kabel yang memiliki penutup plastik luar yang berisi lapisan insulasi yang terbuat dari PVC dan 2 konduktor paralel masing-masing memiliki penutup pelindung terisolasi yang terpisah.



Sumber: www.community.fs.com

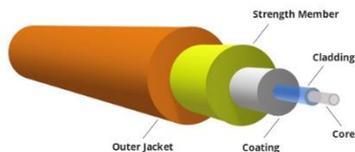
Kabel coaxial mentransmisikan informasi dalam dua mode, yakni:

- Baseband (bandwidth kabel khusus)
- Broadband (bandwidth kabel dibagi menjadi rentang terpisah).

TV kabel dan jaringan televisi analog adalah contoh perangkat komunikasi yang banyak menggunakan kabel coaxial. Kelebihan dari kabel coaxial, yaitu memiliki bandwidth yang tinggi, lebih kebal terhadap noise yang mengganggu jaringan, mudah dipasang dan diperluas, serta murah.

3. Kabel Fiber Optik

Kabel fiber optik adalah jenis kabel transmisi yang menggunakan konsep pemantulan cahaya melalui inti yang terbuat dari kaca atau plastik. Inti dikelilingi oleh kaca atau penutup plastik yang kurang padat yang disebut cladding. Kabel ini umumnya digunakan untuk transmisi data dalam jumlah besar.



Sumber: www.community.fs.com

Kabel fiber bisa searah atau dua arah. WDM (Wavelength Division Multiplexer) mendukung dua mode, yaitu mode satu arah dan dua arah. Kelebihan dari kabel fiber adalah sebagai berikut:

- Kapasitas dan bandwidth-nya cukup besar
- Ringan
- Lebih sedikit redaman sinyal
- Kebal terhadap interferensi elektromagnetik
- Tahan terhadap bahan korosif

4. Stripline

Stripline adalah media saluran transmisi elektromagnetik transversal yang ditemukan oleh Robert M. Barrett dari Pusat Penelitian Angkatan Udara Cambridge pada 1950-an. Stripline adalah bentuk paling awal dari saluran transmisi planar. Stripline menggunakan bahan konduktor untuk mengirimkan gelombang frekuensi tinggi yang disebut waveguide. Bahan konduktor ini diapit di antara dua lapisan bidang tanah untuk meredam gangguan elektromagnetik atau Electromagnetic Interference (EMI)

5. Microstripline

Microstripline adalah jenis saluran transmisi yang terdiri dari konduktor yang dibuat pada substrat dielektrik dengan bidang ground. Microstripline dikembangkan oleh laboratorium ITT sebagai pesaing stripline dan pertama kali diterbitkan oleh Grieg dan Engelmann pada prosiding IRE Desember 1952.

5.3. Media Transmisi Non-Fisik

Media transmisi non-fisik juga disebut sebagai media transmisi wireless atau unbounded. Media ini mengandalkan gelombang elektromagnetik dan tidak memerlukan media fisik untuk transmisi sinyal data. Karakteristik dari media jenis ini adalah sinyal disiarkan melalui udara, cenderung kurang aman, dan dapat digunakan untuk jarak yang lebih jauh.

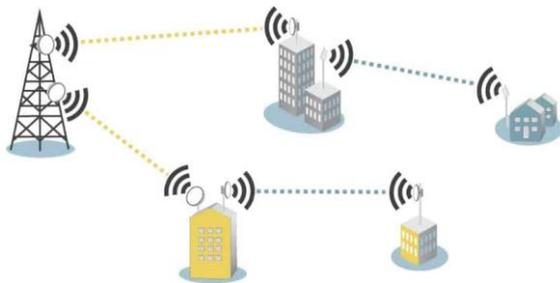


Sumber: www.freepik.com

Banyak pengguna memilih media transmisi wireless karena lebih nyaman daripada memasang kabel. Selain itu, banyak bisnis telekomunikasi yang menggunakan media transmisi wireless pada lokasi yang tidak memungkinkan untuk dipasangi kabel. media transmisi non-fisik pada jaringan adalah gelombang radio, gelombang micro, infrared, dan satelit komunikasi.

1. Gelombang Radio

Gelombang Radio (radiowave) adalah media transmisi wireless yang mendistribusikan sinyal radio melalui udara dalam jarak jauh seperti antar kota, wilayah, dan negara. Juga dapat digunakan pada jarak pendek seperti di dalam kantor atau rumah. Teknologi komunikasi Bluetooth, UWB, Wi-Fi, dan WiMAX menggunakan sinyal gelombang radio untuk mengirimkan data.



Sumber: <https://midteknologi.com/>

2. Gelombang Micro

Gelombang mikro (microwave) adalah gelombang radio yang menyediakan transmisi sinyal berkecepatan tinggi. Gelombang mikro dapat mengirimkan data dengan kecepatan hingga 4.500 kali lebih cepat daripada modem dial-up. Sebuah stasiun gelombang mikro adalah piringan reflektif yang berisi antena, transceiver, dan peralatan lain yang diperlukan untuk komunikasi gelombang mikro. Gelombang mikro menggunakan transmisi line-of-sight. Untuk menghindari kemungkinan penghalang, seperti gedung atau gunung, stasiun gelombang mikro sering ditempatkan di puncak gedung, menara, atau gunung.

Transmisi gelombang mikro digunakan di lingkungan di mana pemasangan media transmisi fisik sulit atau mustahil dilakukan. Misalnya, transmisi gelombang mikro digunakan di area terbuka lebar seperti gurun atau danau; antara bangunan di wilayah geografis yang dekat; atau untuk berkomunikasi dengan satelit. Pengguna transmisi gelombang mikro saat ini seperti universitas, rumah sakit, pemerintah

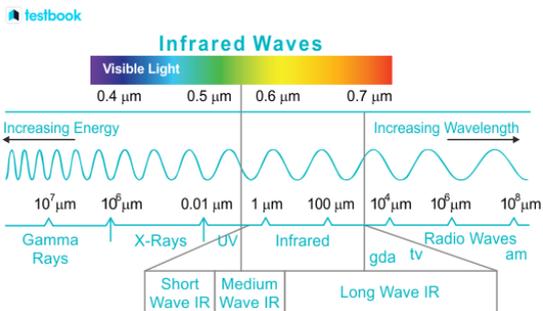
kota, penyedia televisi kabel, dan perusahaan telepon.

Jenis Gelombang	Frekuensi (Hz)
Sinar gamma	$10^{20} - 10^{25}$
Sinar-X	$10^{16} - 10^{20}$
Sinar UV	$10^{15} - 10^{16}$
Cahaya tampak	10^{15}
Sinar inframerah	$10^{12} - 10^{15}$
Gelombang mikro	$10^9 - 10^{12}$
Gelombang radio	$< 10^{12}$

Sumber: <https://roboguru.ruangguru.com/>

3. Infrared

Infrared (IR) adalah media transmisi nirkabel yang mengirimkan sinyal menggunakan gelombang cahaya infrared. Komputer dan perangkat seluler, seperti mouse, printer, dan ponsel pintar, sering kali memiliki port IrDA yang memungkinkan transfer data dari satu perangkat ke perangkat lain menggunakan gelombang cahaya infrared.

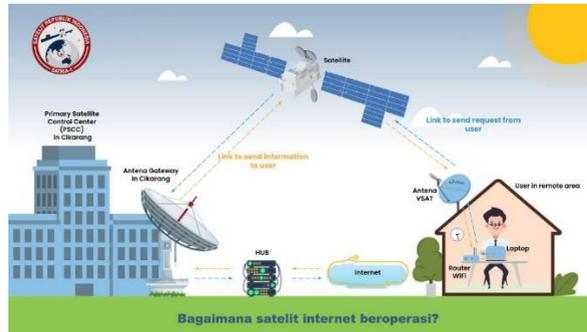


Sumber: <https://testbook.com/>

4. Satelit

Satelit komunikasi adalah stasiun ruang angkasa yang menerima sinyal gelombang mikro dari stasiun berbasis bumi, memperkuat (memperkuat) sinyal, dan memancarkan sinyal kembali ke area yang luas ke sejumlah stasiun earth-based. Stasiun earth-based ini sering kali merupakan stasiun gelombang mikro. Perangkat lain, seperti ponsel pintar dan penerima GPS, juga dapat berfungsi sebagai stasiun earth-based. Transmisi dari stasiun earth-based ke satelit adalah uplink. Transmisi dari satelit ke stasiun earth-based adalah downlink.

Aplikasi seperti navigasi udara, siaran televisi dan radio, prakiraan cuaca, konferensi video, sistem GPS, dan koneksi internet menggunakan satelit komunikasi. Dengan parabola yang tepat dan kartu modem satelit, konsumen mengakses internet menggunakan teknologi satelit. Namun, dengan koneksi internet satelit, transmisi uplink biasanya lebih lambat daripada transmisi downlink.



Sumber: <https://www.kominfo.go.id/>

Perbedaan kecepatan ini biasanya dapat diterima oleh sebagian besar pengguna satelit internet karena mereka cenderung mengunduh lebih banyak data daripada unggah data. Meskipun koneksi internet satelit lebih mahal daripada koneksi internet kabel atau DSL, terkadang ini adalah satu-satunya pilihan internet berkecepatan tinggi di daerah terpencil. Pemahaman tentang berbagai jenis media transmisi dan cara mengelolanya sangat penting dalam perancangan dan pemeliharaan jaringan komputer yang efisien. Hal ini akan memungkinkan jaringan komputer berfungsi dengan baik dan memenuhi kebutuhan komunikasi data yang semakin kompleks.

BAB VI

TOPOLOGI JARINGAN KOMPUTER

6.1. Deskripsi Topology Jaringan

Topologi jaringan komputer adalah susunan fisik dan logis dari perangkat keras dan koneksi jaringan yang terdiri dari beberapa komputer dan perangkat lainnya. Topologi jaringan menentukan bagaimana perangkat-perangkat dalam jaringan tersebut terhubung dan berkomunikasi satu sama lain.

Topologi jaringan dapat berbeda-beda tergantung pada kebutuhan dan keadaan khusus organisasi, serta faktor seperti biaya, keandalan, dan efisiensi yang diinginkan. Beberapa topologi jaringan yang umum digunakan adalah topologi bus, topologi star, topologi ring, topologi mesh, dan topologi tree.

Dalam topologi jaringan, setiap perangkat dalam jaringan memiliki peran penting dalam pengiriman data. Jaringan tersebut harus dapat diatur dengan baik agar tidak terjadi bentrok atau konflik yang dapat menghambat kinerja jaringan. Oleh karena itu, pemilihan topologi jaringan yang tepat sangat penting untuk memastikan keamanan, keandalan, dan efisiensi jaringan.

Topologi jaringan komputer merujuk pada susunan fisik dan logis dari perangkat keras dan koneksi jaringan yang terdiri dari beberapa komputer dan perangkat lainnya. Beberapa topologi jaringan yang umum digunakan adalah:

1. Topologi Bus.
2. Topologi Star.
3. Topologi Ring.
4. Topologi Mesh.
5. Topologi Tree.

Pilihan topologi jaringan tergantung pada kebutuhan dan keadaan khusus organisasi, serta faktor seperti biaya, keandalan, dan efisiensi yang diinginkan.

6.2. Topologi BUS

Topologi bus adalah salah satu jenis topologi jaringan komputer di mana semua perangkat dihubungkan ke bus tunggal (kabel). Informasi dikirim melalui kabel ke setiap perangkat yang terhubung. Topologi bus sangat sederhana dan mudah diimplementasikan.

Kelebihan topologi bus antara lain:

1. Murah: Karena hanya memerlukan satu kabel sebagai media transmisi, topologi bus relatif murah untuk diimplementasikan.
2. Mudah diimplementasikan: Konfigurasi jaringan pada topologi bus sangat sederhana dan mudah diimplementasikan.
3. Mudah dikembangkan: Topologi bus memungkinkan pengembangan jaringan dengan menambahkan simpul baru dengan mudah.

Topologi bus juga memiliki kelemahan, seperti:

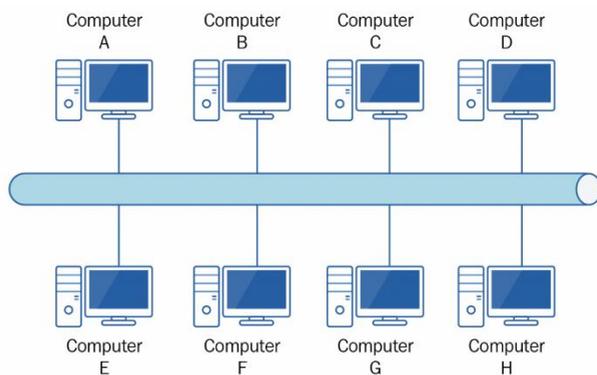
1. Kinerja yang buruk: Jika terdapat banyak perangkat yang terhubung ke bus tunggal, kinerja jaringan dapat menurun.
2. Rentan terhadap kesalahan: Jika terdapat kesalahan pada kabel, keseluruhan jaringan dapat terganggu.
3. Tidak fleksibel: Topologi bus tidak fleksibel dalam hal penambahan dan perubahan konfigurasi jaringan.

Implementasi topologi bus cocok untuk jaringan kecil hingga menengah yang tidak memerlukan performa yang tinggi. Topologi bus dapat diimplementasikan dalam lingkup kantor kecil, seperti

kantor-kantor cabang atau kantor-kantor dengan jumlah pengguna yang tidak terlalu banyak. Namun, untuk jaringan dengan performa yang lebih tinggi dan jumlah pengguna yang banyak, sebaiknya mempertimbangkan topologi jaringan yang lebih canggih seperti topologi star atau mesh.

Cara kerja dari topologi jaringan Bus adalah sebagai berikut:

1. Semua komputer dalam jaringan terhubung ke backbone atau kabel induk yang sama.
2. Sinyal atau data yang dikirimkan dari salah satu komputer akan disebarkan ke seluruh komputer dalam jaringan melalui kabel induk atau backbone.
3. Setiap komputer dalam jaringan dapat mengakses data atau sinyal yang dikirimkan oleh komputer lainnya yang terhubung pada kabel induk yang sama.
4. Di setiap ujung kabel induk, terminator dipasang untuk mencegah sinyal yang dikirimkan kembali ke kabel dan memastikan bahwa data atau sinyal hanya diteruskan ke komputer yang dituju.



Gambar 6.1. Topologi Bus

6.3. Topologi Star

Topologi star adalah salah satu jenis topologi jaringan komputer di mana semua perangkat dihubungkan ke pusat atau hub tunggal. Pusat atau hub ini bertanggung jawab untuk mengirimkan data dari satu perangkat ke perangkat lainnya dalam jaringan.

Kelebihan topologi star antara lain:

1. Mudah diimplementasikan: Topologi star sangat mudah diimplementasikan, bahkan oleh pengguna yang tidak memiliki pengetahuan teknis yang mendalam.
2. Mudah dikelola: Karena semua perangkat terhubung ke satu titik pusat, topologi star sangat mudah dikelola dan dimonitor.

3. Tahan terhadap kesalahan: Jika terdapat kesalahan pada satu perangkat dalam jaringan, hanya perangkat tersebut yang terpengaruh dan tidak mempengaruhi perangkat lain dalam jaringan.

Topologi star juga memiliki kelemahan, seperti:

1. Ketergantungan pada titik pusat: Jika pusat atau hub mengalami kerusakan, seluruh jaringan dapat terganggu.
2. Biaya yang lebih tinggi: Topologi star memerlukan biaya yang lebih tinggi untuk diimplementasikan dibandingkan dengan topologi bus.
3. Keterbatasan jarak: Jarak antara perangkat dan pusat harus terbatas karena penggunaan kabel.

Topology jaringan Star banyak digunakan dalam kehidupan sehari-hari, terutama dalam koneksi jaringan komputer di rumah, kantor, atau bahkan di tempat umum seperti cafe atau pusat perbelanjaan.

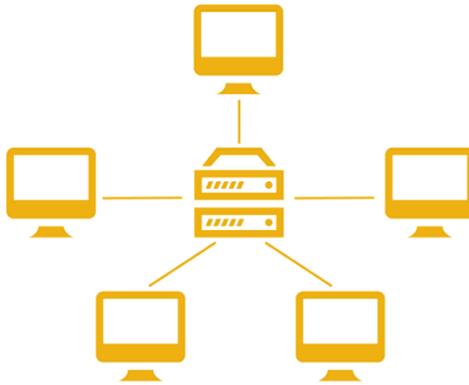
Cara kerja dari topologi jaringan Star adalah sebagai berikut:

1. Setiap komputer dalam jaringan terhubung ke sebuah perangkat pusat yang disebut dengan

switch atau hub melalui kabel yang berbeda-beda.

2. Switch atau hub menjadi pusat kontrol dalam jaringan dan memungkinkan setiap komputer untuk berkomunikasi dengan komputer lainnya dalam jaringan.
3. Data atau sinyal yang dikirimkan dari satu komputer akan terlebih dahulu diterima oleh switch atau hub dan kemudian diteruskan ke komputer yang dituju.
4. Jika ada masalah pada koneksi antara satu komputer dengan switch atau hub, komputer lain dalam jaringan masih dapat terhubung dan berfungsi normal.

Contoh penggunaan topologi jaringan Star dalam kehidupan sehari-hari adalah dalam jaringan komputer di rumah. Setiap komputer dihubungkan dengan router sebagai pusat kontrol jaringan dan router akan memastikan bahwa setiap komputer dapat terhubung dengan komputer lainnya dalam jaringan. Dalam jaringan di kantor, switch atau hub digunakan sebagai pusat kontrol untuk menghubungkan beberapa komputer dan perangkat lainnya dalam satu jaringan yang sama.



