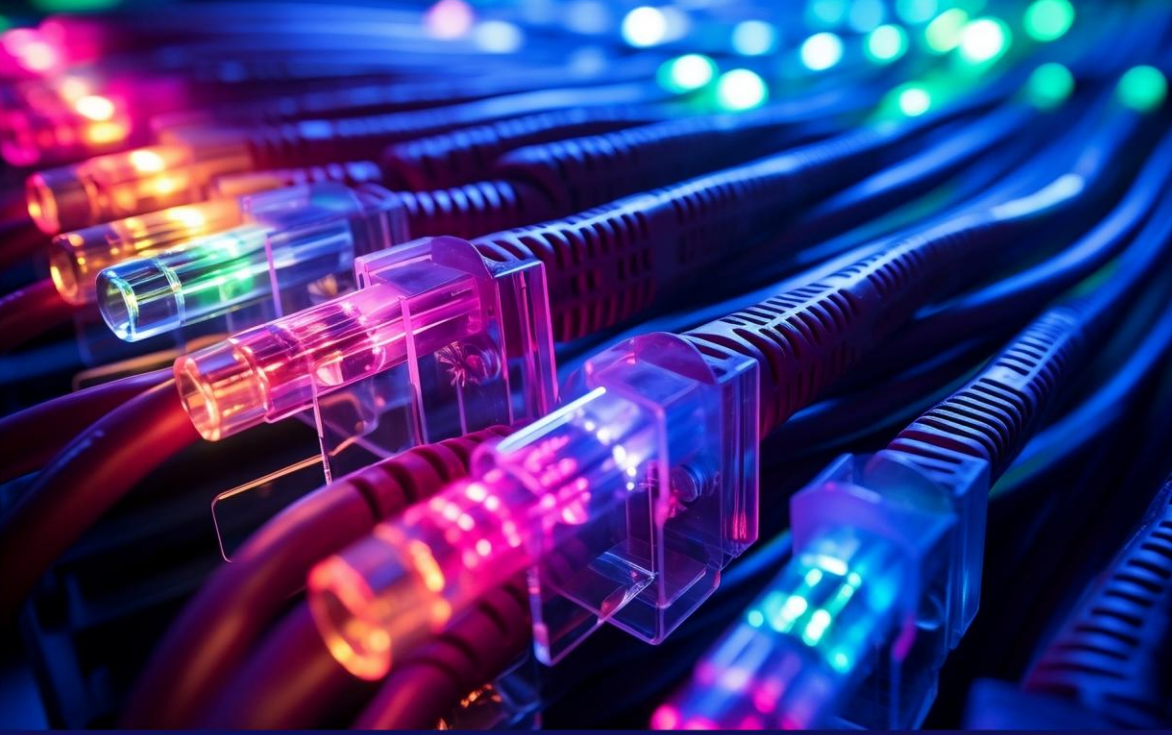


JARINGAN KOMPUTER

Penulis :
Ir. Ida Bagus Kerthyayana Manuaba, S.T., Ph.D
Prof. Dr. Fahrul Agus, S.Si., M.T., MTA., MCE
Ir. I Made Satrya Ramayu, S.Kom., M.Kom
Vian Ardiyansyah Saputro, S.ST., M.Kom
Andy Victor Pakpahan, M.T
Julia R.Skawanti, S.Kom., M.Kom
Loso Judijanto

SONPEDIA.COM
PT. Sonpedia Publishing Indonesia

JARINGAN KOMPUTER

Penulis :
Ir. Ida Bagus Kerthyayana Manuaba, S.T., Ph.D
Prof. Dr. Fahrul Agus, S.Si., M.T., MTA., MCE
Ir. I Made Satrya Ramayu, S.Kom., M.Kom
Vian Ardiyansyah Saputro, S.ST., M.Kom
Andy Victor Pakpahan, MT
Julia R.Skawanti, S.Kom., M.Kom
Loso Judijanto

Penerbit:
SONPEDIA
Publishing Indonesia

JARINGAN KOMPUTER

Penulis :
Ir. Ida Bagus Kerthyayana Manuaba, S.T., Ph.D
Prof. Dr. Fahrul Agus, S.Si., M.T., MTA., MCE
Ir. I Made Satrya Ramayu, S.Kom., M.Kom
Vian Ardiyansyah Saputro, S.ST., M.Kom
Andy Victor Pakpahan, MT
Julia R.Skawanti, S.Kom., M.Kom
Loso Judijanto

ISBN : 978-623-514-639-3

Editor:
Ida Kumala Sari
Penyunting :
Inayah Uzma
Desain sampul dan Tata Letak:
Yayan Agusdi

Penerbit :
PT. Sonpedia Publishing Indonesia
Redaksi :
Jl. Kenali Jaya No 166 Kota Jambi 36129 Tel +6282177858344
Email: sonpediapublishing@gmail.com
Website: www.buku.sonpedia.com
Anggota IKAPI : 006/JBI/2023

Cetakan Pertama, Mei 2025

KATA PENGANTAR

Puji syukur kepada Allah SWT yang telah memberikan rahmat dan hidayah-Nya sehingga penulis dapat menyelesaikan buku ini dengan baik. Buku ini berjudul "*JARINGAN KOMPUTER*". Tidak lupa kami ucapkan terima kasih bagi semua pihak yang telah membantu dalam penulisan dan penerbitan buku ini.

Buku "Jaringan Komputer" membahas secara sistematis dasar-dasar hingga konsep lanjutan dalam dunia jaringan. Dimulai dengan pengenalan jaringan komputer, buku ini menjelaskan jenis-jenis jaringan serta manfaatnya dalam kehidupan modern. Pembahasan dilanjutkan dengan Model Referensi OSI dan TCP/IP sebagai acuan komunikasi data, diikuti dengan penjelasan berbagai media transmisi jaringan, baik kabel maupun nirkabel. Buku ini juga mengulas perangkat jaringan yang berperan penting dalam membentuk infrastruktur jaringan.

Selain itu, buku ini membahas pengalamatan IP dan subnetting secara detail, memungkinkan pembaca memahami cara pengelolaan alamat IP dalam jaringan. Protokol jaringan seperti TCP, UDP, HTTP, dan lainnya juga dijelaskan secara praktis. Di bagian akhir, disajikan topik penting tentang keamanan jaringan, termasuk ancaman dan langkah proteksi seperti firewall dan enkripsi. Buku ini cocok untuk mahasiswa, praktisi, dan siapa saja yang ingin memahami jaringan komputer secara menyeluruh dan aplikatif.
Buku ini mungkin masih terdapat kekurangan dan kelemahan. Oleh karena itu, saran dan kritik para pemerhati sungguh penulis harapkan. Semoga buku ini memberikan manfaat dan menambah khasanah ilmu pengetahuan.

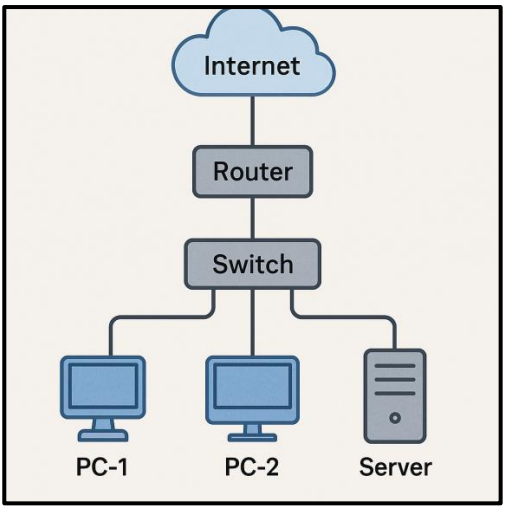
Jakarta, Mei 2025
Penulis

DAFTAR ISI

BAGIAN 1
PENGENALAN JARINGAN KOMPUTER

A. DEFINISI JARINGAN KOMPUTER

Jaringan komputer adalah kumpulan komputer dan perangkat digital lainnya yang saling terhubung dan mampu berbagi sumber daya serta berkomunikasi satu sama lain (Patel, 2024). Jaringan komputer memainkan peran penting dalam lanskap digital modern, secara signifikan mempengaruhi cara informasi diakses, disimpan, dan dipertukarkan secara global. Gambar 1.1 menunjukkan Struktur Dasar Jaringan Komputer.