Gambar 6.2. Topologi Star

6.4. Topologi Ring

Topologi ring adalah jenis topologi jaringan komputer di mana setiap perangkat dihubungkan dengan perangkat lainnya membentuk lingkaran atau cincin. Setiap perangkat hanya terhubung dengan dua perangkat lainnya, satu perangkat di sebelah kiri dan satu perangkat di sebelah kanan. Data dikirimkan dalam satu arah sepanjang jalur cincin.

Kelebihan dari topologi ring antara lain:

1. Tidak ada tabrakan data: Karena data hanya bergerak dalam satu arah, tidak ada tabrakan data yang terjadi.
2. Kinerja yang baik: Topologi ring memiliki kinerja yang baik pada jaringan yang berukuran sedang.

3. Pemasangan yang mudah: Topologi ring mudah dipasang dan dikelola karena hanya terdapat sedikit perangkat yang harus dihubungkan.

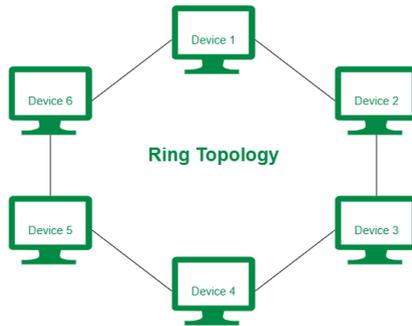
Namun, topologi ring juga memiliki beberapa kekurangan, seperti:

1. Ketergantungan pada satu perangkat: Jika satu perangkat gagal, maka seluruh jaringan akan terganggu.
2. Biaya yang lebih tinggi: Topologi ring memerlukan kabel yang lebih panjang dan mahal untuk diimplementasikan dibandingkan dengan topologi bus atau star.
3. Pengelolaan yang sulit: Jika terjadi gangguan dalam jaringan, pemecahan masalah mungkin memerlukan waktu yang lebih lama.

Cara pemasangan topologi ring melibatkan menghubungkan setiap perangkat dalam lingkaran menggunakan kabel. Setiap perangkat harus dihubungkan dengan perangkat sebelahnya dan harus ada koneksi yang lengkap di seluruh lingkaran. Data kemudian dikirimkan sepanjang jalur cincin.

Contoh implementasi topologi ring termasuk jaringan telepon, jaringan kabel televisi, dan jaringan

optik yang digunakan dalam aplikasi jaringan data dan telekomunikasi. Topologi ini juga cocok untuk digunakan pada jaringan dengan sedikit pengguna yang tersebar di lokasi yang berbeda seperti perusahaan atau kampus yang terletak di berbagai lokasi yang berbeda.



Gambar 6.3. Topologi Ring

6.5. Topologi Mesh

Topologi Mesh adalah jenis topologi jaringan komputer yang memiliki setiap perangkat dihubungkan dengan semua perangkat lainnya dalam jaringan. Setiap perangkat dalam topologi ini bekerja sebagai penerima dan pengirim data. Jadi, jika ada beberapa perangkat yang mengalami kerusakan atau tidak dapat diakses, perangkat lain dapat terus beroperasi.

Karakteristik topologi Mesh antara lain:

- 1) Setiap perangkat dihubungkan dengan semua perangkat lain dalam jaringan.

- 2) Jaringan memiliki redundansi yang tinggi sehingga dapat terus beroperasi bahkan jika beberapa perangkat mengalami kerusakan.
- 3) Pemasangan topologi Mesh membutuhkan kabel yang lebih banyak dibandingkan dengan topologi lainnya.

Kelebihan topologi Mesh antara lain:

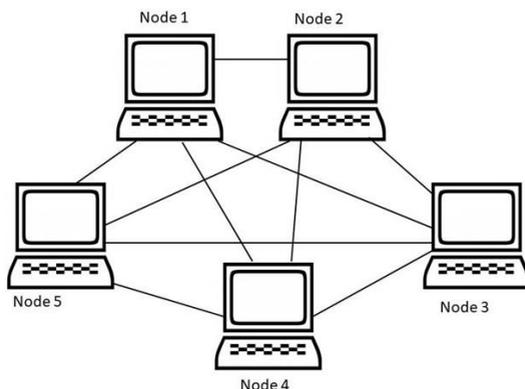
- 1) Kinerja jaringan yang sangat baik karena tidak ada tabrakan data.
- 2) Jaringan memiliki redundansi yang tinggi sehingga dapat terus beroperasi bahkan jika ada beberapa perangkat yang tidak dapat diakses.
- 3) Jaringan memiliki keamanan yang tinggi karena tidak ada perangkat yang memiliki kontrol penuh atas jaringan.

Kekurangan topologi Mesh antara lain:

- 1) Biaya yang lebih tinggi dibandingkan dengan topologi lainnya karena memerlukan lebih banyak kabel.
- 2) Pemasangan dan pengelolaan jaringan yang lebih sulit dibandingkan dengan topologi lainnya.

Cara pemasangan topologi Mesh melibatkan menghubungkan setiap perangkat ke semua perangkat lain dalam jaringan. Pemasangan ini memerlukan kabel yang lebih banyak dan lebih kompleks dibandingkan dengan topologi lainnya. Selain itu, konfigurasi perangkat dalam jaringan juga lebih sulit.

Implementasi topologi Mesh biasanya digunakan pada jaringan komputer dengan skala besar seperti jaringan di pusat data, atau jaringan komputer untuk sejumlah besar organisasi yang berbeda seperti kampus besar atau pusat perbelanjaan. Topologi Mesh juga digunakan pada jaringan komunikasi satelit, karena jaringan harus memiliki redundansi yang tinggi untuk memastikan keandalan komunikasi.



Gambar 6.4. Topologi Mesh

6.6. Topologi Tree

Topologi Tree, juga dikenal sebagai topologi Hierarchical, adalah jenis topologi jaringan komputer yang menggabungkan beberapa topologi Bus dalam jaringan yang lebih besar. Jaringan dalam topologi ini memiliki hierarki dengan beberapa perangkat yang bertindak sebagai "switch" atau "hub" untuk menghubungkan beberapa topologi Bus.

Karakteristik topologi Tree antara lain:

- 1) Topologi Tree menggabungkan beberapa topologi Bus dalam satu jaringan yang lebih besar.
- 2) Hierarki dalam jaringan dimulai dari perangkat paling atas, yang bertindak sebagai switch atau hub, dan berlanjut ke bawah dengan topologi Bus yang terhubung ke perangkat di atasnya.
- 3) Jaringan dalam topologi Tree dapat memiliki jumlah perangkat yang besar dan jarak yang jauh.

Kelebihan topologi Tree antara lain:

- 1) Jaringan Tree dapat menangani jumlah perangkat yang besar dan jarak yang jauh.

- 2) Topologi Tree memiliki struktur hierarki yang memudahkan pengelolaan dan pemeliharaan jaringan.
- 3) Jaringan Tree dapat menangani tabrakan data karena setiap perangkat di topologi Bus memiliki saluran terpisah untuk mengirimkan data.

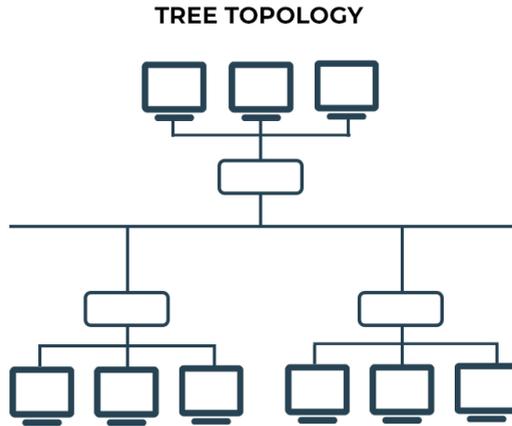
Kekurangan topologi Tree antara lain:

- 1) Topologi Tree memerlukan investasi yang lebih besar dibandingkan dengan topologi Bus.
- 2) Jika perangkat switch atau hub paling atas mengalami kerusakan, seluruh jaringan yang terhubung dapat terpengaruh.

Cara pemasangan topologi Tree melibatkan penggabungan beberapa topologi Bus menjadi satu jaringan Tree. Perangkat switch atau hub paling atas digunakan untuk menghubungkan setiap topologi Bus ke jaringan yang lebih besar. Seluruh jaringan kemudian diatur secara hierarkis.

Implementasi topologi Tree biasanya digunakan pada jaringan yang memerlukan hierarki dan skala besar seperti jaringan di kampus atau organisasi besar. Topologi ini juga sering digunakan dalam jaringan telekomunikasi dan penyedia layanan internet (ISP)

karena memungkinkan untuk menghubungkan beberapa topologi Bus dalam jaringan yang lebih besar dan lebih terorganisir.



Gambar 6.5. Topologi Tree

BAB VII

KONSEP DASAR PROTOKOL TCP/IP

7.1. Asal Mula TCP/IP

Asal mula protokol TCP/IP (Transmission Control Protocol/Internet Protocol) berakar dari sejarah perkembangan komunikasi jaringan dan penelitian di Amerika Serikat selama era Perang Dingin. Berikut adalah ikhtisar singkat tentang asal mula TCP/IP:

1. DARPA dan ARPANET (1960-an): Pada tahun 1960-an, Departemen Pertahanan Amerika Serikat (Department of Defense, DoD) mendirikan Advanced Research Projects Agency (ARPA), yang kemudian dikenal sebagai DARPA (Defense Advanced Research Projects Agency). Salah satu proyek besar DARPA adalah ARPANET (Advanced Research Projects Agency Network), yang merupakan jaringan komunikasi data eksperimental pertama yang memungkinkan komputer di lokasi yang berbeda untuk berkomunikasi satu sama lain. ARPANET adalah embrio dari apa yang nantinya akan menjadi Internet.

2. Pembangunan Protokol NCP: Pada awalnya, ARPANET menggunakan protokol NCP (Network Control Program) untuk mengatur komunikasi antar komputer. Meskipun efektif, NCP memiliki beberapa keterbatasan, terutama dalam hal skalabilitas.
3. Pengembangan TCP/IP oleh Vinton Cerf dan Robert Kahn (1970-an): Pada pertengahan tahun 1970-an, Vinton Cerf dari Stanford University dan Robert Kahn dari DARPA mengembangkan protokol TCP (Transmission Control Protocol) yang lebih kuat dan fleksibel. TCP memungkinkan komunikasi yang handal antar komputer dalam jaringan yang tidak selalu dapat diandalkan.
4. Penggabungan dengan IP: Protokol TCP dikombinasikan dengan protokol IP (Internet Protocol), yang dikembangkan oleh Bob Metcalfe dan David Boggs di Xerox PARC, untuk membentuk protokol TCP/IP. TCP bertanggung jawab untuk pengiriman data yang handal, sementara IP bertanggung jawab untuk pengalamatan dan routing data.
5. Uji Coba Awal dan Penyebaran: Protokol TCP/IP pertama kali diimplementasikan dalam

ARPANET pada tahun 1977. Ini memungkinkan pengiriman data yang lebih andal dan lebih efisien. Setelah itu, protokol TCP/IP terus ditingkatkan dan diadopsi oleh berbagai jaringan komunikasi yang terkait dengan pemerintah, universitas, dan lembaga penelitian di seluruh Amerika Serikat.

6. Standar Internasional: Pada tahun 1983, ARPANET beralih sepenuhnya ke TCP/IP, dan pada saat yang sama, Domain Name System (DNS) juga diperkenalkan untuk memudahkan penggunaan nama domain alih-alih alamat IP numerik. Selama periode ini, TCP/IP mulai menjadi standar internasional untuk komunikasi jaringan.
7. Pembentukan Internet: Dengan adopsi luas protokol TCP/IP dan pengembangan lebih lanjut, Internet pun lahir. Internet menjadi lebih terbuka dan dapat diakses oleh masyarakat umum, dan telah mengubah cara dunia berkomunikasi dan berinteraksi.

Sekarang, TCP/IP adalah kerangka kerja protokol yang mendasari Internet dan telah berkembang menjadi jaringan global yang menghubungkan miliaran

perangkat dan pengguna di seluruh dunia. Asal mula TCP/IP adalah tonggak penting dalam sejarah teknologi informasi dan komunikasi.

7.2. Relevansi TCP/IP di Era Modern

Protokol TCP/IP (Transmission Control Protocol/Internet Protocol) tetap sangat relevan di era modern, bahkan semakin penting seiring dengan perkembangan teknologi informasi dan komunikasi. Berikut adalah beberapa alasan mengapa TCP/IP masih sangat relevan di era digital saat ini:

1. **Dasar Internet Modern:** TCP/IP adalah kerangka kerja protokol yang mendasari Internet modern. Semua layanan dan aplikasi yang kita gunakan secara luas, seperti email, web browsing, media sosial, perbankan online, dan banyak lagi, bergantung pada TCP/IP. Oleh karena itu, TCP/IP adalah pondasi dari semua aktivitas online kita.
2. **Kemampuan Komunikasi Antar Platform:** Salah satu kekuatan TCP/IP adalah kemampuannya untuk mendukung komunikasi antar berbagai platform dan perangkat keras. Dalam era modern, di mana kita menggunakan berbagai jenis perangkat, termasuk komputer,

smartphone, tablet, IoT (Internet of Things) devices, dan lainnya, kemampuan TCP/IP untuk menghubungkan semuanya adalah kunci.

3. Keamanan Jaringan: Protokol TCP/IP telah berkembang seiring dengan kebutuhan akan keamanan jaringan yang semakin kompleks. Sebagai contoh, protokol HTTPS (HTTP Secure) adalah aplikasi dari TCP/IP yang memungkinkan komunikasi web yang aman melalui enkripsi data. Demikian pula, protokol VPN (Virtual Private Network) berdasarkan TCP/IP digunakan untuk menciptakan koneksi jaringan yang aman.
4. Skalabilitas: TCP/IP dirancang dengan kemampuan untuk mengatasi skalabilitas yang tinggi. Ini memungkinkan jaringan modern, termasuk Internet, untuk tumbuh secara signifikan dan mendukung miliaran perangkat yang terhubung secara bersamaan.
5. Inovasi Teknologi: Meskipun telah ada sejak lama, TCP/IP terus mengalami pengembangan dan pembaruan. Ini memungkinkannya untuk mengikuti perkembangan teknologi baru seperti IPv6 (versi baru dari protokol IP) yang dirancang

untuk mengatasi masalah kehabisan alamat IP dalam IPv4.

6. Basis untuk Aplikasi Baru: Ketika kita melihat aplikasi baru seperti Internet of Things (IoT), mobil otonom, dan kecerdasan buatan (AI), semua aplikasi ini menggunakan TCP/IP sebagai dasar komunikasi mereka. Ini menunjukkan fleksibilitas dan relevansi TCP/IP dalam mendukung teknologi baru.
7. Peran dalam Bisnis dan E-Commerce: Bisnis dan perdagangan elektronik (e-commerce) yang semakin berkembang bergantung pada jaringan yang andal dan aman, yang dibangun di atas TCP/IP. Protokol ini memfasilitasi transaksi bisnis, transfer data pelanggan, dan kegiatan e-commerce lainnya.
8. Internet Seluler: Jaringan seluler seperti 4G dan 5G juga menggunakan TCP/IP sebagai dasar komunikasi mereka. Dengan peningkatan penggunaan perangkat seluler, TCP/IP tetap relevan dalam menghubungkan perangkat seluler dengan jaringan Internet.

Dengan semua faktor ini, TCP/IP tetap menjadi tonggak utama dalam infrastruktur jaringan global dan

akan tetap relevan dalam era digital yang semakin maju dan terkoneksi secara global.

7.3. Model TCP/IP

Model TCP/IP (Transmission Control Protocol/Internet Protocol) adalah kerangka kerja protokol komunikasi yang digunakan dalam jaringan komputer untuk menghubungkan dan mengoordinasikan komunikasi antar perangkat dalam jaringan. Model ini menggambarkan cara data dikirim, diterima, dan diproses dalam jaringan. Model TCP/IP terdiri dari empat layer (atau layer dalam beberapa definisi) yang memecah fungsi jaringan menjadi bagian-bagian yang lebih kecil. Berikut adalah komponen utama dalam Model TCP/IP:

1. Layer Jaringan (Network Layer): Ini adalah layer pertama dalam Model TCP/IP dan bertanggung jawab atas pengiriman paket data dari satu node ke node lain dalam jaringan. Layer ini menggunakan alamat IP (Internet Protocol) untuk mengarahkan paket data ke tujuan yang tepat. Layer Jaringan juga dapat mencakup protokol seperti ICMP (Internet Control Message Protocol) untuk mengirim pesan kesalahan dan pengelolaan routing.

2. Layer Transport (Transport Layer): Layer ini mengatur komunikasi antara dua perangkat yang berkomunikasi dalam jaringan. Dalam Model TCP/IP, ada dua protokol transport utama yang digunakan: TCP (Transmission Control Protocol) dan UDP (User Datagram Protocol). TCP menyediakan komunikasi yang handal dan terjamin dengan pemulihan kesalahan dan pengaturan aliran data, sementara UDP adalah protokol yang lebih ringan yang menyediakan komunikasi yang lebih cepat tetapi tidak dijamin handal.
3. Layer Aplikasi (Application Layer): Ini adalah layer tertinggi dalam Model TCP/IP dan berisi berbagai protokol aplikasi yang digunakan untuk tujuan berkomunikasi spesifik. Beberapa contoh protokol aplikasi termasuk HTTP (Hypertext Transfer Protocol) untuk browsing web, SMTP (Simple Mail Transfer Protocol) untuk email, dan FTP (File Transfer Protocol) untuk transfer file.
4. Layer Interface Jaringan (Network Interface Layer): Beberapa interpretasi Model TCP/IP mencakup layer ini, yang bertanggung jawab atas komunikasi fisik langsung dengan media transmisi jaringan, seperti kabel Ethernet atau

sinyal nirkabel. Layer ini mencakup driver perangkat keras dan perangkat lunak yang diperlukan untuk mengirim dan menerima data melalui media fisik.