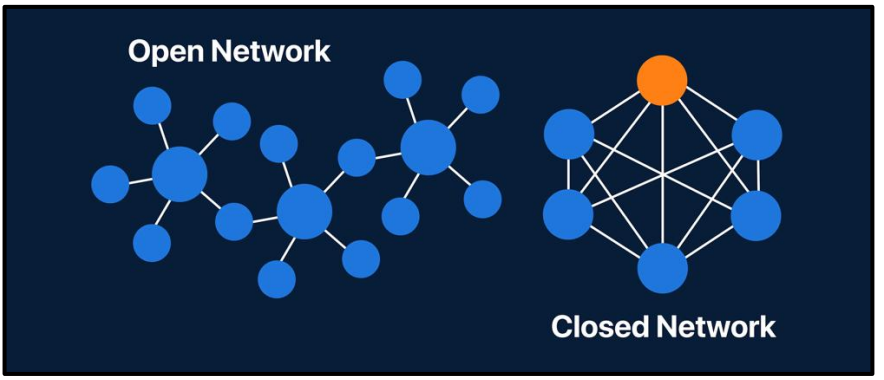


Gambar 1.1 Struktur Dasar Jaringan Komputer

Jaringan-jaringan ini memungkinkan berbagai aplikasi untuk mengakses sumber daya seperti World Wide Web, server aplikasi

dan penyimpanan bersama, printer, mesin faks, dan alat komunikasi seperti email dan platform pesan instan. Mereka memfasilitasi berbagi informasi yang efisien di berbagai tugas dan domain, mendorong kolaborasi dan menyederhanakan alur kerja.

Jaringan komputer umumnya dapat diklasifikasikan ke dalam dua kategori besar: sistem terbuka dan sistem tertutup (Lihat Gambar 1.2). Sistem terbuka dengan mudah terhubung ke jaringan dan dirancang khusus untuk komunikasi, sedangkan sistem tertutup memerlukan autentikasi yang tepat dan biasanya kurang dapat diakses oleh jaringan eksternal (Yeşil, 2023). Perbedaan ini menekankan fleksibilitas dan adaptabilitas jaringan komputer dalam memenuhi berbagai kebutuhan aplikasi dan persyaratan pengguna.



Gambar 1.2 Perbandingan antara Sistem Jaringan Terbuka dan Tertutup

Perkembangan dan adopsi luas jaringan komputer telah menjadi kunci dalam membentuk ekosistem digital saat ini (Sunkari, 2021). Seiring dengan terus berkembangnya teknologi, jaringan komputer

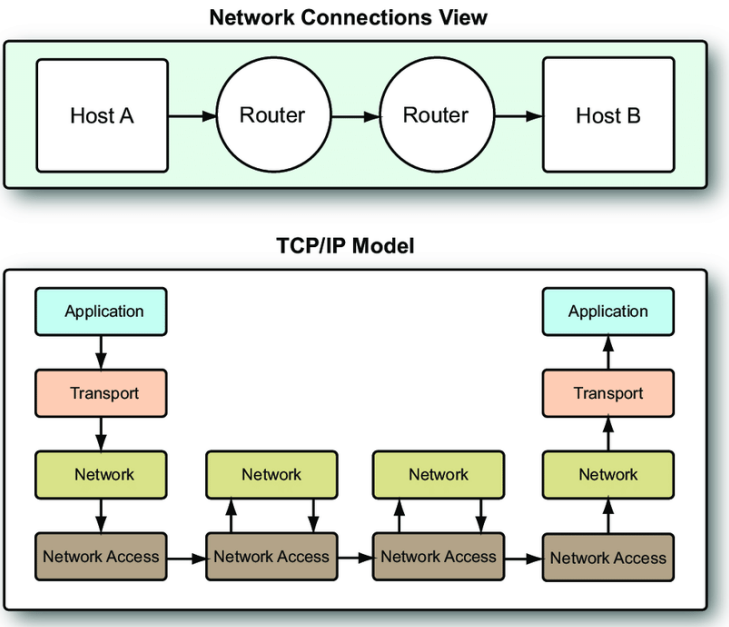
diharapkan akan memainkan peran yang semakin penting dalam memungkinkan inovasi baru dan mengubah cara kita berinteraksi, berkolaborasi, dan mengakses informasi secara global. Internet, contoh paling menonjol dari jaringan komputer, jelas mencerminkan keterhubungan ini.

Node jaringan mengacu pada perangkat komputasi yang berasal, mentransmisikan, dan mengakhiri data dalam jaringan. Contoh umum dari *node* termasuk komputer pribadi, *smartphone*, server, dan peralatan jaringan seperti *router* dan *switch* (Patel, 2024; Sunkari, 2021). Ketika perangkat dapat bertukar informasi, baik terhubung langsung maupun tidak, mereka dianggap terhubung dalam jaringan.

B. PERKEMBANGAN SEJARAH JARINGAN KOMPUTER

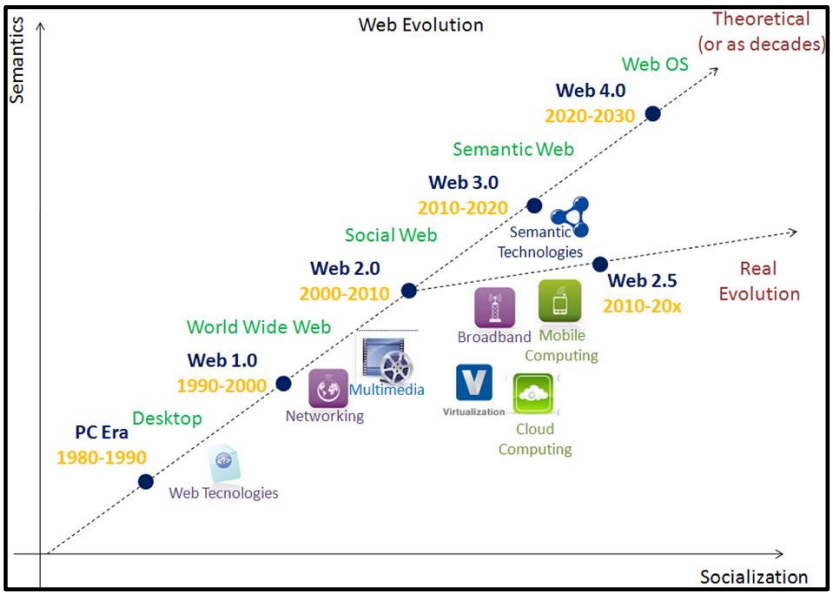
Sejarah jaringan komputer bermula pada akhir 1960-an, dimulai dengan pengembangan Jaringan Proyek Penelitian Lanjutan (ARPANET) oleh Departemen Pertahanan AS. Awalnya, jaringan perintis ini dirancang untuk memfasilitasi komunikasi yang aman dan tangguh selama konflik militer (Campbell-Kelly & Garcia-Swartz, 2013). ARPANET mewakili kemajuan yang signifikan, menandai awal dari sistem komputer yang saling terhubung dan meletakkan dasar penting bagi Internet modern.

Pada tahun 1970-an, tonggak penting lainnya dalam evolusi jaringan komputer dicapai dengan diperkenalkannya Transmission Control Protocol/Internet Protocol (TCP/IP) (Campbell-Kelly & Garcia-Swartz, 2013). Protokol komunikasi standar ini secara signifikan memungkinkan berbagai sistem komputer untuk bertukar data dengan andal dan efisien. TCP/IP menjadi dasar, mendorong adopsi luas dan ekspansi cepat teknologi jaringan di seluruh dunia. Lapisan TCP/IP dan model komunikasi dapat dilihat pada Gambar 1.3.