Penting untuk diingat bahwa Model TCP/IP adalah model konseptual yang digunakan untuk memahami bagaimana komunikasi dalam jaringan berlangsung. Ini bukan model yang sama dengan Model OSI (Open Systems Interconnection) yang memiliki tujuh layer. Namun, Model OSI dan Model TCP/IP sering digunakan bersama-sama untuk memberikan pemahaman yang lebih komprehensif tentang komunikasi jaringan. Dalam praktiknya, Model TCP/IP adalah dasar bagi Internet dan sebagian besar jaringan komputer modern.

7.4. Keamanan dalam TCP/IP

Keamanan dalam protokol TCP/IP (Transmission Control Protocol/Internet Protocol) adalah aspek penting dalam menjaga integritas, kerahasiaan, dan ketersediaan data dalam jaringan. Beberapa aspek keamanan dalam TCP/IP melibatkan pengamanan data, identifikasi, otentikasi, otorisasi, dan monitoring jaringan. Berikut adalah beberapa komponen penting keamanan dalam TCP/IP:

1. Firewall: Firewall adalah perangkat keras atau perangkat lunak yang digunakan untuk melindungi jaringan dari ancaman eksternal. Ini bekerja dengan mengontrol lalu lintas data yang masuk dan keluar dari jaringan. Firewall dapat mengizinkan atau memblokir lalu lintas berdasarkan aturan dan kebijakan keamanan yang telah ditetapkan.
2. Enkripsi Data: Enkripsi adalah proses mengubah data menjadi format yang tidak dapat dibaca kecuali oleh penerima yang memiliki kunci enkripsi yang sesuai. Protokol seperti HTTPS (yang menggunakan SSL/TLS) dan VPN (Virtual Private Network) menggunakan enkripsi untuk melindungi data saat transit melalui jaringan.
3. IPSec (Internet Protocol Security): IPSec adalah set protokol keamanan yang digunakan untuk mengamankan komunikasi dalam jaringan. Ini menyediakan enkripsi, otentikasi, dan integritas data pada tingkat protokol IP, sehingga melindungi lalu lintas data dari potensi ancaman.
4. Antivirus dan Antimalware: Perangkat lunak antivirus dan antimalware digunakan untuk mendeteksi dan menghapus ancaman perangkat lunak jahat, seperti virus, worm, trojan, dan

spyware yang dapat menginfeksi komputer dan jaringan.

5. **Penyaringan Paket:** Teknik penyaringan paket digunakan untuk menginspeksi lalu lintas jaringan dan mengambil tindakan berdasarkan aturan yang telah ditentukan. Ini dapat digunakan untuk mencegah lalu lintas berbahaya atau membatasi akses ke layanan tertentu.
6. **Otentikasi Pengguna:** Untuk mengidentifikasi pengguna yang sah, berbagai metode otentikasi digunakan, termasuk username dan password, kartu pintar, atau metode otentikasi multi-faktor (MFA). Hal ini penting untuk memastikan bahwa hanya pengguna yang sah yang memiliki akses ke jaringan dan sumber daya yang terlindungi.
7. **Otorisasi dan Manajemen Akses:** Setelah otentikasi, otorisasi menentukan apa yang diizinkan untuk dilakukan oleh pengguna atau perangkat. Ini mencakup pengaturan hak akses, peran, dan izin untuk mengakses sumber daya jaringan.
8. **Monitoring Jaringan:** Pemantauan jaringan aktif membantu dalam mendeteksi aktivitas mencurigakan atau ancaman keamanan. Log jaringan, IDS (Intrusion Detection System), dan

IPS (Intrusion Prevention System) digunakan untuk memantau lalu lintas dan mendeteksi pelanggaran keamanan.

9. Pemutusan Jaringan (Disconnect): Ketika ada ancaman atau serangan yang parah, tindakan pemutusan jaringan (disconnect) dapat diambil untuk mengisolasi jaringan dari Internet atau bagian tertentu dari jaringan dari jaringan lainnya untuk mencegah penyebaran ancaman.
10. Pembaruan dan Patch: Memastikan bahwa perangkat keras dan perangkat lunak dijaga tetap terbaru dengan pembaruan keamanan adalah langkah penting dalam menjaga keamanan jaringan. Perusahaan dan pengguna individu perlu secara teratur menginstal patch keamanan.
11. Pelatihan Keamanan: Pengguna jaringan juga perlu mendapatkan pelatihan tentang praktik keamanan yang baik, seperti menghindari membuka lampiran email yang mencurigakan, menghindari mengklik tautan yang mencurigakan, dan menggunakan kata sandi yang kuat.

Keamanan dalam TCP/IP adalah aspek kritis yang harus dikelola dengan serius dalam lingkungan jaringan apa pun, terutama ketika mengakses Internet. Kombinasi berbagai teknik keamanan adalah pendekatan terbaik untuk melindungi jaringan dan data dari ancaman yang beragam.

7.5. Masa Depan Protokol TCP/IP

Protokol TCP/IP (Transmission Control Protocol/Internet Protocol) adalah dasar Internet modern dan infrastruktur jaringan. Meskipun telah ada selama beberapa dekade, TCP/IP terus berkembang dan akan terus menjadi bagian integral dari masa depan teknologi komunikasi dan jaringan. Berikut adalah beberapa perkiraan tentang masa depan protokol TCP/IP:

1. Penggunaan IPv6: Protokol IP versi 4 (IPv4) telah digunakan secara luas dan menghadapi masalah kehabisan alamat IP unik karena pertumbuhan Internet yang pesat. Sebagai alternatif, IPv6 telah diperkenalkan dengan alamat IP yang lebih besar (128-bit dibandingkan dengan 32-bit pada IPv4). Masa depan jaringan akan melibatkan penggunaan IPv6 yang lebih luas untuk mengatasi

kekurangan alamat IP dan mendukung pertumbuhan IoT dan perangkat terhubung lainnya.

2. Kecerdasan Buatan dan Automasi: Dalam era yang semakin terhubung dan kompleks, kecerdasan buatan (AI) dan otomatisasi akan berperan penting dalam mengelola jaringan dan keamanan. Protokol TCP/IP akan bekerja sama dengan alat-alat otomatisasi untuk mendeteksi dan merespons ancaman keamanan secara real-time dan mengoptimalkan kinerja jaringan.
3. 5G dan Edge Computing: Kehadiran jaringan 5G yang lebih cepat dan berlatensi rendah akan membawa perubahan signifikan dalam cara data dikirim dan diproses. Protokol TCP/IP akan digunakan dalam mengelola komunikasi dan transfer data yang efisien dalam lingkungan 5G. Selain itu, komputasi tepi (edge computing) akan semakin diterapkan, dan TCP/IP akan digunakan untuk menghubungkan perangkat di tepi jaringan dengan infrastruktur pusat.
4. Internet of Things (IoT): Pertumbuhan IoT akan terus mendorong evolusi protokol TCP/IP. Protokol ini akan digunakan untuk menghubungkan dan mengelola miliaran

perangkat IoT yang berkomunikasi dalam jaringan, mengarah pada pembaruan dan pengembangan protokol yang lebih efisien dan aman.

5. Keselamatan dan Keamanan Tingkat Tinggi: Dengan semakin rumitnya ancaman siber, perlindungan keamanan jaringan akan menjadi lebih penting daripada sebelumnya. Protokol TCP/IP akan terus diubah dan ditingkatkan untuk memastikan tingkat keamanan yang lebih tinggi, termasuk dalam aspek otentikasi, enkripsi, dan deteksi ancaman.
6. Protokol Aplikasi Baru: Masa depan juga dapat melibatkan pengembangan protokol aplikasi baru yang berfungsi di atas TCP/IP untuk mendukung aplikasi dan layanan yang belum ada saat ini. Misalnya, protokol untuk mendukung komunikasi Augmented Reality (AR) atau Virtual Reality (VR) yang lebih interaktif.
7. Privasi Data: Dalam konteks regulasi privasi data yang semakin ketat seperti GDPR di Uni Eropa, keamanan data dan privasi akan menjadi perhatian utama. Protokol TCP/IP akan berperan dalam mengamankan data yang

ditransmisikan dan diterima dalam lingkungan yang menghormati privasi pengguna.

Protokol TCP/IP akan terus berkembang dan disesuaikan dengan tuntutan masa depan teknologi komunikasi dan jaringan. Dengan perkembangan ini, TCP/IP akan tetap menjadi landasan penting dalam mendukung komunikasi dan konektivitas dalam lingkungan yang semakin terhubung dan maju.

BAB VIII

KEAMANAN JARINGAN KOMPUTER

8.1. Definisi Keamanan Jaringan

Keamanan jaringan merujuk pada praktik, prosedur, dan teknik yang digunakan untuk melindungi jaringan dan data yang melewatinya dari ancaman, serangan, atau akses yang tidak sah. Tujuannya adalah untuk menjamin integritas, kerahasiaan, dan ketersediaan data dan sumber daya jaringan.

8.1.1. Pentingnya Keamanan Jaringan

Pentingnya keamanan jaringan tidak dapat diremehkan karena beberapa alasan:

Perlindungan Data: Jaringan komputer menyimpan dan mengelola data yang seringkali bersifat sensitif atau penting, baik untuk individu, perusahaan, atau pemerintah. Keamanan jaringan menjamin bahwa data ini terlindungi dari pencurian atau kerusakan.

Mempertahankan Reputasi: Serangan jaringan atau kegagalan keamanan dapat merusak reputasi suatu organisasi, yang mungkin membutuhkan waktu bertahun-tahun untuk dibangun kembali.

Aspek Hukum dan Kepatuhan: Banyak industri dan sektor memiliki persyaratan kepatuhan yang mewajibkan perlindungan data. Keamanan jaringan memastikan bahwa organisasi memenuhi persyaratan ini.

Kontinuitas Bisnis: Serangan jaringan bisa menghentikan operasi suatu organisasi. Dengan keamanan jaringan yang tepat, risiko downtime dapat diminimalkan.

8.1.2. Ancaman dan Serangan Jaringan

Ketika kita berbicara tentang keamanan jaringan, salah satu aspek paling penting adalah memahami ancaman dan serangan yang bisa mempengaruhi jaringan. Ancaman ini bisa berasal dari berbagai sumber dan memiliki beragam bentuk. Memahami ancaman ini membantu dalam mengembangkan strategi pertahanan yang efektif.

8.2. Jenis-Jenis Ancaman

Physical Threats: Kerusakan atau gangguan terhadap infrastruktur fisik, seperti pemadaman listrik, kebakaran, atau kerusakan perangkat akibat bencana alam.

Technical Threats: Ancaman yang berkaitan dengan kegagalan perangkat keras atau perangkat lunak, termasuk bug dan kesalahan sistem.

Administrative Threats: Kesalahan oleh personel yang mengelola jaringan, seperti kesalahan konfigurasi atau kegagalan dalam pembaruan keamanan.

Malicious Threats: Upaya yang disengaja oleh individu atau organisasi untuk merusak, mencuri, atau mengakses data tanpa izin.

1. Serangan Pasif dan Aktif

Serangan Pasif: Pada serangan jenis ini, penyerang hanya "mendengar" atau memonitor komunikasi tanpa mengubah data yang ditransmisikan. Contohnya adalah sniffing atau eavesdropping.

Serangan Aktif: Dalam serangan ini, penyerang aktif mengambil tindakan, seperti mengubah data, menghentikan layanan, atau menyebarkan malware.

2. Serangan Terspesifik: Man-in-the-Middle, DDoS, Phishing, dll.

Man-in-the-Middle (MitM): Penyerang berintersepsi di antara dua pihak yang berkomunikasi, dengan potensi untuk

mendengar, mengubah, atau memalsukan komunikasi.

Distributed Denial of Service (DDoS): Serangan ini bertujuan untuk membuat layanan tidak tersedia dengan membanjiri sistem target dengan lalu lintas yang berlebihan.

Phishing: Upaya untuk mendapatkan informasi sensitif seperti kata sandi atau detail kartu kredit dengan menyamar sebagai entitas tepercaya, biasanya melalui email atau situs web palsu.

3. Malware dan Ransomware

Malware: Perangkat lunak jahat yang dirancang untuk menginfeksi, merusak, atau mendapatkan akses tanpa izin ke sistem komputer. Contoh termasuk virus, worm, dan trojan.

Ransomware: Jenis malware yang mengenkripsi data korban dan meminta tebusan (biasanya dalam bentuk mata uang kripto) untuk mendekripsi kembali data tersebut.

4. Insider Threats

Definisi: Ancaman dari individu yang memiliki akses ke organisasi, seperti karyawan, mantan karyawan, kontraktor, atau mitra bisnis.

Motivasi: Insider threats dapat didorong oleh berbagai motivasi, termasuk dendam,

keuntungan finansial, atau manipulasi oleh pihak ketiga.

Contoh: Pengungkapan informasi rahasia, sabotase, atau pencurian data.

8.3. Prinsip Dasar Keamanan Jaringan

Dalam dunia keamanan siber, ada beberapa prinsip dasar yang membentuk fondasi dari semua upaya keamanan. Prinsip-prinsip ini, sering kali disebut sebagai "Pillars of Information Security" atau "Pillars of Cybersecurity," membantu profesional keamanan dalam mendefinisikan, merancang, dan mengimplementasikan solusi keamanan yang efektif.

1. Keotentikkan

Definisi: Keotentikkan merujuk pada proses verifikasi identitas entitas (bisa berupa user, sistem, atau aplikasi) untuk memastikan bahwa mereka adalah siapa yang mereka klaim sebagai diri mereka.

Penerapan: Teknologi seperti password, sertifikat digital, dan otentikasi multi-faktor digunakan untuk memastikan keotentikkan.

Pentingnya: Dengan memastikan keotentikkan, sistem dapat mencegah akses oleh pihak yang tidak berwenang atau pihak ketiga yang

mungkin mencoba menyamar sebagai entitas yang sah.

2. Integritas

Definisi: Integritas mengacu pada keutuhan data, yaitu memastikan bahwa data tidak diubah tanpa otorisasi selama penyimpanan, transmisi, atau pemrosesan.

Penerapan: Teknologi seperti checksums, digital signatures, dan hash functions digunakan untuk memastikan integritas data.

Pentingnya: Mempertahankan integritas data memastikan bahwa informasi yang diterima adalah sama dengan informasi yang dikirim atau disimpan, tanpa modifikasi yang tidak sah.

3. Kerahasiaan

Definisi: Kerahasiaan berkaitan dengan perlindungan data dan informasi dari akses oleh pihak yang tidak berwenang.

Penerapan: Enkripsi, kontrol akses, dan teknologi lainnya digunakan untuk memastikan kerahasiaan data.

Pentingnya: Kerahasiaan memastikan bahwa informasi sensitif, seperti data pribadi atau informasi bisnis, tetap terlindungi dari mata yang tidak diinginkan.

4. Ketersediaan

Definisi: Ketersediaan menjamin bahwa sumber daya informasi tersedia bagi pengguna yang berwenang kapan pun mereka membutuhkannya.

Penerapan: Teknologi dan praktik seperti redundancy, failover, backup, dan pemulihan bencana digunakan untuk memastikan ketersediaan.

Pentingnya: Dalam banyak kasus, terutama untuk layanan bisnis dan kritis, ketersediaan informasi atau layanan adalah esensial. Gangguan, bahkan yang singkat, bisa memiliki konsekuensi finansial dan operasional yang signifikan.

5. Non-Repudiation

Definisi: Non-Repudiation memastikan bahwa pihak yang berkomunikasi tidak dapat menyangkal keterlibatan mereka dalam komunikasi atau transaksi tertentu.

Penerapan: Digital signatures dan sertifikat digital sering digunakan untuk memastikan non-repudiation.

Pentingnya: Dalam banyak transaksi, khususnya yang berkaitan dengan hukum atau finansial,

penting untuk memiliki bukti tindakan atau komunikasi yang tidak dapat disangkal.

Memahami dan menerapkan prinsip-prinsip ini dalam strategi keamanan jaringan sangat krusial. Mereka bekerja bersama-sama untuk membangun dan mempertahankan lingkungan yang aman dan tepercaya bagi pengguna, data, dan sumber daya lainnya.

8.4. Teknologi Keamanan Jaringan

Dengan beragam ancaman yang mengintai di dunia siber, berbagai teknologi telah dikembangkan untuk melindungi jaringan dan data yang melewatinya. Teknologi-teknologi ini berfungsi sebagai perisai, detektor, atau penghalang yang memastikan keamanan data dan sumber daya.

1. Firewalls dan IDS/IPS

Firewalls: Perangkat atau perangkat lunak yang mengontrol lalu lintas jaringan yang masuk dan keluar berdasarkan set aturan tertentu. Firewalls bisa berbasis host atau berbasis jaringan.

IDS (Intrusion Detection System): Sistem yang memantau lalu lintas jaringan atau aktivitas

sistem untuk mencari tanda-tanda aktivitas yang mencurigakan atau tidak sah.

IPS (Intrusion Prevention System): Mirip dengan IDS, tetapi selain mendeteksi, IPS juga bertindak untuk menghentikan atau mencegah aktivitas mencurigakan.

2. VPN dan Tunneling

VPN (Virtual Private Network): Teknologi yang memungkinkan pengguna untuk membuat koneksi aman dan terenkripsi ke jaringan lain melalui internet. VPN sering digunakan untuk akses jarak jauh ke sumber daya perusahaan.

Tunneling: Proses di mana data dikapsulkan dalam protokol lain, memungkinkannya untuk melewati jaringan yang tidak mendukung tipe data asli tersebut.

3. Enkripsi dan Protokol Keamanan

Enkripsi: Proses konversi data menjadi kode untuk mencegah akses tanpa izin. Ada dua jenis utama: enkripsi simetris (kunci yang sama untuk enkripsi dan dekripsi) dan enkripsi asimetris (dua kunci terkait, satu publik dan satu pribadi).

Protokol Keamanan: Seperti TLS (Transport Layer Security) dan SSL (Secure Sockets Layer)

yang digunakan untuk mengamankan transmisi data antara klien dan server.

4. Sandboxing

Definisi: Teknologi yang memungkinkan program atau aplikasi berjalan dalam lingkungan yang terisolasi sehingga tidak dapat mempengaruhi sistem lain. Ini sering digunakan untuk menganalisis perilaku malware tanpa mempengaruhi sistem host.

5. Sistem Deteksi Intrusi

Meskipun sebelumnya disebutkan dalam konteks IDS/IPS, sistem deteksi intrusi patut mendapatkan penjelasan lebih rinci:

Network-based IDS (NIDS): Memantau lalu lintas jaringan keseluruhan untuk mendeteksi aktivitas yang mencurigakan.

Host-based IDS (HIDS): Diinstal pada host tertentu dan memantau aktivitas pada host tersebut untuk mendeteksi perubahan atau ancaman.

Signature-based Detection: Mendeteksi ancaman berdasarkan signature atau pola yang diketahui dari serangan sebelumnya.

Anomaly-based Detection: Menggunakan model dari aktivitas jaringan atau sistem yang dianggap

normal dan kemudian memberi peringatan saat aktivitas yang menyimpang dari norma tersebut terdeteksi.

Memahami dan mengintegrasikan teknologi keamanan jaringan yang tepat adalah krusial bagi setiap organisasi. Setiap teknologi memiliki kelebihan dan kekurangan serta aplikasi yang paling sesuai tergantung pada kebutuhan dan arsitektur jaringan tertentu.

8.5. Manajemen Keamanan

Sementara teknologi keamanan adalah fondasi dari sebuah jaringan yang aman, manajemen yang efektif dari keamanan tersebut merupakan kunci untuk memastikan bahwa semua elemen bekerja bersama dengan cara yang optimal. Manajemen keamanan mencakup kebijakan, prosedur, dan tindakan pencegahan lainnya untuk memastikan bahwa jaringan dan data tetap aman.

1. Kebijakan Keamanan

Definisi: Dokumen formal yang menetapkan panduan dan aturan untuk mengakses dan menggunakan sumber daya TI perusahaan.

Pentingnya: Kebijakan keamanan memastikan bahwa semua anggota organisasi memahami

harapan dan tanggung jawab mereka dalam menjaga keamanan informasi.

Komponen Utama: Tujuan kebijakan, ruang lingkup, tanggung jawab, regulasi, dan prosedur penegakan.

2. Penilaian Risiko

Definisi: Proses identifikasi, evaluasi, dan prioritasasi risiko berdasarkan potensi dampak dan kemungkinan terjadinya.

Pentingnya: Dengan memahami risiko, organisasi dapat mengalokasikan sumber daya dengan cara yang paling efektif untuk memitigasi ancaman terbesar.

Langkah-langkah: Identifikasi aset, identifikasi ancaman dan kerentanan, tentukan dampak dan kemungkinan, dan prioritaskan risiko.

3. Audit dan Monitoring Keamanan

Audit Keamanan: Proses formal untuk mengevaluasi efektivitas kontrol keamanan yang ada berdasarkan kebijakan dan standar yang telah ditetapkan.

Monitoring Keamanan: Pengawasan berkelanjutan atas operasi jaringan dan sistem untuk mendeteksi aktivitas yang mencurigakan atau melanggar kebijakan.

Pentingnya: Audit dan monitoring memungkinkan organisasi untuk mengidentifikasi kelemahan dan potensi pelanggaran sebelum mereka menjadi masalah serius.

4. Backup dan Pemulihan

Backup: Proses membuat salinan data untuk tujuan pemulihan dalam kasus kehilangan data.

Pemulihan: Mengembalikan data dari salinan cadangan setelah kehilangan data.

Pentingnya: Kehilangan data, baik karena kesalahan manusia, kerusakan perangkat keras, atau serangan siber, dapat memiliki konsekuensi serius bagi organisasi. Memiliki solusi backup dan pemulihan yang efektif memastikan kelangsungan bisnis.

Manajemen keamanan memastikan bahwa langkah-langkah keamanan yang tepat diterapkan dan dikelola dengan benar. Ini melibatkan koordinasi antara orang, proses, dan teknologi untuk membangun lingkungan yang aman dan tangguh terhadap ancaman.

8.6. Teknik Pertahanan dan Proteksi

Saat kita berbicara tentang keamanan jaringan, penting untuk memiliki lapisan pertahanan yang beragam untuk melindungi dari ancaman yang mungkin timbul. Dengan memadukan beberapa teknik pertahanan, organisasi dapat meminimalkan kerentanan mereka dan meningkatkan postur keamanan mereka.

1. Hardening Sistem

Definisi: Proses pengoptimalan sistem untuk mengurangi permukaan serangan dengan menghapus atau menonaktifkan fungsi, aplikasi, dan layanan yang tidak diperlukan.

Pentingnya: Hardening membantu dalam mengurangi risiko dengan meminimalkan jumlah potensi titik masuk bagi penyerang.

Contoh: Menonaktifkan port yang tidak digunakan, menghapus atau menonaktifkan layanan atau perangkat lunak yang tidak diperlukan, memperbarui dan mengonfigurasi perangkat keras dan perangkat lunak.

2. Multi-factor Authentication (MFA)

Definisi: Metode otentikasi yang memerlukan lebih dari satu bentuk verifikasi untuk mengkonfirmasi identitas pengguna.

Pentingnya: MFA mempersulit bagi penyerang untuk mendapatkan akses hanya dengan mencuri atau menebak satu bentuk kredensial.

Contoh: Sesuatu yang Anda ketahui (password), sesuatu yang Anda miliki (token atau kode SMS), dan sesuatu yang Anda (biometrik seperti sidik jari atau pengenalan wajah).

3. Patch Management

Definisi: Proses mengidentifikasi, mengakuisisi, menginstal, dan memverifikasi patch untuk produk perangkat lunak dan sistem.

Pentingnya: Banyak serangan memanfaatkan kerentanan yang diketahui dalam perangkat lunak yang belum diperbaiki. Patch management memastikan bahwa sistem diperbarui dengan perbaikan terbaru.

4. Isolasi Jaringan dan Segregasi

Definisi: Praktek memisahkan bagian-bagian jaringan untuk membatasi akses antara mereka.

Pentingnya: Dengan mengisolasi segmen jaringan, organisasi dapat membatasi dampak serangan dan mencegah pergerakannya melintasi jaringan.

Contoh: VLANs, jaringan DMZ, dan firewall untuk memisahkan lalu lintas produksi dari lalu lintas administratif.

5. Honeypots

Definisi: Sistem atau sumber daya jaringan yang sengaja dibuat rentan dan ditempatkan untuk menarik dan mendeteksi penyerang.

Pentingnya: Honeypots memungkinkan organisasi untuk mempelajari taktik, teknik, dan prosedur penyerang serta memberikan waktu tambahan untuk mendeteksi dan merespons serangan yang sedang berlangsung.

Menggabungkan berbagai teknik pertahanan ini memungkinkan pendekatan yang disebut "pertahanan dalam kedalaman," di mana beberapa lapisan proteksi bekerja bersama-sama untuk mencegah, mendeteksi, dan merespons ancaman keamanan.

8.7. Aspek Hukum dan Kepatuhan

Di era digital saat ini, kepatuhan terhadap standar dan regulasi keamanan informasi adalah hal yang krusial bagi banyak organisasi. Selain itu, peraturan ini juga dirancang untuk melindungi konsumen dan bisnis dari

ancaman siber dan meningkatkan transparansi antara perusahaan dan konsumen.

8.7.1. Peraturan dan Undang-undang Terkait Keamanan Jaringan

Definisi: Kumpulan ketentuan hukum dan regulasi yang mengatur bagaimana data harus dilindungi dan bagaimana insiden keamanan harus ditangani.

Pentingnya: Peraturan ini memastikan bahwa organisasi menjalankan tindakan keamanan yang sesuai dan melindungi data konsumen dan bisnis dari pelanggaran.

Contoh: GDPR (General Data Protection Regulation) di Eropa, CCPA (California Consumer Privacy Act) di Amerika Serikat, dan lain-lain tergantung pada yurisdiksi.

8.7.2. Pelaporan Insiden Keamanan

Definisi: Proses resmi menginformasikan pihak yang berwenang atau berkepentingan tentang kejadian keamanan atau pelanggaran data.

Pentingnya: Pelaporan memungkinkan pemangku kepentingan untuk mengambil tindakan yang diperlukan, termasuk pemberitahuan kepada

korban, serta memenuhi kewajiban hukum dan regulasi.

Adalah penting bagi organisasi untuk memahami dan mematuhi aspek hukum dan regulasi yang berlaku bagi mereka. Kegagalan untuk melakukannya dapat mengakibatkan sanksi hukum, kerugian finansial, dan kerusakan reputasi.

8.8. Tantangan dan Trend Masa Depan

Seiring dengan perkembangan teknologi, dunia keamanan jaringan juga terus menghadapi tantangan baru dan evolusi dalam cara melindungi infrastruktur dan data. Mari kita jelajahi beberapa trend dan tantangan utama yang dihadapi oleh profesional keamanan jaringan di masa depan.

8.8.1. Keamanan di Era IoT (Internet of Things)

Definisi: IoT merujuk pada jaringan perangkat fisik yang saling terhubung dan berbagi data, mulai dari peralatan rumah tangga pintar hingga perangkat industri.

Tantangan: Dengan miliaran perangkat IoT yang diharapkan terhubung dalam beberapa tahun mendatang, keamanan menjadi isu utama. Banyak perangkat ini memiliki keamanan yang lemah atau

tidak ter-update, menjadikannya sasaran empuk untuk serangan.

Pengaruh: Serangan terhadap perangkat IoT dapat mengganggu operasi sehari-hari, merusak properti, atau bahkan membahayakan nyawa jika perangkat tersebut berhubungan dengan infrastruktur kritis.

8.8.2. Ancaman Baru dan Perkembangan Teknik Serangan

Evolusi Malware: Varian baru dari malware, ransomware, dan teknik serangan lainnya terus muncul, memerlukan deteksi dan respons yang lebih cepat.

Serangan Supply Chain: Penyerang mungkin mencoba mengkompromikan perangkat lunak atau perangkat keras pada tahap produksi atau distribusi.

Serangan terhadap Infrastruktur Kritis: Sebagai contoh, serangan terhadap fasilitas energi atau pasokan air dapat memiliki konsekuensi yang luas dan merusak.

8.8.3. Kecerdasan Buatan dalam Keamanan

Jaringan

Definisi: Penggunaan algoritma dan model machine learning untuk mendeteksi, mencegah, dan merespons ancaman dalam waktu nyata.

Potensi: AI dapat membantu dalam analisis lalu lintas jaringan yang mencurigakan, mendeteksi pola yang tidak biasa, dan secara otomatis menangani serangan.

Tantangan: Sementara AI memiliki potensi besar, penyerang juga bisa menggunakan AI untuk mengidentifikasi kerentanan atau untuk melakukan serangan yang lebih canggih.

Etika dan Kepercayaan: Penggunaan AI dalam keamanan memerlukan pemikiran etis, khususnya jika digunakan untuk membuat keputusan otomatis yang mungkin mempengaruhi individu atau organisasi.

Ketiga area ini hanya sebagian kecil dari tantangan dan trend yang mungkin dihadapi oleh profesional keamanan jaringan. Penting bagi mereka untuk terus belajar dan beradaptasi dengan perubahan teknologi dan ancaman untuk tetap mempertahankan integritas dan keamanan jaringan yang mereka kelola.

8.9. Kesimpulan

Pentingnya Keamanan Jaringan: Seiring dengan peningkatan ketergantungan masyarakat dan bisnis pada teknologi, perlindungan terhadap infrastruktur dan data menjadi suatu keharusan. Ancaman keamanan, baik dari aktor eksternal maupun internal, terus meningkat dan menjadi semakin canggih.

Teknologi dan Tantangan yang Berkembang: Era IoT, keberlanjutan AI dalam keamanan, dan teknik serangan baru menggambarkan lingkungan yang dinamis dan terus berubah, memerlukan adaptasi dan pembaruan strategi keamanan.

Kepatuhan dan Tanggung Jawab: Selain melindungi dari ancaman siber, perusahaan juga harus mematuhi standar dan regulasi yang berlaku, memastikan bahwa mereka tidak hanya melindungi data pelanggan, tetapi juga menjalankan operasi dengan cara yang etis dan transparan.

BAB IX

APLIKASI JARINGAN KOMPUTER

9.1. Definisi Aplikasi Jaringan Komputer

Aplikasi jaringan komputer adalah perangkat lunak atau program komputer yang dirancang khusus untuk digunakan dalam jaringan komputer. Aplikasi ini memungkinkan pengguna atau perangkat untuk berkomunikasi, berbagi informasi, dan melakukan tugas-tugas tertentu dalam lingkungan jaringan. Aplikasi jaringan komputer dapat beroperasi dalam jaringan lokal (LAN), jaringan luas (WAN), atau bahkan di seluruh Internet. Aplikasi jaringan komputer memainkan peran penting dalam menghubungkan perangkat dan pengguna dalam jaringan, dan mereka berperan dalam berbagai aspek kehidupan sehari-hari, bisnis, dan industri.

9.2. Peran Penting Aplikasi dalam Jaringan

Aplikasi dalam jaringan komputer memiliki peran yang sangat penting karena mereka adalah alat yang memungkinkan pengguna untuk berinteraksi dengan jaringan, mengakses sumber daya, berbagi informasi,

dan menjalankan tugas-tugas tertentu. Berikut adalah beberapa peran penting aplikasi dalam jaringan:

1. **Komunikasi dan Kolaborasi:** Aplikasi jaringan memungkinkan komunikasi dan kolaborasi antara pengguna, baik itu melalui pesan teks, panggilan suara, atau konferensi video. Ini memungkinkan tim dan individu untuk bekerja sama dalam proyek, berbagi informasi, dan membuat keputusan bersama.
2. **Akses ke Sumber Daya:** Aplikasi memungkinkan pengguna untuk mengakses sumber daya jaringan, termasuk berkas-berkas yang disimpan di server, printer bersama, dan perangkat jaringan lainnya. Ini memungkinkan berbagi dan penggunaan sumber daya secara efisien.
3. **Pengelolaan Email dan Pesan:** Aplikasi email memungkinkan pengguna untuk mengirim, menerima, dan mengelola pesan email. Ini adalah alat komunikasi penting dalam bisnis dan komunikasi pribadi.
4. **Akses ke Informasi:** Aplikasi web memungkinkan pengguna untuk mengakses informasi dari internet, mencari data, membaca berita, berbelanja online, dan berinteraksi dengan layanan online. Ini mencakup segala hal

dari pencarian web hingga media sosial dan e-commerce.

5. Keamanan dan Manajemen Jaringan: Aplikasi keamanan jaringan digunakan untuk memantau, mengelola, dan mengamankan jaringan. Ini mencakup firewall, perangkat lunak antivirus, dan alat manajemen jaringan.
6. Layanan Cloud: Aplikasi cloud memungkinkan penyimpanan dan akses ke data dan aplikasi yang disimpan di cloud computing. Ini memungkinkan pengguna untuk mengakses informasi dari mana saja dengan koneksi internet.
7. Kendali IoT (Internet of Things): Aplikasi IoT digunakan untuk mengendalikan dan memantau perangkat IoT yang terhubung dalam jaringan, seperti perangkat pintar rumah atau sistem industri yang terotomatisasi.
8. VoIP (Voice over IP): Aplikasi VoIP memungkinkan panggilan suara dan video melalui jaringan IP, menggantikan telepon tradisional. Ini adalah cara yang ekonomis dan efisien untuk berkomunikasi.
9. Aplikasi Bisnis: Aplikasi bisnis termasuk perangkat lunak yang digunakan untuk

manajemen keuangan, sumber daya manusia, inventaris, analisis data, dan berbagai tugas bisnis lainnya. Mereka memungkinkan efisiensi operasional dan pengambilan keputusan yang lebih baik.

10. Hiburan dan Media: Aplikasi streaming media memungkinkan pengguna untuk menikmati hiburan seperti film, musik, dan konten video melalui internet.
11. Pendidikan dan Pelatihan: Aplikasi pendidikan memungkinkan pembelajaran online, kursus e-learning, dan pelatihan jarak jauh.

Aplikasi dalam jaringan adalah yang membuat jaringan menjadi lebih berguna dan bermanfaat bagi pengguna. Mereka memungkinkan konektivitas yang lebih efektif, penggunaan sumber daya yang lebih baik, dan berbagai kemungkinan interaksi dan produktivitas dalam dunia digital saat ini.

9.3. Sejarah Perkembangan Aplikasi Jaringan

Sejarah perkembangan aplikasi jaringan mencerminkan evolusi teknologi komunikasi dan komputer selama beberapa dekade. Berikut adalah

gambaran umum tentang sejarah perkembangan aplikasi jaringan:

1. 1950-an hingga 1960-an: Pada awal sejarah komputer, jaringan masih dalam tahap eksperimen dan terbatas pada lingkungan militer dan penelitian. Aplikasi jaringan sangat terbatas dan terutama berfokus pada pemrosesan batch dan pertukaran data di antara komputer mainframe.
2. 1970-an: Era ARPANET, cikal bakal Internet modern, dimulai pada tahun 1969. Pada tahun 1970-an, pengembangan protokol awal seperti Telnet untuk remote login dan FTP (File Transfer Protocol) untuk pertukaran file mulai muncul. Ini adalah langkah awal dalam mengembangkan aplikasi jaringan.
3. 1980-an: ARPANET berkembang menjadi Internet dan digunakan oleh komunitas akademik dan penelitian. Pada tahun 1980-an, email menjadi aplikasi jaringan yang sangat penting dengan munculnya standar SMTP (Simple Mail Transfer Protocol) dan POP (Post Office Protocol).
4. 1990-an: Era web dimulai dengan penemuan World Wide Web oleh Tim Berners-Lee pada

tahun 1990. Ini mengarah pada munculnya browser web seperti Mosaic, yang mengubah cara pengguna berinteraksi dengan Internet. Selama dekade ini, aplikasi web seperti pencarian web, forum, dan situs e-commerce mulai muncul.