Gambar 1.3 Diagram yang menggambarkan lapisan TCP/IP dan model komunikasi

Tahun 1980-an membawa kemajuan transformatif lainnya—penciptaan World Wide Web, yang diperkenalkan oleh Tim Berners-Lee pada tahun 1989 (Sudeep et al., 2022). Gambar 1.4 menunjukkan bahwa Web merevolusi cara informasi diakses, dibagikan, dan disebarluaskan secara global. Ini memfasilitasi penciptaan jaringan luas yang saling terhubung dari situs web dan sumber daya online, yang sangat meningkatkan komunikasi, kolaborasi, dan aksesibilitas informasi.



Gambar 1.4 Garis waktu yang menggambarkan tonggak-tonggak penting yang mengarah ke World Wide Web dan pertumbuhannya yang pesat (sumber: https://medium.com/@vivekmadurai/web-evolution-from-1-0-to-3-0-e84f2c06739)

Beberapa dekade berikutnya menyaksikan ekspansi cepat teknologi *broadband* dan nirkabel, yang secara signifikan meningkatkan cakupan, kecepatan, dan kemampuan jaringan komputer secara global (Kan & Kim, 2019). Teknologi seperti serat optik kecepatan tinggi, standar jaringan nirkabel (misalnya, *Wi-Fi*, data seluler), dan proliferasi perangkat seluler mengubah aksesibilitas dan ketersediaan jaringan, mengintegrasikannya secara mendalam ke dalam kehidupan sehari-hari.

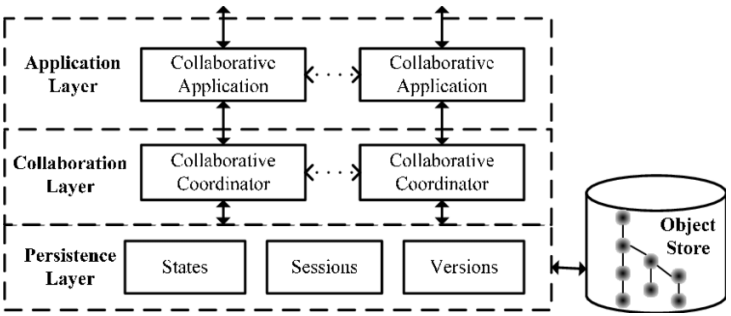
C. MANFAAT JARINGAN KOMPUTER

Jaringan komputer menawarkan banyak keuntungan, secara signifikan mengubah cara kita mengakses, berbagi, dan mengelola informasi. Salah satu manfaat utamanya adalah berbagi sumber daya. Melalui perangkat yang saling terhubung, pengguna dapat mengakses sumber daya bersama seperti printer, server penyimpanan, basis data, dan daya komputasi dengan lancar. Sentralisasi sumber daya ini tidak hanya meningkatkan efisiensi tetapi juga mengurangi biaya operasional bagi organisasi (Rahman et al., 2022).

Selain itu, jaringan komputer telah secara signifikan meningkatkan kemampuan komunikasi dan kolaborasi. Karyawan dan pengguna dapat dengan mudah bertukar ide, dokumen, dan menerima pembaruan secara real-time, yang mendorong lingkungan kerja yang lebih terhubung, gesit, dan produktif (Patel, 2024).

Kemampuan untuk berkomunikasi dan berkolaborasi tanpa memandang batasan geografis telah mengubah dinamika tempat kerja tradisional, memungkinkan tim untuk beroperasi secara efektif dari lokasi terpencil dan di berbagai zona waktu.

Keuntungan signifikan lainnya yang diberikan oleh jaringan komputer adalah manajemen informasi yang lebih baik. Sistem penyimpanan data terpusat memungkinkan organisasi untuk lebih baik mengatur, mengamankan, mencadangkan, dan mengambil informasi penting dengan efisien. Sentralisasi semacam itu memastikan integritas, keamanan, dan ketersediaan data, yang sangat meningkatkan ketahanan dan responsivitas organisasi (Open-E, 2023).



Gambar 1.5 Ilustrasi yang menggambarkan Lingkungan Kerja Kolaboratif yang didukung oleh Jaringan Komputer

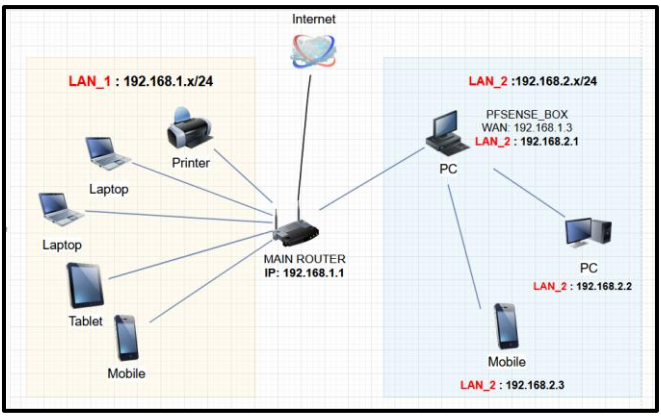
Selain itu, seperti yang diilustrasikan dalam Gambar 1.5, sifat kolaboratif dari jaringan komputer telah secara mendasar mengubah praktik kerja. Dengan memfasilitasi berbagi sumber daya yang mudah dan menyederhanakan komunikasi, jaringan telah

memungkinkan kerja tim yang lebih efisien dan efektif. Karyawan dapat berkolaborasi dengan lancar dalam proyek, berbagi pengetahuan, dan mengoordinasikan tugas, yang mengarah pada peningkatan produktivitas, inovasi, dan kelincahan organisasi.

D. JENIS-JENIS JARINGAN KOMPUTER

Jaringan komputer dapat diklasifikasikan berdasarkan beberapa faktor, termasuk ukuran, cakupan geografis, dan tujuan yang dimaksudkan (Ahmad, 2023):

Jaringan Area Lokal (Local Area Network - LAN)



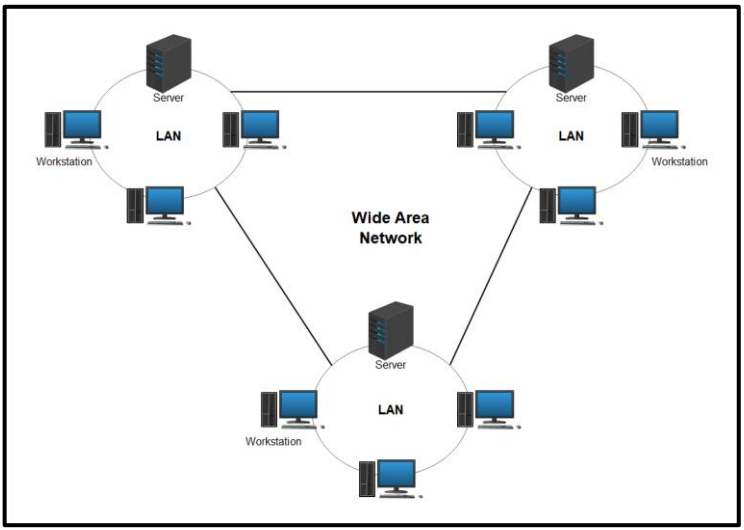
Gambar 1.8 Tipikal Konfigurasi LAN

Jaringan Area Lokal (LAN) mencakup area geografis yang relatif kecil, seperti kantor, kampus, atau gedung. Ini memungkinkan perangkat yang berdekatan untuk berkomunikasi secara efektif dan efisien berbagi sumber daya. LAN biasanya mendukung kecepatan

transfer data yang tinggi, yang membuatnya ideal untuk lingkungan rumah, institusi pendidikan, dan bisnis kecil hingga menengah.

Jaringan lokal (LAN) umumnya menggunakan teknologi seperti Ethernet dan Wi-Fi. Jaringan Ethernet menggunakan kabel fisik, biasanya pasangan berpilin tembaga atau serat optik, untuk menghubungkan perangkat dan mengirimkan data dengan kecepatan tinggi. Jaringan LAN nirkabel (WLAN) memanfaatkan teknologi Wi-Fi, memungkinkan perangkat untuk terhubung tanpa kabel fisik, sehingga memberikan fleksibilitas dan mobilitas yang lebih besar (Jalil, 2022).

Jaringan Area Luas (Wide Area Network - WAN)



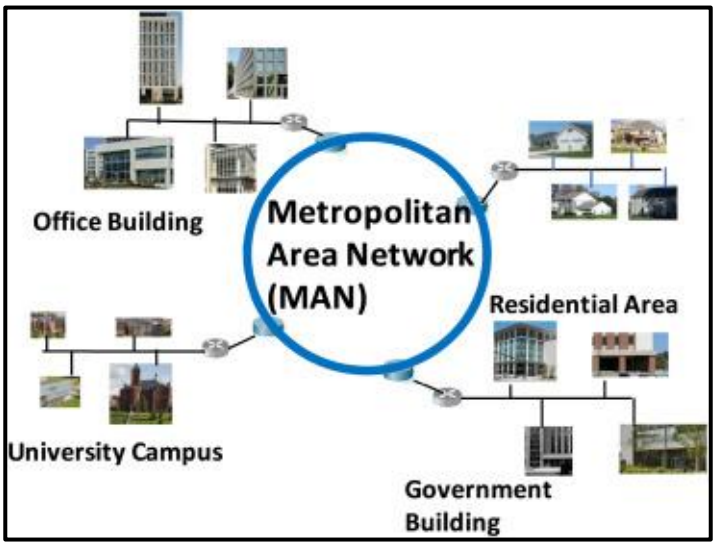
Gambar 1.9 Contoh Konektivitas WAN

Jaringan Area Luas (WAN) mencakup wilayah geografis yang jauh lebih besar, sering kali menghubungkan beberapa LAN di berbagai jarak yang jauh. WAN memungkinkan komunikasi dan berbagi data antara lokasi yang tersebar secara geografis seperti kantor cabang, kantor pusat, dan fasilitas jarak jauh. WAN umumnya menawarkan kecepatan transfer data yang lebih rendah dibandingkan dengan LAN karena jarak dan keterbatasan infrastruktur, tetapi keuntungan utamanya adalah cakupan geografis yang luas.

WAN sering menggunakan teknologi seperti leased lines, Multi-Protocol Label Switching (MPLS), Virtual Private Networks (VPN), dan komunikasi satelit untuk mencapai konektivitas jarak jauh. Organisasi besar dan perusahaan multinasional sangat bergantung pada infrastruktur WAN untuk memastikan komunikasi yang andal antara lokasi-lokasi mereka yang tersebar, meningkatkan koordinasi operasional dan produktivitas (Ahmed et al., 2016).

Jaringan Area Metropolitan (Metropolitan Area Network - MAN)

Jaringan Area Metropolitan (MAN) melayani daerah perkotaan atau seluruh kota, menjembatani kesenjangan antara LAN dan WAN. Ini biasanya mencakup area geografis yang lebih besar dari LAN tetapi lebih kecil dari WAN, biasanya terbatas pada wilayah metropolitan. MAN menghubungkan beberapa LAN, menyediakan layanan komunikasi data berkecepatan tinggi kepada organisasi dan individu di dalam kota atau wilayah.



Gambar 1.10 Struktur MAN dalam sebuah Kota

Implementasi MAN sering menggunakan kabel serat optik atau koneksi nirkabel berkecepatan tinggi seperti jaringan Wi-Fi metropolitan. Mereka biasanya diterapkan oleh lembaga pemerintah, sistem kesehatan, institusi pendidikan, dan perusahaan besar untuk menyediakan konektivitas yang andal dan berkecepatan tinggi antara berbagai fasilitas mereka di dalam sebuah kota. MAN membantu memastikan berbagi informasi yang efisien dan meningkatkan operasi sektor publik dan swasta di dalam area perkotaan.

Jaringan Area Pribadi (Personal Area Network - PAN)

Jaringan Area Pribadi (PAN) menghubungkan perangkat elektronik pribadi seperti *smartphone*, tablet, laptop, dan teknologi yang dapat dikenakan dalam jarak pendek, biasanya dalam jarak 10

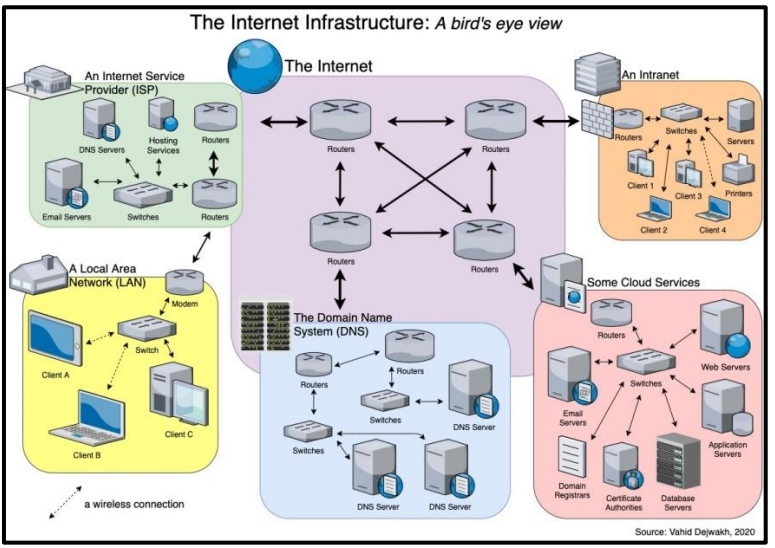
meter atau kurang. PAN memfasilitasi pertukaran data dan sinkronisasi antara perangkat individu, memungkinkan konektivitas yang mulus dan nyaman dalam lingkungan pribadi atau terlokalisasi.

PAN biasanya menggunakan standar komunikasi nirkabel jarak pendek seperti *Bluetooth*, *Zigbee*, dan *Near-Field Communication* (NFC). Contoh aplikasi PAN termasuk ekosistem *wearable* pintar untuk pemantauan kesehatan, konektivitas *headphone* nirkabel, dan sinkronisasi perangkat pribadi, yang meningkatkan kenyamanan dan pengalaman pengguna yang dipersonalisasi (Viehland & Zhao, 2010).

Gambar 1.11 Konfigurasi Jaringan Area Pribadi

Internet

Internet adalah jaringan komputer yang paling dikenal dan luas di seluruh dunia (Sunkari, 2021). Ini terdiri dari jaringan global yang luas dari jaringan komputer yang saling terhubung yang menggunakan Protokol Internet (IP) standar untuk memfasilitasi komunikasi dan berbagi sumber daya di antara miliaran pengguna di seluruh dunia (Sunkari, 2021). Internet memungkinkan konektivitas di berbagai jaringan, memungkinkan perangkat di seluruh dunia untuk berkomunikasi, mengakses sumber daya seperti World Wide Web, berbagi aplikasi dan server penyimpanan, menggunakan printer dan mesin faks secara jarak jauh, serta berkomunikasi melalui email dan aplikasi pesan instan (Patel, 2024; Sunkari, 2021).



Gambar 1.12 Infrastruktur Global Internet

Jaringan komputer sangat penting untuk komunikasi modern, mendukung berbagai aplikasi mulai dari konektivitas pribadi hingga operasi perusahaan global. Memahami dasar-dasar jaringan, termasuk konteks historisnya, jenisnya, komponennya, topologinya, dan protokolnya, memberikan fondasi yang solid untuk mengeksplorasi konsep jaringan yang lebih lanjut.