5. Awal abad ke-21: Munculnya aplikasi media sosial seperti Friendster (2002), MySpace (2003), Facebook (2004), dan Twitter (2006) mengubah cara kita berinteraksi secara sosial dan berbagi informasi secara online.
6. Pertengahan hingga akhir abad ke-21: Era perangkat seluler dimulai dengan munculnya smartphone dan tablet. Ini memicu perkembangan aplikasi seluler (mobile apps) yang berkembang pesat, termasuk aplikasi perpesanan instan, media sosial seluler, dan aplikasi yang memanfaatkan GPS dan sensor perangkat seluler.
7. Pertumbuhan Internet of Things (IoT): Pada abad ke-21, IoT menjadi tren yang signifikan, di mana perangkat yang terhubung ke Internet mendapatkan kehadiran yang lebih besar. Aplikasi jaringan dalam konteks IoT mencakup kendali rumah pintar, kendaraan terhubung, dan

sensor industri yang mengumpulkan dan berbagi data dalam jaringan.

8. **Kontinuitas Aplikasi Web:** Aplikasi web terus berkembang dengan meningkatnya kecepatan internet dan teknologi web. Layanan cloud, seperti Google Workspace dan Microsoft 365, menyediakan alat kolaborasi dan produktivitas melalui web.

Seiring berjalannya waktu, aplikasi jaringan menjadi semakin beragam, kompleks, dan terintegrasi. Mereka membentuk bagian integral dari kehidupan sehari-hari kita, mencakup komunikasi, bisnis, hiburan, dan banyak lagi. Sejarah perkembangan ini mencerminkan bagaimana teknologi jaringan telah memengaruhi cara kita berkomunikasi, bekerja, dan berinteraksi di dunia yang semakin terhubung.

9.4. Aplikasi Web dan Layanan

Aplikasi web dan layanan adalah komponen penting dalam ekosistem internet modern. Mereka memungkinkan pengguna untuk melakukan berbagai tugas, berinteraksi dengan informasi dan konten, serta berkolaborasi secara online. Berikut adalah beberapa contoh aplikasi web dan layanan yang umum digunakan:

1. **Browser Web:** Browser web adalah aplikasi yang digunakan untuk mengakses dan menjelajahi World Wide Web. Contoh browser termasuk Google Chrome, Mozilla Firefox, Microsoft Edge, dan Safari.
2. **Mesin Pencari:** Layanan mesin pencari seperti Google Search, Bing, dan Yahoo Search memungkinkan pengguna untuk mencari informasi di web dengan cepat dan efisien.
3. **Email dan Layanan Surat Elektronik:** Layanan email seperti Gmail, Outlook, dan Yahoo Mail memungkinkan pengguna untuk mengirim, menerima, dan mengelola pesan elektronik.
4. **Media Sosial:** Platform media sosial seperti Facebook, Twitter, Instagram, LinkedIn, dan TikTok memungkinkan pengguna untuk berinteraksi dengan teman-teman, berbagi konten, dan terlibat dalam komunitas online.
5. **Layanan Cloud:** Layanan cloud seperti Google Drive, Dropbox, dan Microsoft OneDrive menyediakan penyimpanan online dan berbagi berkas, serta kolaborasi dokumen secara real-time.
6. **Aplikasi Office Online:** Google Workspace (sebelumnya G Suite) dan Microsoft 365

(sebelumnya Office 365) menyediakan aplikasi produktivitas online seperti Google Docs, Google Sheets, Microsoft Word Online, dan Excel Online yang dapat diakses melalui browser web.

7. Layanan E-commerce: Platform e-commerce seperti Amazon, eBay, dan Alibaba memungkinkan pengguna untuk berbelanja online, melacak pesanan, dan berinteraksi dengan penjual.
8. Layanan Streaming Media: Layanan streaming seperti Netflix, YouTube, Spotify, dan Apple Music memungkinkan pengguna untuk menikmati konten multimedia seperti film, video, musik, dan podcast secara online.
9. Aplikasi Web Kolaboratif: Aplikasi web seperti Slack untuk komunikasi tim, Trello untuk manajemen proyek, dan Asana untuk manajemen tugas membantu tim berkolaborasi secara efisien.
10. Pendidikan Online: Platform pendidikan online seperti Coursera, edX, dan Khan Academy menyediakan kursus online dan sumber belajar bagi siswa dan profesional.
11. Telekonferensi dan Video Konferensi: Layanan seperti Zoom, Microsoft Teams, dan Google Meet

memungkinkan pertemuan dan konferensi video online.

12. Layanan Perjalanan: Situs web seperti Booking.com, Airbnb, dan TripAdvisor membantu pengguna merencanakan perjalanan, mencari akomodasi, dan memesan tiket.
13. Layanan Berita: Situs berita online seperti BBC News, CNN, dan The New York Times menyediakan berita dan informasi terkini.
14. Layanan Kesehatan dan Konsultasi: Aplikasi dan situs web kesehatan seperti WebMD, Healthline, dan aplikasi telemedicine memungkinkan konsultasi medis dan akses informasi kesehatan.
15. Layanan Sosial dan Kencan: Aplikasi seperti Tinder, Bumble, dan OKCupid digunakan untuk bertemu orang baru dan menjalin hubungan sosial atau romantis.

Aplikasi web dan layanan ini mencakup berbagai aspek kehidupan, mulai dari komunikasi dan produktivitas hingga hiburan dan belanja online. Mereka membentuk bagian integral dari pengalaman internet modern dan terus berkembang dengan peningkatan teknologi dan kebutuhan pengguna.

9.5. Aplikasi Kolaboratif

Aplikasi kolaboratif adalah perangkat lunak yang dirancang khusus untuk memfasilitasi kerja sama dan komunikasi antara individu atau tim dalam suatu proyek atau tugas. Ini adalah alat yang penting dalam lingkungan bisnis dan kerja sama tim, memungkinkan anggota tim untuk berbagi informasi, bekerja bersama pada dokumen, mengelola proyek, dan berkomunikasi dengan efisien. Berikut adalah beberapa contoh aplikasi kolaboratif yang umum digunakan:

1. Slack: Slack adalah platform komunikasi yang memungkinkan tim untuk berkomunikasi melalui pesan teks, kanal, dan grup. Ini juga mendukung berbagai integrasi dengan aplikasi lain, seperti Google Drive, Trello, dan GitHub.
2. Microsoft Teams: Microsoft Teams adalah aplikasi yang terintegrasi dengan Microsoft 365 (sebelumnya Office 365) dan memungkinkan tim untuk berkolaborasi dalam chat, panggilan video, dan berbagi dokumen dalam lingkungan yang terstruktur.
3. Trello: Trello adalah aplikasi manajemen proyek yang menggunakan sistem papan dan kartu untuk mengorganisasi tugas dan proyek. Ini

memungkinkan kolaborasi tim dalam mengelola proyek dan tugas.

4. Asana: Asana adalah aplikasi manajemen tugas yang memungkinkan tim untuk membuat, mengatribusi, dan melacak tugas-tugas proyek. Ini juga menyediakan alat kolaborasi untuk tim yang berkolaborasi pada proyek yang sama.
5. Google Workspace (sebelumnya G Suite): Google Workspace menyediakan berbagai alat kolaborasi seperti Google Docs, Google Sheets, Google Slides, dan Google Drive yang memungkinkan pengguna untuk membuat, berbagi, dan bekerja sama pada dokumen secara real-time.
6. Monday.com: Monday.com adalah platform kolaborasi dan manajemen proyek yang memungkinkan pengguna untuk merencanakan, melacak, dan berkolaborasi dalam berbagai jenis proyek.
7. Notion: Notion adalah platform kolaborasi yang menyatukan alat manajemen tugas, wiki, dan pembuatan dokumen. Ini sangat fleksibel dan dapat disesuaikan dengan berbagai kebutuhan tim.

8. Evernote Business: Evernote Business memungkinkan pengguna untuk membuat catatan, dokumen, dan penjadwalan yang dapat diakses dan dibagikan dengan tim. Ini memfasilitasi kerja sama dan manajemen pengetahuan.
9. Jira: Jira adalah aplikasi manajemen proyek yang digunakan oleh pengembang perangkat lunak dan tim IT untuk melacak dan mengelola tugas pengembangan perangkat lunak.
10. Basecamp: Basecamp adalah aplikasi manajemen proyek dan kolaborasi yang menyediakan berbagai alat untuk berkomunikasi, mengorganisasi tugas, dan berbagi dokumen.
11. GitHub: GitHub adalah platform kolaborasi pengembangan perangkat lunak yang digunakan oleh pengembang perangkat lunak untuk berkolaborasi pada proyek pengembangan perangkat lunak.
12. Zoom: Selain menjadi platform untuk konferensi video, Zoom juga memiliki fitur kolaborasi, seperti berbagi layar dan berkolaborasi pada dokumen dalam pertemuan online.

Aplikasi kolaboratif ini memungkinkan tim untuk bekerja bersama secara efisien, mengurangi ketidaknyamanan dalam komunikasi dan manajemen proyek, dan meningkatkan produktivitas. Mereka memiliki berbagai fitur yang membantu pengguna dalam merencanakan, melacak, dan mengeksekusi proyek dan tugas dengan lebih baik.

9.6. Aplikasi Keamanan

Aplikasi keamanan adalah perangkat lunak yang dirancang untuk melindungi sistem, data, dan pengguna dari ancaman keamanan yang beragam. Mereka berperan penting dalam menjaga keamanan dan privasi informasi dalam dunia digital yang semakin kompleks. Berikut adalah beberapa contoh aplikasi keamanan yang umum digunakan:

1. **Antivirus:** Aplikasi antivirus seperti Norton, McAfee, dan Bitdefender digunakan untuk mendeteksi, mencegah, dan menghapus perangkat lunak berbahaya (malware) seperti virus, trojan, dan spyware dari komputer dan perangkat mobile.
2. **Firewall:** Aplikasi firewall seperti Windows Firewall dan ZoneAlarm membantu mengontrol lalu lintas jaringan dan melindungi sistem dari

serangan luar. Mereka dapat mengizinkan atau memblokir akses ke aplikasi dan layanan tertentu.

3. Aplikasi Enkripsi: Aplikasi enkripsi seperti VeraCrypt dan BitLocker memungkinkan pengguna untuk mengenkripsi data di perangkat penyimpanan, sehingga data tidak dapat diakses tanpa kunci enkripsi yang benar.
4. Aplikasi Keamanan Jaringan: Aplikasi keamanan jaringan seperti Wireshark digunakan untuk memantau lalu lintas jaringan dan mendeteksi aktivitas yang mencurigakan atau serangan jaringan.
5. Aplikasi VPN (Virtual Private Network): Aplikasi VPN seperti NordVPN dan ExpressVPN memungkinkan pengguna untuk mengakses internet melalui koneksi yang aman dan anonim, melindungi data dari mata-mata dan mengakses konten yang dibatasi geografis.
6. Password Manager: Aplikasi manajemen kata sandi seperti LastPass, Dashlane, dan 1Password membantu pengguna mengelola dan menyimpan kata sandi dengan aman, serta menghasilkan kata sandi yang kuat.

7. Aplikasi Keamanan Email: Aplikasi keamanan email seperti Proofpoint dan Mimecast membantu mengidentifikasi dan menghentikan email phishing, malware, dan ancaman keamanan email lainnya.
8. Aplikasi Keamanan Mobile: Aplikasi keamanan mobile seperti Lookout dan McAfee Mobile Security melindungi perangkat seluler dari ancaman seperti aplikasi berbahaya, malware, dan pencurian data.
9. Aplikasi Keamanan Web: Aplikasi keamanan web seperti Sucuri dan Cloudflare melindungi situs web dari serangan DDoS, injeksi SQL, dan ancaman web lainnya.
10. Aplikasi Keamanan Perangkat IoT (Internet of Things): Aplikasi keamanan IoT seperti Norton IoT Security dan Bitdefender IoT Security melindungi perangkat terhubung dari potensi eksploitasi keamanan.
11. Aplikasi Keamanan Perusahaan: Aplikasi keamanan perusahaan seperti Cisco Umbrella dan Palo Alto Networks membantu perusahaan melindungi infrastruktur IT mereka dari serangan cyber dan mengelola keamanan secara keseluruhan.

12. Aplikasi Keamanan Identitas: Aplikasi keamanan identitas seperti Okta dan Ping Identity membantu organisasi mengelola akses pengguna dan memastikan identitas digital tetap aman.
13. Aplikasi Keamanan Perangkat Lunak (Software Security): Aplikasi ini membantu pengembang perangkat lunak mengidentifikasi dan mengatasi kerentanannya dalam perangkat lunak mereka sebelum dirilis ke publik.
14. Aplikasi Keamanan Pengujian: Aplikasi ini digunakan oleh para profesional keamanan untuk menguji dan mengevaluasi keamanan sistem dan aplikasi. Contohnya adalah Burp Suite dan Metasploit.

Aplikasi keamanan ini memainkan peran penting dalam melindungi sistem, data, dan identitas pengguna dari ancaman keamanan seperti serangan malware, peretasan, dan pencurian data. Mereka membantu menjaga integritas dan kerahasiaan informasi dalam dunia digital yang penuh risiko.

BAB X

KONSEP DASAR INTERNET

10.1. Pengenalan Internet

Internet adalah salah satu inovasi terbesar dalam sejarah manusia yang telah mengubah cara kita hidup, bekerja, dan berkomunikasi. Sejak kemunculannya, Internet telah menjadi bagian yang tidak terpisahkan dalam kehidupan sehari-hari kita. Internet memiliki akar yang dalam dalam pengembangan jaringan komunikasi. Pada tahun 1960-an, Departemen Pertahanan Amerika Serikat memulai proyek ARPANET, yang merupakan leluhur Internet modern. ARPANET bertujuan untuk memungkinkan pertukaran informasi antara berbagai lembaga penelitian dan militer. Pada tahun 1969, ARPANET melakukan percobaan pertukaran pesan komputer pertama antara dua universitas, Universitas California, Los Angeles (UCLA), dan Stanford Research Institute (SRI).

Selama beberapa dekade berikutnya, ARPANET tumbuh menjadi apa yang kita kenal sebagai Internet saat ini. Pengenalan protokol TCP/IP pada tahun 1980-an memungkinkan perangkat dari berbagai produsen dan sistem operasi berbeda untuk berkomunikasi

dengan mudah melalui Internet. Pada tahun 1990-an, World Wide Web (WWW) yang dikembangkan oleh Tim Berners-Lee mengubah Internet menjadi jaringan yang lebih mudah diakses oleh orang-orang biasa. Internet terus berkembang sejak saat itu, dan sekarang menjadi sarana komunikasi global yang tak terhindarkan.

Internet adalah jaringan global yang terdiri dari jutaan jaringan komputer yang terhubung satu sama lain. Cara kerja dasar Internet melibatkan pengiriman dan penerimaan data melalui kabel serat optik, kabel tembaga, dan sinyal nirkabel. Data dikirim dalam bentuk paket-paket kecil, yang terurai dan disusun kembali oleh perangkat komputer di kedua ujung koneksi. Protokol TCP/IP adalah kerangka kerja yang mendasari Internet. Protokol ini mengatur cara data dikirim, diterima, dan diarahkan melalui jaringan. DNS (Domain Name System) mengubah nama domain menjadi alamat IP yang sesuai, memungkinkan kita mengakses situs web dengan mudah dengan hanya memasukkan alamat webnya.

Internet telah membawa dampak yang signifikan pada masyarakat modern di berbagai bidang, termasuk komunikasi, bisnis, pendidikan, hiburan, dan banyak lagi. Beberapa dampak utama Internet adalah:

1. Komunikasi Global: Internet memungkinkan orang di seluruh dunia untuk berkomunikasi

dengan mudah melalui email, media sosial, dan aplikasi perpesanan.

2. **Bisnis dan E-Commerce:** Internet telah mengubah cara bisnis dilakukan dengan memungkinkan perdagangan elektronik (e-commerce) yang berkembang pesat dan meningkatkan jangkauan pasar global.
3. **Pendidikan:** Internet memberikan akses ke sumber daya pendidikan yang luas, baik dalam bentuk kursus online, tutorial, atau sumber daya belajar lainnya.
4. **Hiburan:** Streaming video, musik, dan konten online lainnya telah mengubah cara kita mengakses hiburan.
5. **Inovasi Teknologi:** Internet telah menjadi landasan bagi inovasi teknologi seperti Internet of Things (IoT), kecerdasan buatan (AI), dan blockchain.

10.2. Protokol Internet

Protokol Internet, atau yang lebih dikenal sebagai IP (Internet Protocol), merupakan fondasi dari segala aktivitas komunikasi di dunia maya saat ini. Protokol Internet adalah seperangkat aturan dan konvensi yang mengatur bagaimana data dan informasi dikirim dan

diterima melalui jaringan komputer global yang kita kenal sebagai internet. Protokol ini memungkinkan jutaan perangkat di seluruh dunia untuk saling berkomunikasi dengan cara yang terstandarisasi.