BAGIAN 2
MODEL REFERENSI OSI DAN TCP/IP

A. PENGANTAR DAN RUANG LINGKUP

Dalam dunia jaringan komputer, komunikasi antar perangkat tidak mungkin terjadi tanpa adanya standar yang mengatur bagaimana data dikirim dan diterima. Dua model arsitektur jaringan yang paling dikenal dan digunakan secara luas adalah Model Referensi OSI (Open Systems Interconnection) dan Model TCP/IP (Transmission Control Protocol/Internet Protocol). Kedua model ini berperan penting dalam memahami dan merancang sistem komunikasi data yang kompleks agar dapat bekerja secara efektif dan efisien.

Model OSI dikembangkan oleh International Organization for Standardization (ISO) sebagai kerangka kerja konseptual yang membagi fungsi komunikasi jaringan ke dalam tujuh lapisan terstruktur. Sementara itu, model TCP/IP pertama kali dikembangkan oleh Departemen Pertahanan Amerika Serikat dan digunakan sebagai dasar dari internet. Model ini lebih sederhana dan terdiri dari empat lapisan utama yang menggambarkan bagaimana data diproses dan ditransmisikan melalui jaringan.

Pembahasan bab ini akan memberikan pengantar umum mengenai konsep dasar kedua model tersebut, membahas tujuan, manfaat,

serta ruang lingkup penggunaannya dalam dunia jaringan komputer. Fokus utama pembahasan mencakup perbandingan struktur lapisan, fungsi masing-masing lapisan, serta relevansinya dalam implementasi teknologi jaringan modern. Dengan pemahaman ini, diharapkan pembaca dapat memperoleh gambaran menyeluruh mengenai pentingnya model referensi dalam mendesain dan mengelola sistem jaringan.

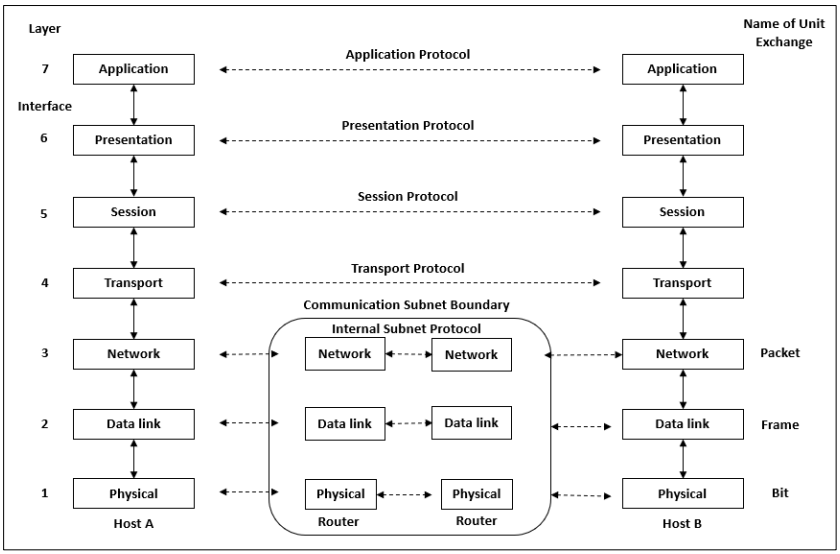
B. MODEL REFERENSI OSI

Model Referensi OSI (Open Systems Interconnection) merupakan kerangka kerja konseptual yang dikembangkan oleh ISO untuk menjelaskan bagaimana sistem komunikasi jaringan dapat berinteraksi. Model ini terdiri dari tujuh lapisan (layers) yang masing-masing memiliki fungsi khusus. Model OSI seperti yang ilustrasikan oleh Gambar 2.1.

Prinsip-prinsip yang diterapkan untuk mencapai tujuh lapisan tersebut dapat diringkas secara singkat sebagai berikut:

1. Lapisan harus dibuat jika abstraksi yang berbeda diperlukan.
2. Setiap lapisan harus menjalankan fungsi yang terdefinisi dengan baik.
3. Fungsi setiap lapisan harus dipilih dengan mempertimbangkan pendefinisian protokol standar internasional.
4. Batasan lapisan harus dipilih untuk meminimalkan aliran informasi di antara antarmuka.

5. Jumlah lapisan harus cukup besar sehingga fungsi-fungsi yang berbeda tidak perlu disatukan dalam lapisan yang sama karena kebutuhan dan cukup kecil sehingga arsitekturnya tidak menjadi sulit diatur.



Gambar 2.1 Lapisan Model Referensi OSI (Sumber: Tanembaum & Wetherall 2011)

Penjelasan tiap layer disajikan sebagai berikut. Pengiriman bit mentah melalui saluran komunikasi adalah tugas utama dari Physical layer. Ini berkaitan dengan keyakinan bahwa, ketika satu pihak mengirim bit 1, pihak lain akan menerima bit tersebut sebagai bit 1, bukan sebagai bit 0.

Selanjutnya, mengubah fasilitas transmisi mentah menjadi saluran yang tampak bebas dari kesalahan transmisi yang tidak terdeteksi

adalah tugas utama Data link layer. Untuk mencapai tujuan ini, kesalahan sebenarnya ditutup sehingga lapisan jaringan tidak dapat melihatnya. Lapisan ini menyelesaikan tugas ini dengan meminta pengirim memecah data input menjadi Frame, yang biasanya terdiri dari ratusan atau ribu byte, dan kemudian mengirimkan Frame secara berurutan. Penerima mengirimkan kembali Acknowledgement Frame untuk mengonfirmasi bahwa setiap Frame diterima dengan benar jika layanan tersebut dapat dipercaya.

Operasi subnet diawasi oleh Network layer. Ini berkaitan dengan menentukan paket mana yang harus dirutekan dari sumber ke tujuan. Tabel statis yang "dihubungkan" ke jaringan dapat menjadi dasar rute, yang seringkali dapat diperbarui secara otomatis untuk menghindari komponen yang tidak berfungsi. Rute juga dapat ditetapkan di awal setiap percakapan, seperti sesi terminal atau login ke mesin jarak jauh. Terakhir, rute dapat sangat dinamis, ditetapkan ulang untuk setiap paket untuk menunjukkan beban jaringan saat ini.

Transport layer berfungsi secara utama untuk menerima data dari atas, membaginya menjadi unit yang lebih kecil jika perlu, meneruskannya ke lapisan jaringan, dan memastikan bahwa semua bagian sampai dengan benar di ujung lainnya. Selain itu, semua tindakan ini harus dilakukan dengan cara yang efektif dan menghindari lapisan atas dari perubahan yang tak terelakkan dalam teknologi perangkat keras.

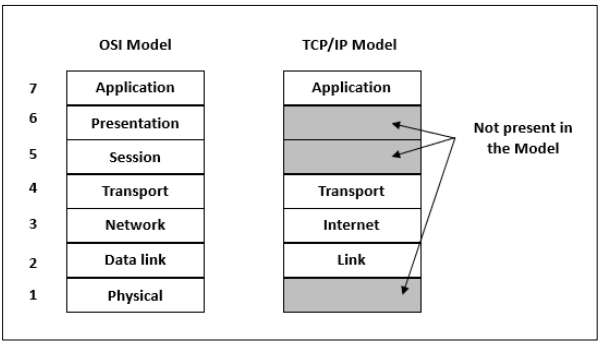
Session layer memungkinkan pengguna pada mesin yang berbeda untuk membuat sesi satu sama lain. Sesi memberikan banyak layanan, seperti kontrol dialog (melacak siapa yang akan mentransmisikan), manajemen token (mencegah dua pihak melakukan operasi penting yang sama secara bersamaan), dan sinkronisasi titik pemeriksaan transmisi panjang (memungkinkan mereka melanjutkan dari tempat mereka berhenti jika terjadi kerusakan dan pemulihan berikutnya).

Presentation layer menangani semantik dan sintaksis informasi yang dikirimkan. Ini berbeda dengan lapisan bawah, yang sebagian besar berurusan dengan pemindahan bit. Layar ini mengelola struktur data abstrak ini dan memungkinkan definisi dan pertukaran struktur data tingkat tinggi. Selain itu, struktur data yang akan dipertukarkan dapat didefinisikan secara abstrak, sehingga komputer dengan berbagai representasi data internal dapat berkomunikasi satu sama lain.

Application layer mencakup berbagai protokol yang biasanya digunakan oleh pengguna. HTTP (HyperText Transfer Protocol), yang merupakan dasar World Wide Web, digunakan oleh banyak aplikasi. Ketika browser mencari halaman web, browser mengirimkan nama halaman tersebut ke server yang menghosting halaman tersebut melalui HTTP, dan server kemudian mengirimkan kembali halaman tersebut. Transfer file, surat elektronik, dan berita jaringan dilakukan melalui protokol aplikasi tambahan.

C. MODEL REFERENSI TCP/IP

Sekarang kita beralih dari model referensi Open Systems Interconnection (OSI) ke model referensi yang digunakan oleh ARPANET, induk semua jaringan komputer area luas, dan Internet, sebagai penggantinya. ARPANET adalah jaringan penelitian yang didukung oleh Departemen Pertahanan Amerika Serikat. Jaringan ini menghubungkan ratusan universitas dan fasilitas pemerintah melalui saluran telepon sewaan. Ketika jaringan radio dan satelit ditambahkan, protokol yang ada mengalami masalah untuk bekerja sama satu sama lain. Akibatnya, arsitektur referensi baru diperlukan. Berdasarkan dua protokol utama, arsitektur ini kemudian dikenal sebagai Model Referensi TCP/IP. Dalam komunitas Internet, model ini ditetapkan sebagai standar pada tahun 1974 oleh Cerf dan Kahn (Braden, 1989). Model TCP/IP terdiri dari empat layer, seperti yang dijelaskan pada Gambar 2.2.



Gambar 2.2 Model Referensi TCP/IP (Sumber: Tanembaum & Wetherall 2011)

Link layer menjelaskan apa yang harus dilakukan tautan, seperti saluran serial dan Ethernet klasik, untuk memenuhi kebutuhan lapisan internet tanpa koneksi. Ini sebenarnya antarmuka antara host dan tautan transmisi, bukan layer. Materi awal tentang model TCP/IP tidak membahasnya secara menyeluruh.

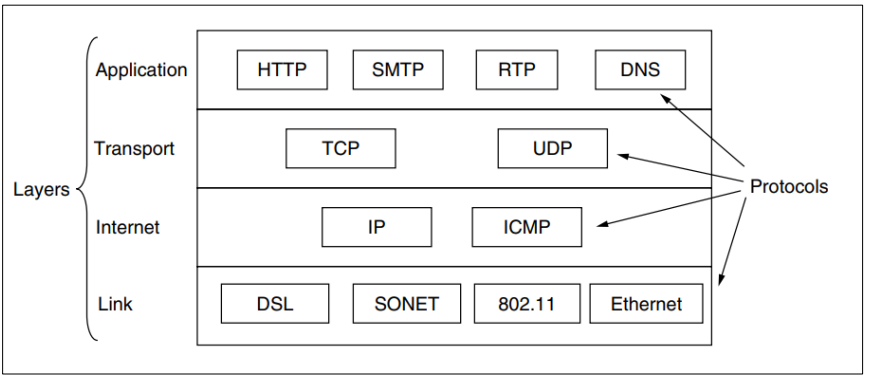
Seluruh arsitektur terhubung melalui lapisan internet. Gambar 3.2 menunjukkan lapisan ini, yang hampir mirip dengan lapisan jaringan OSI. Internet layer mengizinkan host untuk menyuntikkan paket ke jaringan mana pun dan menjadi tugasnya untuk mengirimkan paket secara mandiri. Paket tersebut mungkin tiba dalam urutan yang sama sekali berbeda dari saat dikirim. Meskipun lapisan ini terletak di Internet, namun istilah "internet" di sini digunakan dalam pengertian umum.

Protokol IP (Internet Protocol) dan format paket resminya didefinisikan oleh lapisan internet. Protokol pendamping, ICMP (Internet Control Message Protocol), membantu fungsinya. Lapisan internet bertanggung jawab untuk mengirimkan paket IP ke lokasi yang dimaksud. Seperti halnya kemacetan, perutean paket jelas merupakan masalah utama di model ini.

Dalam model TCP/IP, lapisan transportasi berada di atas lapisan Internet. Ini memungkinkan entitas terkait untuk terhubung ke host sumber dan tujuan dan melakukan percakapan. Dua protokol transportasi ujung ke ujung telah ditetapkan di sini. Yang pertama, Transmission Control Protocol atau TCP, adalah protokol

berorientasi koneksi yang kuat yang memungkinkan aliran byte dari satu mesin ke mesin lain mana pun di Internet dengan aman. Ia membagi aliran byte yang masuk menjadi pesan terpisah dan mengirimkannya ke lapisan internet. Tujuan proses TCP adalah untuk menyusun kembali pesan yang diterima penerima menjadi aliran output. Selain itu, TCP menangani kontrol aliran untuk memastikan pengirim yang cepat tidak dapat membanjiri penerima yang lambat dengan lebih banyak pesan daripada yang dapat mereka tangani. Protokol kedua di lapisan ini adalah User Datagram Protocol (UDP).

Model TCP/IP rinci dengan protokolnya seperti yang diilustrasikan pada Gambar 2.3.



Gambar 2.3 Protokol pada Model Referensi TCP/IP (Sumber: Tanembaum & Wetherall 2011)

D. PERBANDINGAN MODEL OSI DAN TCP/IP

Berikut adalah uraian rinci mengenai Perbandingan antara Model Referensi OSI dan TCP/IP, lengkap dengan keunggulan dan kelemahan masing-masing:

Model OSI dan TCP/IP merupakan dua pendekatan berbeda dalam menggambarkan proses komunikasi data di jaringan komputer. Keduanya memiliki struktur dan filosofi pengembangan yang unik. Perbandingan keduanya penting untuk dipahami agar dapat memilih pendekatan yang tepat dalam desain, analisis, dan implementasi jaringan.

Tabel 2.1 Perbandingan Model Referensi OSI dan TCP/IP

Aspek	Model OSI	Model TCP/IP
Jumlah Lapisan	7 lapisan	4 lapisan
Pengembangan	Dikembangkan oleh ISO	Dikembangkan oleh DARPA (AS) untuk Internet
Tipe Model	Model konseptual	Model implementatif
Nama Lapisan	Application, Presentation, Session, Transport, Network, Data Link, Physical	Application, Transport, Internet, Network Access
Pendekatan	Teoritis dan edukatif	Praktis dan

Aspek	Model OSI	Model TCP/IP
		berdasarkan protokol nyata
Standarisasi Protokol	Terpisah antara model dan protokol	Model dan protokol dikembangkan bersamaan
Dukungan pada Protokol	Tidak terikat pada protokol tertentu	Menggunakan protokol nyata seperti TCP, IP
Kesesuaian Dunia Nyata	Kurang diterapkan secara langsung	Digunakan luas di Internet
Kejelasan Lapisan	Setiap lapisan punya fungsi yang jelas	Beberapa fungsi digabung dalam satu lapisan

Berikut merupakan penjelasan Keunggulan dan Kelemahan masing-masing model.

1. *Model OSI*

   Keunggulan:

   a. Struktur Modular**:** Memiliki pembagian fungsi yang jelas antar lapisan, memudahkan dalam belajar dan memahami sistem jaringan.

b. Fleksibel untuk Pengembangan: Karena tidak bergantung pada protokol tertentu, cocok untuk pengembangan dan riset.
c. Dokumentasi Lengkap: Standar yang sangat lengkap dan terstruktur.