Protokol Internet bekerja dengan membagi data menjadi paket-paket kecil yang dapat dikirimkan melalui berbagai rute ke tujuan akhir. Ketika sebuah perangkat ingin mengirim data, data tersebut dibagi menjadi paket-paket yang dikemas dengan informasi seperti alamat sumber dan tujuan. Paket-paket ini kemudian dikirimkan ke perangkat tujuan melalui berbagai titik dalam jaringan. Di tujuan, paket-paket ini diambil, diurutkan, dan digabungkan kembali untuk membentuk data awal. Protokol Internet menjadi dasar bagi semua aktivitas online, termasuk browsing web, mengirim email, bermain game online, dan streaming video. Keberadaan protokol ini memungkinkan jutaan perangkat yang berbeda, termasuk komputer, smartphone, tablet, dan perangkat IoT (Internet of Things), untuk saling berkomunikasi di seluruh dunia. Tanpa Protokol Internet yang solid, internet tidak akan menjadi apa yang kita kenal saat ini.

Protokol TCP/IP, singkatan dari Transmission Control Protocol/Internet Protocol, adalah fondasi utama dari seluruh komunikasi di internet. Protokol

TCP/IP adalah seperangkat aturan dan konvensi yang mengatur cara data dikirim, diterima, dan diarahkan di seluruh internet. Dua protokol utama yang membentuk Protokol TCP/IP adalah Transmission Control Protocol (TCP) dan Internet Protocol (IP). TCP bertanggung jawab untuk mengatur komunikasi antara aplikasi di perangkat yang berbeda, sementara IP bertanggung jawab untuk mengirimkan paket-paket data melalui jaringan. Protokol TCP/IP bekerja dengan cara memecah data menjadi paket-paket kecil yang dapat dikirimkan melalui jaringan. Setiap paket dilengkapi dengan alamat sumber dan tujuan. Protokol IP mengarahkan paket-paket ini melalui berbagai perangkat jaringan, termasuk router, menuju tujuan akhir. Ketika paket-paket ini mencapai tujuan akhir, Protokol TCP digunakan untuk memastikan bahwa data tersebut tiba dengan benar, dalam urutan yang benar, dan tanpa kesalahan.

Protokol TCP/IP adalah tulang punggung internet modern. Ini adalah apa yang memungkinkan jutaan perangkat di seluruh dunia untuk berkomunikasi dengan standar yang terstandarisasi. Protokol ini telah menjadi dasar bagi berbagai layanan internet yang kita nikmati sehari-hari, seperti browsing web, email, panggilan video, dan streaming media.

10.3. Lapisan OSI (*Open Systems Interconnection*)

Lapisan OSI adalah kerangka kerja yang digunakan untuk memahami, merancang, dan menjelaskan cara jaringan komputer berkomunikasi satu sama lain. Model ini terdiri dari tujuh lapisan, masing-masing memiliki peran khusus dalam proses komunikasi.

1. Lapisan Fisik (Physical Layer)

Lapisan ini fokus pada aspek fisik komunikasi, seperti kabel, sinyal listrik, dan transmisi data mentah. Ini adalah lapisan yang mengatur bagaimana bit-bit data diubah menjadi sinyal fisik yang dapat dikirim melalui media transmisi.

2. Lapisan Data Link (Data Link Layer)

Lapisan ini mengelola aliran data antara dua perangkat dalam satu segmen jaringan. Ini juga bertanggung jawab untuk mendeteksi dan memperbaiki kesalahan dalam transmisi data.

3. Lapisan Jaringan (Network Layer)

Lapisan ini menangani pengiriman data antar segmen jaringan yang berbeda. Ini melibatkan routing, pengalamatan, dan pembuatan tabel routing.

4. Lapisan Transport (Transport Layer)

Lapisan ini memastikan data yang dikirim tiba dengan benar dan dalam urutan yang tepat. Ini

juga menangani kontrol kesalahan dan aliran data.

5. Lapisan Sesi (Session Layer)

Lapisan ini mengatur dan memelihara sesi komunikasi antara dua perangkat, termasuk pengelolaan dialog dan sinkronisasi.

6. Lapisan Presentasi (Presentation Layer)

Lapisan ini bertanggung jawab untuk menerjemahkan, mengenkripsi, dan mengompresi data agar dapat diinterpretasikan dengan benar oleh aplikasi.

7. Lapisan Aplikasi (Application Layer)

8. Lapisan ini adalah lapisan teratas dalam model OSI dan berhubungan langsung dengan aplikasi yang digunakan oleh pengguna akhir. Ini adalah tempat di mana berbagai aplikasi seperti web browser, email, dan aplikasi lain beroperasi.

Model Lapisan OSI membantu para profesional jaringan memahami bagaimana komponen berbeda dalam jaringan berinteraksi satu sama lain. Ini juga menjadi dasar untuk pengembangan protokol jaringan seperti TCP/IP. Dengan memahami prinsip-prinsip yang mendasari setiap lapisan, insinyur jaringan dapat

merancang, mengimplementasikan, dan mengelola jaringan dengan lebih efektif.

10.4. Arsitektur Internet

Internet telah mengubah cara kita hidup, bekerja, dan berkomunikasi. Di balik kemudahan dan kelancaran yang kita nikmati saat berselancar di dunia maya, ada arsitektur internet yang kompleks yang memungkinkan jutaan perangkat dan orang di seluruh dunia untuk terhubung. Berikut adalah komponen-komponen kunci dalam Arsitektur Internet

1. **Perangkat Akhir (End Devices):** Ini adalah komputer, smartphone, tablet, dan perangkat lainnya yang kita gunakan untuk mengakses internet. Mereka terhubung ke jaringan internet melalui penyedia layanan internet (ISP) lokal.
2. **ISP (Internet Service Provider):** ISP adalah perusahaan yang menyediakan akses ke internet. Mereka memiliki infrastruktur untuk menghubungkan pelanggan mereka ke internet. ISP terbagi menjadi ISP lokal (yang menyediakan akses ke rumah-rumah dan bisnis) dan ISP tingkat atas (yang menghubungkan ISP lokal ke internet global).

3. Server: Server adalah komputer khusus yang menyimpan dan mengelola berbagai jenis data dan layanan yang tersedia di internet. Contoh server termasuk server web, server email, dan server basis data.
4. Router: Router adalah perangkat yang mengarahkan lalu lintas data antara berbagai jaringan. Mereka memutuskan rute terbaik untuk data yang harus dikirim dari satu tempat ke tempat lain di internet.
5. Switch: Switch adalah perangkat yang menghubungkan perangkat dalam jaringan lokal (LAN). Mereka memutuskan ke mana data harus dikirim dalam LAN tersebut.
6. Protokol: Protokol adalah aturan dan standar yang mengatur bagaimana data dikirim, diterima, dan diproses di internet. Beberapa protokol penting termasuk Internet Protocol (IP) untuk pengiriman data, Transmission Control Protocol (TCP) untuk pengiriman data yang andal, dan Hypertext Transfer Protocol (HTTP) untuk mengakses situs web.

Berikut adalah yang merupakan konsep-konsep kunci dalam arsitektur internet :

1. IP Address: Setiap perangkat yang terhubung ke internet memiliki alamat IP yang unik. Alamat IP digunakan untuk mengidentifikasi perangkat di internet. Ada dua versi utama alamat IP, yaitu IPv4 dan IPv6.
2. Domain Name System (DNS): DNS adalah sistem yang mengaitkan alamat IP dengan nama domain yang mudah diingat. Ini memungkinkan kita untuk mengakses situs web dengan menggunakan nama seperti "www.example.com" daripada alamat IP numerik.
3. Pengiriman Data Paket: Data dipecah menjadi paket-paket kecil sebelum dikirimkan melalui internet. Setiap paket memiliki header yang berisi informasi seperti sumber, tujuan, dan urutan paket.
4. Jaringan Publik dan Swasta: Internet terdiri dari jaringan publik, yang dapat diakses oleh siapa saja, dan jaringan swasta, yang terbatas pada pengguna tertentu seperti perusahaan atau pemerintah.

10.4.1. Arsitektur Klien-Server

Arsitektur klien-server adalah model arsitektur perangkat lunak yang digunakan dalam komputasi terdistribusi untuk mengorganisasi sistem komputer dan aplikasi menjadi dua entitas utama: klien dan server. Arsitektur ini memiliki sejumlah karakteristik utama:

1. Klien: Klien adalah entitas yang meminta layanan atau sumber daya dari server. Klien dapat berupa perangkat keras (seperti komputer atau ponsel) atau perangkat lunak (seperti aplikasi desktop atau aplikasi web). Klien bertanggung jawab untuk mengirim permintaan ke server dan menerima respons dari server.
2. Server: Server adalah entitas yang menyediakan layanan atau sumber daya kepada klien. Server biasanya merupakan perangkat keras yang kuat dan terhubung ke jaringan yang dapat diakses oleh klien. Server menjalankan aplikasi atau layanan tertentu yang diinginkan oleh klien, seperti penyimpanan data, basis data, atau layanan web.

3. **Komunikasi:** Klien dan server berkomunikasi melalui jaringan komputer. Klien mengirim permintaan kepada server, dan server merespons dengan memberikan layanan atau sumber daya yang diminta. Komunikasi ini dapat menggunakan berbagai protokol seperti HTTP (untuk aplikasi web), FTP (untuk transfer file), atau protokol khusus lainnya.
4. **Distribusi Tugas:** Dalam arsitektur klien-server, tugas-tugas dibagi antara klien dan server. Klien bertanggung jawab untuk antarmuka pengguna, pemrosesan awal, dan presentasi data, sedangkan server mengelola logika bisnis, pemrosesan data yang lebih intensif, dan penyimpanan data.
5. **Skalabilitas:** Arsitektur ini memungkinkan skalabilitas yang baik. Anda dapat menambahkan lebih banyak klien atau server sesuai kebutuhan untuk meningkatkan kapasitas atau mengatasi lonjakan lalu lintas.
6. **Keamanan:** Pengendalian akses dan keamanan sering dikelola di server. Ini memungkinkan pengelolaan keamanan

yang lebih terpusat dan pengendalian akses ke sumber daya.

7. Manajemen Sumber Daya: Server umumnya bertanggung jawab untuk mengelola sumber daya seperti basis data, file, atau perangkat keras fisik. Hal ini memungkinkan pengelolaan sumber daya yang lebih efisien.
8. Pemeliharaan dan Pembaruan: Pemeliharaan dan pembaruan aplikasi atau layanan biasanya dilakukan di server, sehingga memungkinkan perubahan yang lebih mudah dikelola dan diterapkan.

Contoh penerapan arsitektur klien-server termasuk sistem basis data terdistribusi (klien mengakses dan memanipulasi data dari server database), aplikasi web (klien web berkomunikasi dengan server web untuk mengambil dan menampilkan halaman web), dan permainan online (klien permainan berinteraksi dengan server permainan untuk bermain dengan pemain lain).

Arsitektur klien-server memberikan cara yang efisien untuk mengelola sumber daya dan layanan dalam sistem terdistribusi, dengan memisahkan tugas dan tanggung jawab antara klien

dan server. Hal ini memungkinkan untuk membangun aplikasi yang skalabel, mudah dikelola, dan memiliki keamanan yang lebih baik.

10.4.2. Arsitektur Peer-to-Peer

Arsitektur P2P adalah model jaringan dimana setiap perangkat memiliki peran yang sama dan dapat berinteraksi langsung satu sama lain tanpa memerlukan server pusat. Prinsip dasar arsitektur ini adalah desentralisasi, di mana otoritas dan kontrol terdistribusi di antara semua perangkat dalam jaringan. Hal ini memungkinkan perangkat untuk berbagi sumber daya, seperti file, informasi, atau layanan, dengan cara yang lebih fleksibel dan adaptif.

Beberapa karakteristik utama dari arsitektur P2P adalah:

1. Desentralisasi: Tidak ada satu entitas pusat yang mengontrol seluruh jaringan. Setiap perangkat memiliki otonomi untuk berinteraksi dengan yang lain.
2. Redundansi: Data atau layanan dalam jaringan P2P dapat disimpan atau tersedia di beberapa perangkat, meningkatkan ketahanan terhadap kegagalan.

3. Skalabilitas: Jaringan P2P dapat diperluas dengan mudah dengan menambahkan perangkat baru tanpa mengubah infrastruktur yang ada.
4. Toleransi terhadap Kegagalan: Kegagalan perangkat individual tidak menghentikan operasi jaringan karena sumber daya dan data tersebar.
5. Keamanan: Arsitektur P2P memerlukan tindakan keamanan yang cermat karena akses langsung antara perangkat.

Arsitektur P2P memiliki akar yang panjang dalam sejarah jaringan komputer. Salah satu tonggak penting adalah protokol file sharing Napster yang muncul pada tahun 1999. Namun, perkembangan yang lebih signifikan terjadi dengan munculnya BitTorrent pada tahun 2001, yang mengintegrasikan mekanisme desentralisasi untuk berbagi file dengan efisien. Selanjutnya, teknologi blockchain, yang digunakan oleh Bitcoin pada tahun 2008, membawa arsitektur P2P ke dunia mata uang digital dan kontrak pintar.

Arsitektur P2P telah memberikan dasar bagi berbagai aplikasi, termasuk:

1. Berbagi File: BitTorrent adalah contoh terkenal untuk berbagi file dengan desentralisasi yang tinggi.
2. Komunikasi: Aplikasi seperti Skype dan WhatsApp menggunakan arsitektur P2P untuk panggilan video dan pesan teks.
3. Teknologi Blockchain: Bitcoin dan Ethereum adalah protokol blockchain yang bergantung pada arsitektur P2P untuk mengamankan dan mendistribusikan data transaksi.

Arsitektur P2P telah membawa dampak besar dalam dunia teknologi. Hal ini telah menggoyahkan model bisnis tradisional, mengaktifkan kolaborasi tanpa batas, dan membuka pintu bagi inovasi seperti mata uang kripto dan aplikasi terdesentralisasi.

10.5. Layanan Internet

Layanan internet adalah berbagai fasilitas dan fitur yang memungkinkan pengguna untuk berinteraksi, berbagi informasi, dan mengakses sumber daya online. Di bawah ini, tiga layanan internet utama: World Wide Web (WWW), email, dan komunikasi internet.

1. World Wide Web (WWW):

- World Wide Web, atau sering disingkat sebagai WWW atau web, adalah sistem informasi global yang terdiri dari berbagai dokumen dan sumber daya yang dapat diakses melalui internet. Berikut adalah komponen utama dari layanan WWW:
- Halaman Web: Halaman web adalah dokumen yang ditampilkan di peramban web pengguna. Halaman ini dapat berisi teks, gambar, video, tautan, dan elemen-elemen interaktif lainnya.
- URL (Uniform Resource Locator): URL adalah alamat unik yang digunakan untuk mengidentifikasi lokasi dokumen di web. Contohnya adalah "https://www.example.com".
- Hyperlink: Hyperlink adalah tautan yang menghubungkan halaman web satu dengan yang lain. Pengguna dapat mengklik tautan ini untuk berpindah antarhalaman.
- Peramban Web: Peramban web seperti Google Chrome, Mozilla Firefox, dan Microsoft Edge adalah aplikasi yang digunakan untuk mengakses dan menampilkan halaman web.

- Search Engine: Mesin pencari seperti Google, Bing, dan Yahoo! membantu pengguna menemukan halaman web yang relevan dengan kata kunci pencarian.

2. Email (Electronic Mail):

Email adalah salah satu layanan internet pertama dan tetap menjadi metode komunikasi yang sangat penting di era digital. Berikut adalah komponen utama dari layanan email:

- Alamat Email: Alamat email adalah alamat unik yang digunakan untuk mengirim dan menerima pesan email. Contoh alamat email adalah "namaanda@example.com."
- Inbox: Inbox adalah tempat di mana pesan-pesan yang diterima disimpan. Pengguna dapat membaca, membalas, dan mengarsipkan pesan di dalamnya.
- Pesan Email: Pesan email adalah komunikasi tertulis yang dikirim melalui internet. Pesan dapat berisi teks, gambar, lampiran, dan tautan.
- Lampiran: Lampiran adalah file yang dapat dikirim bersama pesan email, seperti dokumen, gambar, atau video.

- SMTP dan POP/IMAP: Protokol seperti SMTP (Simple Mail Transfer Protocol) digunakan untuk mengirim email, sementara POP (Post Office Protocol) dan IMAP (Internet Message Access Protocol) digunakan untuk mengakses email dari server.

3. Komunikasi Internet:

Komunikasi internet mencakup berbagai cara untuk berkomunikasi secara online, termasuk:

- Pesan Teks: Aplikasi pesan teks seperti WhatsApp, Telegram, dan iMessage memungkinkan pengguna mengirim pesan singkat dan berbagi media.
- Panggilan Suara dan Video: Aplikasi seperti Zoom, Skype, dan FaceTime memungkinkan panggilan suara dan video berkualitas tinggi melalui internet.
- Media Sosial: Platform media sosial seperti Facebook, Twitter, dan Instagram memungkinkan pengguna berinteraksi, berbagi konten, dan terhubung dengan orang lain secara online.
- Konferensi Online: Layanan seperti Zoom dan Microsoft Teams digunakan untuk

mengadakan konferensi online, pertemuan bisnis, dan kuliah daring.

- Forum dan Grup Diskusi: Forum web dan grup diskusi online memungkinkan pengguna berpartisipasi dalam diskusi topik tertentu.
- VoIP (Voice over Internet Protocol): VoIP memungkinkan pengguna untuk membuat panggilan telepon melalui internet, sering kali dengan biaya yang lebih rendah daripada layanan telepon tradisional.

Penting untuk diingat bahwa dalam semua layanan internet ini, keamanan dan privasi adalah faktor penting. Ini melibatkan penggunaan sandi yang kuat, enkripsi, dan waspada terhadap ancaman keamanan seperti phishing dan malware. Dengan kemajuan teknologi dan evolusi internet, layanan ini terus berkembang dan memainkan peran yang semakin besar dalam kehidupan kita. Mereka telah mengubah cara kita berkomunikasi, mengakses informasi, dan berinteraksi dengan dunia digital secara keseluruhan.

10.6. Keamanan dan Privasi

Di era digital yang semakin maju, internet telah menjadi bagian integral dalam kehidupan sehari-hari kita. Kita menggunakannya untuk berkomunikasi, berbelanja, mencari informasi, dan banyak lagi. Meskipun internet membawa banyak manfaat, ini juga membuka pintu bagi risiko keamanan dan privasi yang serius. Oleh karena itu, keamanan dan privasi menjadi dua aspek yang sangat penting dalam pengalaman kita di dunia maya.

Keamanan internet mencakup berbagai langkah dan praktik yang dirancang untuk melindungi sistem, data, dan layanan dari potensi ancaman dan serangan. Beberapa konsep penting dalam keamanan internet meliputi:

1. Firewall: Ini adalah perangkat lunak atau perangkat keras yang berfungsi sebagai "tembok" virtual untuk mencegah akses yang tidak sah ke jaringan atau komputer Anda.
2. Enkripsi: Enkripsi adalah proses mengubah data menjadi format yang hanya dapat dibaca oleh pihak yang memiliki kunci dekripsi. Ini penting untuk melindungi data pribadi dan transaksi online.

3. Pembaruan Perangkat Lunak: Menjaga sistem operasi, perangkat lunak antivirus, dan aplikasi terbaru sangat penting. Pembaruan ini seringkali mengatasi kerentanannya yang dapat dimanfaatkan oleh penjahat cyber.
4. Manajemen Kata Sandi: Menggunakan kata sandi yang kuat dan berbeda untuk setiap akun online, serta mengganti kata sandi secara berkala, membantu melindungi akun Anda dari peretasan.
5. Pengenalan Ancaman: Menggunakan perangkat lunak yang dapat mendeteksi dan merespons ancaman seperti malware, phishing, dan serangan DDoS.

Privasi internet adalah hak individu untuk menjaga kerahasiaan data pribadi mereka saat menggunakan layanan online. Praktik privasi internet yang penting meliputi:

1. Kebijakan Privasi: Memeriksa dan memahami kebijakan privasi situs web dan aplikasi yang Anda gunakan. Pastikan mereka menjaga privasi data Anda.
2. Pemberian Izin: Berikan izin dengan bijak ketika diminta untuk mengakses data pribadi Anda.

Pertimbangkan apakah izin tersebut benar-benar diperlukan untuk fungsi aplikasi atau layanan tertentu.

3. Penggunaan VPN: Menggunakan layanan Virtual Private Network (VPN) dapat membantu menyembunyikan alamat IP Anda dan meningkatkan privasi saat browsing.
4. Pemutusan Identifikasi: Hindari berbagi informasi pribadi yang tidak perlu secara online, seperti nomor identitas, alamat rumah, atau nomor kartu kredit, kecuali jika benar-benar diperlukan.
5. Mengelola Jejak Digital: Hapus jejak digital Anda secara berkala dengan membersihkan riwayat penelusuran dan cookie browser.

Keamanan dan privasi adalah dua pilar yang harus selalu dijaga dalam penggunaan layanan internet. Kita harus terus meningkatkan pemahaman kita tentang cara melindungi diri dari ancaman online dan memahami pentingnya privasi data pribadi kita. Dengan tindakan bijak dan pengetahuan yang tepat, kita dapat menjaga kepercayaan dalam berinteraksi dengan dunia digital yang semakin kompleks.

10.6.1. Ancaman Internet

Ancaman Internet adalah beragam risiko dan potensi kerentanannya yang terkait dengan penggunaan dan ketergantungan kita pada teknologi dan layanan internet. Ancaman ini dapat merusak privasi, keamanan, dan stabilitas individu, bisnis, pemerintah, dan masyarakat secara keseluruhan. Beberapa ancaman utama Internet meliputi:

1. **Malware:** Program-program jahat seperti virus, trojan, dan perangkat lunak berbahaya lainnya dapat merusak atau mencuri data pengguna. Malware juga bisa digunakan untuk mengambil alih komputer atau perangkat mobile.
2. **Phishing:** Teknik ini melibatkan pemalsuan situs web atau pesan email yang tampak asli untuk mencuri informasi pribadi atau keuangan dari pengguna yang tidak curiga.
3. **Serangan DDoS:** Serangan Denial of Service (DDoS) bertujuan menggulungkan situs web atau layanan dengan membanjiri server dengan lalu lintas data palsu, membuatnya tidak dapat diakses oleh pengguna yang sah.

4. Pelanggaran Data: Pencurian data dari perusahaan atau organisasi dapat mengakibatkan penyalahgunaan informasi sensitif seperti kartu kredit atau data identitas.
5. Ransomware: Jenis malware ini mengenkripsi data pengguna dan meminta pembayaran tebusan untuk mengembalikan akses. Ancaman ini telah merugikan banyak perusahaan dan individu.
6. Kejahatan Siber Terorganisir: Kelompok kriminal terorganisir menggunakan internet untuk berbagai kegiatan ilegal, termasuk perdagangan narkoba, pencucian uang, dan serangan keuangan.
7. Desinformasi dan Propaganda: Internet digunakan untuk menyebarkan informasi palsu atau propaganda yang dapat memengaruhi opini publik atau pemilihan umum.
8. Pelanggaran Privasi: Pengumpulan data yang meluas oleh perusahaan teknologi dan praktik pengawasan oleh pemerintah dapat mengancam privasi individu.

9. Serangan terhadap Infrastruktur Kritis: Infrastruktur vital seperti sistem listrik, air, dan transportasi dapat menjadi target serangan siber yang berpotensi berdampak besar.

Ancaman Internet terus berkembang seiring dengan perkembangan teknologi, dan penting untuk terus mengikuti perkembangan ini dan mengambil langkah-langkah yang tepat untuk melindungi diri sendiri dan organisasi dari potensi ancaman.

10.6.2. Privasi di Internet

Di era digital yang semakin maju, privasi di internet menjadi semakin penting dan juga semakin sulit untuk dijaga. Internet telah mengubah cara kita berkomunikasi, berbelanja, berbagi informasi, dan menjalani kehidupan sehari-hari. Namun, dengan manfaat ini juga datang tantangan dalam menjaga privasi pribadi kita. Berikut ini adalah beberapa aspek penting tentang privasi di internet dan cara melindunginya.

1. Data Pribadi di Internet

Ketika kita menggunakan internet, kita sering kali memberikan informasi pribadi

kita kepada berbagai platform dan layanan online. Ini bisa berupa data pribadi seperti nama, alamat, nomor telepon, atau informasi keuangan seperti nomor kartu kredit. Organisasi dan perusahaan sering mengumpulkan data ini untuk berbagai tujuan, termasuk iklan yang disesuaikan, analisis konsumen, dan pengembangan produk.

2. Ancaman terhadap Privasi

Ada beberapa ancaman terhadap privasi di internet, termasuk:

- **Pelanggaran Data:** Data pribadi yang disimpan oleh perusahaan dapat diretas atau dicuri, mengakibatkan risiko pencurian identitas atau penyalahgunaan informasi.
- **Pelacakan Online:** Perusahaan menggunakan teknologi pelacakan untuk mengumpulkan data tentang perilaku online kita. Ini dapat digunakan untuk menyusun profil kita dan menargetkan iklan.
- **Pelanggaran Privasi oleh Pemerintah:** Beberapa pemerintah memonitor

aktivitas online warga mereka, yang dapat mengancam privasi dan kebebasan berbicara.

- Serangan Phishing: Penipuan online dapat mengancam privasi dengan mencoba mendapatkan informasi sensitif dari pengguna yang tidak curiga.

3. Cara Melindungi Privasi di Internet

Meskipun privasi di internet mungkin sulit untuk dijaga sepenuhnya, ada langkah-langkah yang dapat kita ambil untuk melindunginya:

- Pengaturan Privasi: Selalu periksa pengaturan privasi di akun media sosial, peramban web, dan aplikasi. Sesuaikan pengaturan sesuai dengan preferensi Anda.
- Gunakan VPN: Virtual Private Network (VPN) dapat membantu menyembunyikan alamat IP Anda dan mengenkripsi data yang Anda kirimkan melalui internet.
- Hati-hati dengan Data Pribadi: Berikan informasi pribadi hanya kepada situs web dan layanan yang tepercaya. Hindari

membagikan informasi sensitif di platform yang tidak dikenal.

- Perangkat Keamanan: Instal perangkat keamanan yang baik di perangkat Anda, seperti firewall dan program antivirus, dan pastikan mereka selalu diperbarui.
- Edukasi Diri: Pelajari tentang ancaman privasi di internet dan bagaimana melindungi diri dari mereka. Edukasi diri adalah langkah pertama yang kuat dalam menjaga privasi.

Privasi di internet adalah hak yang penting dan layak untuk dilindungi. Karena melibatkan peran penting bagi individu, perusahaan, dan pemerintah untuk bekerja sama dalam menciptakan lingkungan online yang lebih aman dan lebih terpercaya. Dengan langkah-langkah yang tepat, kita dapat menikmati manfaat internet sambil tetap menjaga privasi kita sendiri.

10.7. Masa Depan Internet

Internet telah menjadi salah satu pencapaian paling revolusioner dalam sejarah manusia, mengubah cara kita berkomunikasi, bekerja, dan berinteraksi

dengan dunia sekitar kita. Namun, masa depan Internet menjanjikan lebih banyak terobosan teknologi yang akan membentuk kehidupan kita dalam beberapa tahun mendatang. Berikut adalah beberapa tren dan perkembangan yang mungkin terjadi dalam masa depan Internet.

1. Internet 5G dan 6G: Internet 5G sedang mengalami peningkatan di seluruh dunia, memberikan kecepatan yang jauh lebih tinggi dan latency yang lebih rendah. Selanjutnya, teknologi 6G diharapkan untuk menyajikan kecepatan yang tak terbayangkan dan konektivitas yang lebih baik, membuka peluang baru dalam komunikasi dan IoT (Internet of Things).

Contoh Kasus: Layanan streaming VR dan AR yang mulus, seperti konser virtual yang dapat dihadiri dari seluruh dunia dengan kualitas gambar dan suara yang mendekati pengalaman langsung.

2. Kecerdasan Buatan (AI) dan Internet of Things (IoT): Integrasi AI dan IoT akan semakin mendalam. Perangkat yang lebih pintar dan terhubung akan memberikan kemampuan untuk mengotomatisasi lebih banyak aspek kehidupan

kita, mulai dari rumah pintar hingga mobil otonom.

Contoh Kasus: Pemantauan kesehatan real-time dengan perangkat medis terhubung yang dapat memberikan data vital pasien kepada dokter untuk diagnosis dan perawatan yang lebih baik.

3. Keamanan Cyber: Dengan semakin meningkatnya ketergantungan kita pada Internet, tantangan keamanan cyber akan semakin besar. Solusi keamanan yang lebih kuat dan inovatif akan menjadi fokus utama dalam memastikan bahwa data pribadi dan sistem penting tetap aman.

Contoh Kasus: Sistem keamanan rumah pintar yang mampu mendeteksi ancaman siber, seperti peretasan kamera keamanan, dan mengambil tindakan pencegahan.

4. Metaverse: Konsep metaverse, yang menggabungkan dunia fisik dan virtual, mungkin akan menjadi kenyataan. Ini akan membuka peluang baru dalam hiburan, pendidikan, dan interaksi sosial.

Contoh Kasus: Pengembangan dunia virtual yang memungkinkan interaksi sosial, belanja, pekerjaan, dan hiburan dalam lingkungan virtual

yang realistis, seperti yang dilakukan oleh perusahaan seperti Meta (dulu Facebook).

5. Akses Internet Global: Upaya untuk memberikan akses Internet global kepada semua orang terus berlanjut. Proyek-proyek seperti Starlink dari SpaceX memiliki potensi untuk menghubungkan wilayah yang terpencil dan terisolasi.
Contoh Kasus: Starlink, proyek Internet satelit milik SpaceX, yang menyediakan akses Internet cepat di daerah yang sulit dijangkau, seperti pedalaman Afrika atau daerah terpencil di Alaska.
6. Pertumbuhan e-Commerce: e-Commerce akan terus berkembang dengan peningkatan adopsi pembelian online. Teknologi seperti Augmented Reality (AR) dapat memungkinkan pengalaman belanja yang lebih interaktif.
Contoh Kasus: Penggunaan teknologi Augmented Reality (AR) untuk menguji produk sebelum pembelian dalam aplikasi belanja online.
7. Penggunaan Energi Hijau: Dalam upaya untuk mengurangi dampak lingkungan, Internet masa

depan akan lebih mengandalkan sumber energi terbarukan dan teknologi efisiensi energi.

Contoh Kasus: Data center yang menggunakan sumber energi terbarukan, seperti tenaga surya atau angin, untuk mengurangi dampak lingkungan dari infrastruktur Internet.

Semua contoh-contoh ini menunjukkan bahwa Internet masa depan akan mengubah banyak aspek dalam kehidupan kita, mulai dari cara kita bekerja, bermain, berinteraksi dengan orang lain, hingga memanfaatkan teknologi untuk meningkatkan kualitas hidup dan lingkungan. Dengan adanya inovasi terus menerus, kita dapat memperkirakan bahwa masa depan Internet akan menjadi lebih terkoneksi, cerdas, dan berkelanjutan.

10.8. Internet of Things (IoT)

Internet of Things (IoT) adalah konsep yang semakin mengubah cara kita berinteraksi dengan dunia sekitar. IoT membawa perangkat dan objek sehari-hari ke dalam ekosistem digital, memungkinkan mereka untuk berkomunikasi, mengumpulkan data, dan memberikan solusi yang lebih cerdas.

IoT adalah istilah yang merujuk pada jaringan perangkat fisik yang terhubung ke internet dan saling berkomunikasi. Perangkat-perangkat ini dapat berupa apa saja, mulai dari smartphone dan perangkat rumah tangga hingga kendaraan dan sensor industri. Mereka dapat berinteraksi dan berbagi data secara otomatis melalui internet, menghasilkan keuntungan dalam berbagai bidang.

Aplikasi IoT yang Umum:

- **Rumah Cerdas (Smart Home):**
IoT memungkinkan pengguna untuk mengendalikan perangkat di rumah seperti lampu, thermostat, dan kamera keamanan melalui aplikasi ponsel mereka. Ini tidak hanya meningkatkan kenyamanan, tetapi juga dapat menghemat energi.
- **Kesehatan dan Perawatan Kesehatan:**
Perangkat IoT seperti monitor detak jantung, perangkat pelacakan tidur, dan alat kesehatan pintar memungkinkan individu dan profesional medis untuk mengakses data kesehatan yang penting dalam waktu nyata.
- **Industri dan Manufaktur:**
IoT digunakan dalam pemantauan produksi, pemeliharaan prediktif mesin, dan rantai

pasokan yang lebih efisien. Hal ini membantu perusahaan mengurangi biaya dan meningkatkan produktivitas.

- Kendaraan Terhubung (Connected Vehicles): Mobil yang terhubung memungkinkan pengemudi mendapatkan informasi lalu lintas secara real-time, pemantauan kendaraan, dan bahkan otomatisasi kendaraan, membantu mengurangi risiko kecelakaan.

IoT menawarkan potensi besar untuk memudahkan hidup kita, meningkatkan efisiensi, dan mengurangi limbah. Namun, ada beberapa tantangan yang harus diatasi, seperti masalah privasi dan keamanan data, standar interoperabilitas, dan kebutuhan untuk mengelola jumlah data yang sangat besar.

DAFTAR PUSTAKA

- A Brief History of the Internet" oleh Barry M. Leiner, Vinton G. Cerf, David D. Clark, et al. (2012). Internet Society.
- Akbar, R. I., Anwar, C., & Siregar, J. H. (2022). MONOGRAF Pengembangan Infrastruktur Wireless Extended LAN. Nas Media PustakaIndonesia.
- Alaydrus, Mudrik (2009). Saluran Transmisi Telekomunikasi. Jogjakarta: Graha Ilmu.
- Anderson, R. (2018). Security Engineering. Wiley.
- Andrew S, Tanenbaum., & David J, Wetherall. (2011). Computer networks fifth edition.
- Bonaventure, O. (2011). *Computer Networking: Principles, Protocols and Practice*. Saylor foundation Washington.
- Buhagiar, J. (2018). CompTIA Network+ Review Guide: Exam N10-007. John Wiley & Sons.
- Byrnes, K. G., Kiely, P. A., Dunne, C. P., McDermott, K. W., & Coffey, J. C. (2021). Communication, collaboration and contagion: "Virtualisation" of anatomy during COVID-19. *Clinical Anatomy*, 34(1), 82-89.
- Carter, J. B., & Farrell, R. B. (2015). Computer Organization and Architecture. Cengage Learning.

- Chang, S. L. (2019). *The Next Wave of Cloud Computing: Architectures, Platforms, and Applications*. Springer.
- Chapman, D. B. (2016). *Clean Code: A Handbook of Agile Software Craftsmanship*. Prentice Hall.
- Cheswick, W. R., Bellovin, S. M., & Rubin, A. D. (2003). *Firewalls and Internet Security: Repelling the Wily Hacker*. Addison-Wesley.
- Cisco. (2022). *Introduction to Network*. Cisco Network Academy. <https://contenthub.netacad.com/itn-dl/1.2.3>.
- Comer, D. (2014). *Fundamentals of computer networking and internetworking*.
- Comer, D. E. (2006). *Internetworking with TCP/IP: Principles, Protocols, and Architecture (Vol. 1)*. Pearson Education.
- Comer, D. E. (2013). *Internetworking with TCP/IP*. Addison-Wesley Professional.
- Computer Networking Problems and Solutions: An innovative approach to building resilient, modern networks" oleh Russ White dan Ethan Banks. (2020). Cisco Press.
- Computer Networking: A Top-Down Approach" oleh James F. Kurose dan Keith W. Ross.
- Computer Networking: Principles, Protocols and Practice" oleh Olivier Bonaventure. (2019). CreateSpace Independent Publishing Platform.