Kelemahan:

a. Kurang Relevan di Dunia Praktik: Banyak protokol modern tidak secara ketat mengikuti struktur OSI.
b. Terlalu Kompleks: Tujuh lapisan sering dianggap berlebihan untuk kebutuhan implementasi praktis.
c. Perlambatan Implementasi: Tidak secepat TCP/IP dalam adopsi teknologi jaringan global.

2. Model TCP/IP

Keunggulan:

a. Digunakan Secara Luas: Merupakan dasar komunikasi Internet dan protokol dunia nyata.
b. Efisien dan Ringkas: Hanya memiliki 4 lapisan dengan fungsi nyata yang disesuaikan dengan kebutuhan jaringan.
c. Interoperabilitas Tinggi: Protokol seperti IP, TCP, UDP terbukti sangat interoperatif antar perangkat dan vendor.

Kelemahan:

a. Tidak Terstruktur Secara Konseptual: Kurang cocok untuk pembelajaran mendalam karena fungsinya tidak sejelas OSI.

b. Gabungan Fungsi: Beberapa fungsi seperti presentasi dan sesi tidak ditangani secara eksplisit.
c. Kurangnya Pemisahan Abstraksi: Pemisahan tanggung jawab tiap lapisan tidak sejelas model OSI.

E. REKOMENDASI DAN PENERAPAN MODEL

Model OSI ideal digunakan sebagai kerangka pembelajaran dan dokumentasi, sedangkan model TCP/IP digunakan secara realistis dalam pembangunan dan pengoperasian jaringan modern.

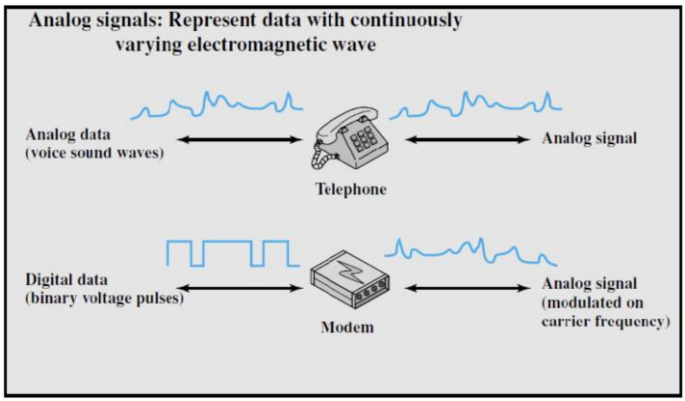
Keduanya tidak saling menggantikan, melainkan saling melengkapi:

1. Mahasiswa dan profesional jaringan belajar dari OSI untuk memahami konsep.
2. Implementasi sistem dan troubleshooting sehari-hari dilakukan menggunakan TCP/IP.

BAGIAN 3
MEDIA TRANSMISI JARINGAN

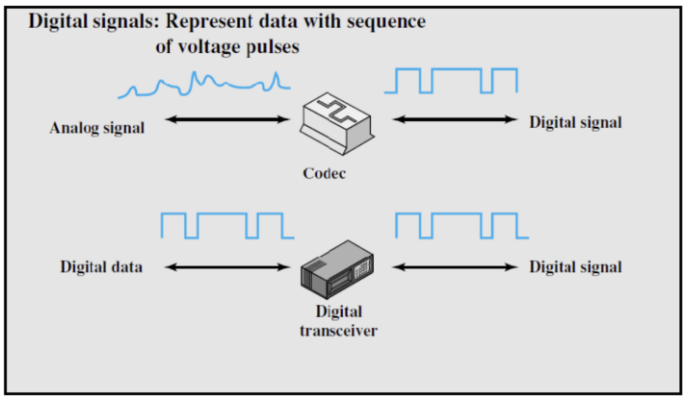
A. TRANSMISI ANALOG DAN DIGITAL

Transmisi merujuk pada proses komunikasi data yang melibatkan penyebaran dan pemrosesan sinyal (Wibowo, 2023). Dalam konteks transmisi analog, usaha ini bertujuan untuk mentransmisikan sinyal-sinyal analog tanpa memperhatikan informasi yang terkandung di dalamnya. Sinyal ini dapat berupa data analog, seperti suara, atau data digital, seperti data biner yang melewati modem.



Gambar 3.1 Representasi Data Sinyal Analog

Pada transmisi digital lebih berfokus pada pengiriman data yang terkait dengan muatan sinyal, dan dapat dilakukan dalam jarak tertentu sebelum mengalami atenuasi, derau, atau gangguan lainnya yang dapat mengancam integritas data.



Gambar 3.2 Representasi Data Sinyal Analog

Untuk mencapai jarak transmisi yang lebih jauh, digunakan perangkat repeater. Repeater berfungsi untuk menerima sinyal digital, memulihkan pola 1 dan 0, dan kemudian mentransmisikan kembali sinyal yang telah diperbarui, sehingga mengatasi masalah atenuasi yang terjadi selama transmisi.

B. MODE TRANSMISI DALAM SISTEM KOMUNIKASI DATA

Transmisi data adalah proses penting dalam sistem komunikasi yang mencakup berbagai metode pengiriman data dari pengirim ke penerima (Agustini, 2021). Secara umum, mode transmisi dapat dibagi menjadi dua kategori utama berdasarkan cara pengiriman data, yakni transmisi serial dan paralel. Kedua mode ini memiliki karakteristik yang berbeda dalam hal kecepatan, efisiensi, dan aplikasi penggunaannya.

1. Mode Transmisi Serial

Pada mode transmisi serial, data yang dikirimkan melalui saluran komunikasi dikirimkan secara berurutan, bit demi bit, satu per satu. Data paralel internal yang ada di perangkat pengirim diubah menjadi format serial menggunakan perangkat pengubah paralel-serial (IC Converter). Karena pengiriman bit dilakukan satu per satu, kecepatan pemindahan data lebih rendah dibandingkan dengan transmisi paralel. Transmisi dimulai dengan pengiriman bit yang paling tidak signifikan (Least Significant Bit / LSB) dan diakhiri dengan bit yang paling signifikan (Most Significant Bit / MSB). Penerima harus dapat memecahkan isyarat data dengan tepat pada waktu yang benar agar data dapat dibentuk kembali menjadi karakter yang diterima secara akurat. Agar proses ini berhasil, pengirim dan penerima harus disinkronisasi dengan menggunakan detak waktu atau time pulse, yang memastikan kedua pihak beroperasi pada waktu yang serupa.

2. Mode Transmisi Paralel

Berbeda dengan mode serial, pada transmisi paralel, data dikirimkan secara simultan, misalnya, 8 bit secara bersamaan. Mode ini memungkinkan kecepatan transmisi yang lebih tinggi, namun hanya efektif jika karakteristik media transmisi mendukungnya. Salah satu tantangan utama pada transmisi paralel adalah terjadinya efek "skew", yakni ketidaksesuaian waktu kedatangan bit-bit pada penerima, yang dapat

menyebabkan kesalahan dalam pengiriman data. Oleh karena itu, media transmisi harus sangat berkualitas dan memiliki kapasitas untuk menangani beberapa bit sekaligus dengan akurat.

C. JENIS-JENIS MODE TRANSMISI SERIAL BERDASARKAN SINKRONISASI

Berdasarkan sinkronisasi yang digunakan, transmisi serial terbagi menjadi tiga jenis utama, yakni asinkron, sinkron, dan isokron (Setiawan dkk., 2024).

1. Asinkron

Pada transmisi asinkron, pengiriman data dilakukan per karakter, dan tidak ada waktu yang tetap antara pengiriman karakter satu dengan lainnya. Transmisi ini membutuhkan *start pulse* untuk menandakan dimulainya pengiriman data dan diakhiri dengan *stop bit* setelah setiap karakter. Jika terjadi kesalahan dalam transmisi, maka satu blok data bisa hilang. Meskipun transmisi ini dapat dilakukan dengan kecepatan tinggi, penggunaannya terbatas karena kurangnya sinkronisasi antar karakter.