- Computer Organization and Design: The Hardware/Software Interface" oleh David A. Patterson dan John L. Hennessy. (2020). Addison-Wesley.
- Cucculelli, M., & Bettinelli, C. (2015). Business models, intangibles and firm performance: evidence on corporate entrepreneurship from Italian manufacturing SMEs. *Small Business Economics*, 45, 329-350.
- Data Communications and Networking" oleh Behrouz A. Forouzan. *Computer Networks*" oleh Andrew S. Tanenbaum dan David J. Wetherall.
- Dhanjani, N., Rios, B., & Hardin, B. (2017). IoT (Internet of Things) Penetration Testing. O'Reilly Media.
- Diechmann, J., Heineke, K., Reinbacher, T., & Wee, D. (2018). The Internet of Things: How to capture the value of IoT (pp. 1-124). Technical Report, Technical Report.
- Erickson, J. (2014). Hacking: The Art of Exploitation. No Starch Press.
- Esabella, S. (2016). Perancangan Infrastruktur Jaringan Komputer. *Jurnal Matrik*, 6(1),4455. <https://journal.universitاسbumigora.ac.id/index.php/matrik/article/view/16>.
- Evans, P. B., & Wurster, T. S. (1997). Strategy and the new economics of information. *Harvard business review*, 75(5), 70-83.

- Farhat, D., & Awan, M. S. (2021). A brief survey on ransomware with the perspective of internet security threat reports. *2021 9th International Symposium on Digital Forensics and Security (ISDFS)*, 1–6.
- Fatahillah, G. (2019). perkembangan jaringan komputer di indonesia.
- Fitriani, Y. (2021). Pemanfaatan media sosial sebagai media penyajian konten edukasi atau pembelajaran digital. *JISAMAR (Journal of Information System, Applied, Management, Accounting and Research)*, 5(4), 1006-1013.
- Flanagan, D. (2011). *JavaScript: The Definitive Guide: Activate Your Web Pages*. O'Reilly Media.
- Forouzan, B. A. (2007). *Data communications and networking*. Huga Media.
- Forouzan, B. A. (2017). *Cryptography and Network Security*. McGraw-Hill Education.
- Ghosh, P., & Sharma, A. K. (2017). *Internet of Things and Big Data Analytics Toward Next-Generation Intelligence*. Springer.
- Graham, J., Olson, R., & Howard, R. (Eds.). (2016). *Cyber security essentials*. CRC Press.
- Grant, August E. & Meadows, Jennifer H. (2008). *Communication Technology Update and Fundamental*. (ed. 06). Boston: Focal Press. Page 46.
- Green, B., & McDermott, J. D. (2016). *Cybersecurity for Industrial Control Systems*. CRC Press.

- Hacking Exposed: Network Security Secrets & Solutions" oleh Stuart McClure, Joel Scambray, dan George Kurtz. (2018). McGraw-Hill Education.
- Hamacher, V. C., Vranesic, Z. G., & Zaky, S. A. (2011). Computer Organization and Embedded Systems. McGraw-Hill Education.
- Hartpence, B. (2013). A system Administrator's Guide to VoIP Technologies: Packet Guide to Voice over IP (first edit). O'Reilly.
- Hayes, J. P. (2014). Computer Architecture and Organization: An Integrated Approach. Wiley.
- Hennessy, J. L., & Patterson, D. A. (2017). Computer Architecture: A Quantitative Approach. Morgan Kaufmann.
- Hennessy, J. L., & Patterson, D. A. (2019). A New Golden Age for Computer Architecture Research. Communications of the ACM, 62(2), 48-60.
- Hernandez, L., Jimenez, G., Baloco, C., Jimenez, A., & Hernandez, H. (2018). Characterization of the Use of the Internet of Things in the Institutions of Higher Education of the City of Barranquilla and Its Metropolitan Area. In HCI International 2018- Posters' Extended Abstracts: 20th International Conference, HCI International 2018, Las Vegas, NV, USA, July 15-20, 2018, Proceedings, Part III 20 (pp. 17-24). Springer International Publishing.
- Heryana, N., & Hananto, A. (2022). Analysis of Signal Quality, Voice Service, and Data Access on Telkomsel and Indosat Providers in Pakisjaya

District. Buana Information Technology and Computer Sciences (BIT and CS), 3(2), 59-62.

Heryana, N., Solehudin, A., Juardi, D., & Mayasari, R. (2020). Pengukuran Quality of Service (QoS) pada Jaringan Hotspot Universitas Singaperbangsa Karawang. JISICOM (Journal of Information System, Informatics and Computing), 4(1), 99-106.

Hevery, M., & Dahan, G. (2007). Dependency Injection (PDF). Google.

High-Speed Networks and Internets: Performance and Quality of Service" oleh William Stallings.

Howard, M., & Lipner, S. (2006). The Security Development Lifecycle. Microsoft Press.

https://www.google.co.id/books/edition/Ethernet_Switches/_ak0iJuHqQC?hl=en&gbpv=1&dq=switch+network+is&printsec=frontcover.

Hua, J., & Shunwuritu, N. (2021). Research on term extraction technology in computer field based on wireless network technology. Microprocessors and Microsystems, 80, 103336.

Hunt, C. (2012). Networked Applications: A Guide to the New Computing Infrastructure. Elsevier.

Hwang, K., & Briggs, F. A. (2018). Computer Architecture and Parallel Processing. McGraw-Hill Education.

Internetworking with TCP/IP, Vol.1: Principles, Protocols, and Architecture" oleh Douglas E. Comer. (2017). Pearson.

- IPv6 Essentials" oleh Silvia Hagen. (2014). O'Reilly Media.
- Javaid, M., Haleem, A., Singh, R. P., Suman, R., & Gonzalez, E. S. (2022). Understanding the adoption of Industry 4.0 technologies in improving environmental sustainability. *Sustainable Operations and Computers*.
- Kantrowitz, B., & Rogers, A. (1994). The birth of the Internet. *Newsweek*, 124(6), 56-58.
- Karthika, K. C. (2016, March). Wireless mesh network: A survey. In *2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)* (pp. 1966-1970). IEEE.
- Kaur Chahal, J., Bhandari, A., & Behal, S. (2019). Distributed denial of service attacks: a threat or challenge. *New Review of Information Networking*, 24(1), 31-103.
- Khanh, Q. V., Hoai, N. V., Manh, L. D., Le, A. N., & Jeon, G. (2022). Wireless communication technologies for IoT in 5G: Vision, applications, and challenges. *Wireless Communications and Mobile Computing*, 2022, 1-12.
- Khanvilkar, S., & Khokhar, A. (2004). Virtual private networks: an overview with performance evaluation. *IEEE Communications Magazine*, 42(10), 146-154.
- Kizza, J. M., & Kizza, J. M. (2017). *Computer Network Security Fundamentals. Guide to Computer Network Security*, 41-57.

- Kozierok, C. (2005). *The TCP/IP guide: A comprehensive, illustrated Internet protocols reference*. No Starch Press.
- Kurose J., F., and Ross K. (2017). *Computer Networking: a top-down approach, 7th edition*. Amherst. University of Massachusetts, NYU and NYU Shanghai. LCCN 2016004976 | ISBN 9780133594140 | ISBN 0133594149.
- Kurose J., F., and Ross K. (2020). *Computer Networking: a top-down approach, 8th edition*. Amherst. University of Massachusetts. ISBN-13: 9780135928615.
- Kurose, J. F., & Ross, K. W. (2007). *Computer Networking: A Top-Down Approach*. Edition. Addison Wesley.
- Kurose, J. F., & Ross, K. W. (2016). *Computer Networking: Principles, Protocols and Practice*. CreateSpace Independent Publishing Platform.
- Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., ... & Wolff, S. S. (1997). The past and future history of the Internet. *Communications of the ACM*, 40(2), 102-108.
- Lelisa, W. A., Barovich, G., Bayu H. S., dkk. (2022). *Teknologi Jaringan Komputer*. Bandung. Penerbit Widina.
- Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, 7, 8176-8186.

- Lili, C. (2012). VoIP System Simulation Design and Implementation. 2012 Second International Conference on Instrumentation, Measurement, Computer, Communication and Control, 296–298. <https://doi.org/10.1109/IMCCC.2012.73>.
- Liu, X., & Deng, N. (2020). Emerging optical communication technologies for 5G. In Optical fiber telecommunications VII (pp. 751-783). Academic Press.
- Liu, X., Zhang, T., Hu, N., Zhang, P., & Zhang, Y. (2020). The method of Internet of Things access and network communication based on MQTT. Computer Communications, 153, 169-176.
- Mahendran, R. (2016, May). Integrated LiFi (Light Fidelity) for smart communication through illumination. In 2016 International Conference on Advanced Communication Control and Computing Technologies (ICACCCT) (pp. 53-56). IEEE.
- Mano, M. M., & Kime, C. R. (2019). Logic and Computer Design Fundamentals. Pearson.
- Network Security Essentials: Applications and Standards" oleh William Stallings. (2016). Pearson.
- Network Warrior: Everything You Need to Know That Wasn't on the CCNA Exam" oleh Gary A. Donahue.
- Newman, S. (2015). Building Microservices: Designing Fine-Grained Systems. O'Reilly Media.
- Northcutt, S., & Novak, J. (2016). Network Intrusion Detection: An Analyst's Handbook. New Riders.

- Nuaymi, L. (2007). WiMAX: technology for broadband wireless access. John Wiley & Sons.
- Nurakun Kyzy, Z., Ismailova, R., & Dündar, H. (2018). Learning management system implementation: a case study in the Kyrgyz Republic. *Interactive Learning Environments*, 26(8), 1010-1022.
- Osterwalder, A., Pigneur, Y., & Clark, T. (2010). *Business Model Generation: A Handbook for Visionaries, Game Changers, and Challengers*. Wiley.
- Parhami, B. (2017). *Computer Architecture: From Microprocessors to Supercomputers*. Oxford University Press.
- Patterson, D. A., & Hennessy, J. L. (2017). A New Golden Age for Computer Architecture. *ACM Computing Surveys*, 50(2), 1-39.
- Patterson, D. A., & Hennessy, J. L. (2017). *Computer Organization and Design: The Hardware/Software Interface*. Morgan Kaufmann.
- Patterson, D. A., Asanović, K., & Asanović, K. (2017). *RISC-V Reader: An Open Architecture Atlas*. Strawberry Canyon LLC.
- Pavlicek, A., & Sudzina, F. (2018, December). Internet Security and Privacy in VPN. In *International Conference on Digital Information Management* International Conference on Digital Information Management (Vol. 9, pp. 133-139).
- Peterson, L. L., & Davie, B. S. (2007). *Computer networks: a systems approach*. Elsevier.

- Porumb, C., Porumb, S., Orza, B., & Budura, D. (2010, July). Computer-supported collaborative work and its application to e-health. In 2010 Third International Conference on Advances in Mesh Networks (pp. 75-80). IEEE.
- Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems" oleh Chris Sanders. (2017). No Starch Press.
- Press, C. (2013). Exploring the Modern Computer Network: Types, Functions, and Hardware. CiscoPress.
<https://www.ciscopress.com/articles/article.asp?p=2158215>.
- Qian, Y., Wu, D., Bao, W., & Lorenz, P. (2019). The internet of things for smart cities: Technologies and applications. *IEEE Network*, 33(2), 4–5.
- Rao, S. K., & Prasad, R. (2018). Impact of 5G technologies on industry 4.0. *Wireless personal communications*, 100, 145-159.
- Richardson, L., & Amundsen, M. (2020). *Microservice Architecture: Aligning Principles, Practices, and Culture*. O'Reilly Media.
- RISC-V Reader: An Open Architecture Atlas" oleh David A. Patterson dan Andrew Waterman. (2017). SiFive.
- Ristic, I., & Dierks, T. (2013). *Bulletproof SSL and TLS: Understanding and Deploying SSL/TLS and PKI to Secure Servers and Web Applications*. Syngress.

- Roberts, D. F., & Foehr, U. G. (2008). Trends in media use. The future of children, 11-37.
- Rodrigues, T. K., Verma, S., Kawamoto, Y., Kato, N., Fouda, M. M., & Ismail, M. (2023). Smart Handover with Predicted User Behavior using Convolutional Neural Networks for WiGig Systems. arXiv preprint arXiv:2303.15731.
- Samsudin, dkk (2019). Pengenalan Koputer dan teknologi Informasi. Medan. Perdana Publishin
- Sari, I. P., Hutagalung, F. S., & Hutasuhut, B. K. (2020). InfoTekJar: Jurnal Nasional Informatika dan Teknologi Jaringan Analisa Model Pemanfaatan Jaringan Komputer yang Efektif untuk Peningkatan Produktivitas pada Jaringan LAN Universitas Muhammadiyah Sumatera Utara. Infotekjar, 5(1),193–197.
<https://doi.org/https://doi.org/10.30743/infotekjar.v5i1.3229>.
- Scarfone, K., & Mell, P. (2007). Guide to Intrusion Detection and Prevention Systems (IDPS). NIST Special Publication.
- Scott, J. (2017). The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities. Addison-Wesley Professional.
- Securing the Internet of Things" oleh Shancang Li, Li Da Xu, dan Surya Nepal. (2017). Syngress.
- Severance, C. R. (2013). Python for Informatics: Exploring Information. CreateSpace Independent Publishing Platform.

- Shostack, A. (2014). *Threat Modeling: Designing for Security*. Wiley.
- Sidhu, J. (2017). Syscoin: A peer-to-peer electronic cash system with blockchain-based services for e-business. *2017 26th International Conference on Computer Communication and Networks (ICCCN)*, 1–6
- Smith, M., & Marchesini, J. (2011). *The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws*. Wiley.
- Spurgeon, C. E., & Zimmerman, J. (2013). *Ethernet Switches (First Edit)*. O'Reilly Media.
- Stallings, W. (2015). *Computer Organization and Architecture: Designing for Performance*. Pearson.
- Stallings, W. (2016). *Data and Computer Communications (10th Edition)*. Pearson.
- Stallings, W. (2016). *Data and Computer Communications (10th Edition)*. Pearson.
- Stallings, W. (2016). *Network security essentials: applications and standards*. Pearson.
- Stallings, W. (2017). *Network Security Essentials: Applications and Standards*. Pearson.
- Stark, D. (1997). The rise of the network society. *Contemporary Sociology*, 26(6), 725.
- Straubhaar, Joseph & LaRose, Robert. (2004). *Media Now: Communications Media in the Information Age*. Belmont, CA: Wadsworth. Page 30-63.

- Sundmaeker, H., Guillemin, P., Friess, P., & Woelfflé, S. (2010). Vision and Challenges for Realising the Internet of Things. Cluster of European Research Projects on the Internet of Things.
- Syahrial, Melwin. (2005). Pengantar Jaringan Komputer. Andi. Yogyakarta.
- Tanenbaum, A. S., & Austin, T. (2015). Structured Computer Organization. Pearson.
- Tanenbaum, A. S., & Bos, H. (2014). Modern Operating Systems. Pearson.
- Tanenbaum, A. S., & Wetherall, D. J. (2011). Computer networks (5th ed.). Pearson.
- Tanenbaum, A. S., & Wetherall, D. J. (2018). Computer Networks (6th Edition). Pearson.
- Tanenbaum, A. S., Wetherall, D. (2011). Computer networks (5th ed.). Pearson.
- TCP/IP Illustrated, Volume 1: The Protocols" oleh W. Richard Stevens.
- TCP/IP Illustrated, Volume 1: The Protocols" oleh W. Richard Stevens. (2011). Addison-Wesley Professional.
- TCP/IP Protocol Suite" oleh Behrouz A. Forouzan. (2016). McGraw-Hill Education.
- The Internet's Coming of Age" oleh Mike Sendall. (2017). CreateSpace Independent Publishing Platform.
- Thohari, A N. A., Karima, A. (2021). Pengenalan Perangkat Jaringan Komputer Menggunakan

Teknologi Augmented Reality. Politeknik Negeri Semarang. JTET (Jurnal Teknik Elektro Terapan), 10(1), 58–66. e-ISSN:2503-2941.

Tilkov, S., & Vinoski, S. (2010). Node.js: Using JavaScript to Build High-Performance Network Programs. *ACM Queue*, 8(1), 24-32.

Whitman, M. E., & Mattord, H. J. (2017). *Principles of Information Security*. Cengage Learning.

Yigit, M., Gungor, V. C., & Baktir, S. (2014). Cloud computing for smart grid applications. *Computer Networks*, 70, 312-329.

Zikopoulos, P., & Eaton, C. (2011). *Understanding Big Data: Analytics for Enterprise Class Hadoop and Streaming Data*. McGraw-Hill Osborne Media.

Zorzi, M., Gluhak, A., Lange, S., & Bassi, A. (2010). From today's intranet of things to a future internet of things: a wireless-and mobility-related view. *IEEE Wireless communications*, 17(6), 44-51.

PENGENALAN DASAR JARINGAN KOMPUTER

Dalam era teknologi informasi yang semakin berkembang pesat, pemahaman dasar tentang jaringan komputer menjadi sangat penting. Pengetahuan mengenai bagaimana data dan informasi dapat berpindah dengan cepat antar perangkat, baik dalam skala lokal maupun global, telah menjadi bagian tak terpisahkan dari kehidupan sehari-hari.

Buku ini, "Pengenalan Dasar Jaringan Komputer," disusun dengan tujuan untuk memberikan pemahaman dasar tentang konsep jaringan komputer kepada pembaca. Buku ini akan membantu pembaca memahami bagaimana jaringan komputer bekerja, jenis-jenisnya, serta manfaat dan tantangan yang terkait dengan penggunaan jaringan komputer.



CV REY MEDIA GRAFIKA
EMAIL:
REYMEDIAGRAFIKA.RGM@GMAIL.COM

ISBN 978-623-88689-3-3



9 786238 868933