2. Sinkron

Pada transmisi sinkron, pengiriman dilakukan per blok data. Transmisi ini lebih efisien karena tidak memerlukan bit awal atau bit akhir seperti pada mode asinkron. Ketika terjadi

kesalahan, satu blok data akan hilang, tetapi saluran komunikasi dapat digunakan secara lebih efektif, karena transmisi dilakukan hanya ketika terdapat sejumlah blok data yang siap dikirimkan.

3. Isokron

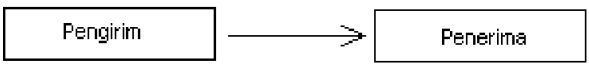
Mode isokron menggabungkan elemen dari mode asinkron dan sinkron. Dalam mode ini, setiap karakter data didahului dengan bit awal dan diakhiri dengan bit akhir, memberikan keandalan yang lebih tinggi dalam transmisi dibandingkan dengan mode asinkron.

D. METODE TRANSMISI

Metode transmisi merujuk pada cara pengiriman data dalam saluran komunikasi. Terdapat tiga metode utama, yaitu simplex, half duplex (HDX), dan full duplex (FDX) (Abdullah, 2015).

1. Simplex

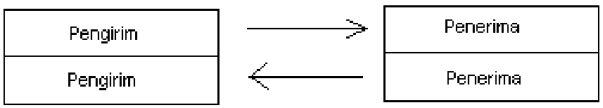
Pada mode simplex, data hanya dikirimkan dalam satu arah saja. Pemancar dan penerima memiliki tugas yang tetap, dengan pemancar hanya mengirimkan data dan penerima hanya menerima data. Mode ini jarang digunakan untuk sistem komunikasi data karena terbatasnya arah pengiriman.



Gambar 3.3 Ilustrasi Metode Simplex

2. Half Duplex (HDX)

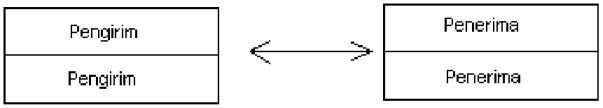
Dalam mode half duplex, data dapat dikirimkan kedua arah, namun tidak bersamaan. Data dikirimkan secara bergantian antara pengirim dan penerima, dan terdapat waktu untuk mengubah arah transmisi, yang dikenal dengan turnaround time.



Gambar 3.4 Ilustrasi Metode Half Duplex

3. Full Duplex (FDX)

Mode full duplex memungkinkan pengiriman dan penerimaan data secara bersamaan. Keuntungan utama dari mode ini adalah efisiensi yang lebih tinggi, karena transmisi data dapat terjadi secara simultan di kedua arah tanpa harus menunggu giliran.



Gambar 3.5 Ilustrasi Metode Full Duplex

E. KARAKTERISTIK TRANSMISI

Transmisi data menggunakan dua jenis arus utama, yakni arus searah (DC) dan arus bolak-balik (AC) (Pujowati & Harianto, 2021).

1. DC (Direct Current)

   Arus DC jarang digunakan dalam sistem transmisi data modern, kecuali untuk aplikasi jarak dekat dan kecepatan rendah, biasanya di bawah 300 bps.

2. AC (Alternating Current)

   Sebaliknya, arus AC lebih sering digunakan dalam transmisi data, terutama untuk jarak jauh dan kecepatan tinggi. Teknologi ini mendukung transmisi data pada kecepatan yang lebih tinggi.

F. KECEPATAN TRANSMISI

Kecepatan transmisi data diukur dalam satuan seperti karakter per detik (kps) atau bit per detik (bps). Kecepatan transmisi dipengaruhi oleh lebar frekuensi (bandwidth) saluran komunikasi (Syafrizal & Yogyakarta, 2020). Beberapa variasi umum kecepatan transmisi meliputi 110, 300, 600, 1200, 2400, 4800, dan 9600 bps. Saluran komunikasi juga dapat digolongkan berdasarkan bandwidth-nya:

1. **Broadband Channel:** Saluran ini digunakan untuk sinyal berfrekuensi tinggi, seperti pada gelombang mikro, kabel koaksial, dan serat optik.
2. **Voice Grade Channel:** Saluran ini digunakan untuk transmisi dial-up atau saluran pribadi dengan frekuensi 300 hingga 3000 Hz.
3. **Subvoice Channel:** Saluran ini digunakan untuk transmisi dengan kecepatan rendah, biasanya di bawah 600 bps.

4. **Telegraph Channel:** Saluran ini digunakan untuk transmisi dengan kecepatan sangat rendah, yaitu 45 hingga 75 bps.

Tabel 3.1 Tabel Spektrum Elektromagnetik

Frequency Band	Name
3 - 10 kHz	Extremely Low Frequency (ELF)
10 - 30 kHz	Very Low Frequency (VLF)
30 - 300 kHz	Low Frequency (LF)
300 - 3000 kHz	Medium Frequency (MF)
3 - 30 MHz	High Frequnecy (HF) (also called "short wave")
30 - 300 MHz	Very High Frequency (VHF)
300 - 3000 MHz	Ultra High Frequency (UHF) (also called "microwaves")
3 - 30 GHz	Super High Frequency (SHF)

G. MULTIPLEXING

Multiplexing adalah teknik untuk meningkatkan efisiensi penggunaan media komunikasi, dengan memungkinkan beberapa transmisi data untuk berbagi saluran transmisi yang sama (Irawati dkk., 2018). Teknologi multiplexing dapat dilakukan dengan menggunakan perangkat seperti multiplexer (MUX) dan demultiplexer (DEMUX). Tiga teknik utama multiplexing yang digunakan dalam komunikasi data adalah:

1. Time Division Multiplexing (TDM)

   Teknik ini memberikan alokasi waktu pada setiap transmisi untuk mengirimkan data secara bergiliran. TDM sering

digunakan ketika kapasitas transmisi melebihi kapasitas medium komunikasi, seperti pada saluran baseband.

2. Frequency Division Multiplexing (FDM)

   FDM membagi saluran komunikasi menjadi beberapa sub-saluran frekuensi, dengan masing-masing transmisi menggunakan frekuensi yang berbeda. Teknik ini digunakan pada saluran broadband dan memungkinkan berbagai jenis data, seperti suara, video, dan data, untuk dikirimkan bersama dalam satu kabel.

3. Code Division Multiplexing (CDM)

   Teknik CDM memungkinkan beberapa transmisi menggunakan kode yang berbeda untuk berkomunikasi dalam waktu yang bersamaan. Teknik ini memungkinkan penggunaan bandwidth secara lebih efisien, seperti yang digunakan dalam sistem komunikasi seluler.

H. FUNGSI MEDIA TRANSMISI

Media transmisi merujuk pada saluran yang menghubungkan pengirim dan penerima dalam proses pertukaran informasi atau data (Arius, 2020). Dalam konteks komunikasi data, media transmisi memainkan peran krusial dalam mengantarkan sinyal dari satu titik ke titik lainnya, baik dalam bentuk gelombang elektromagnetik maupun melalui saluran fisik. Pemilihan media

transmisi yang tepat sangat mempengaruhi efisiensi dan keandalan sistem komunikasi.

Media transmisi digunakan untuk menghubungkan berbagai perangkat elektronik yang memungkinkan pertukaran data. Berbagai alat elektronik seperti telepon, komputer, televisi, dan radio memanfaatkan media transmisi untuk menerima dan mengirim data. Sebagai contoh, dalam sistem telekomunikasi, kabel merupakan media transmisi yang menghubungkan dua perangkat telepon untuk memungkinkan percakapan. Setiap perangkat elektronik memiliki jenis media transmisi yang berbeda sesuai dengan kebutuhan pengiriman data yang diperlukan.

I. KARAKTERISTIK MEDIA TRANSMISI

Karakteristik media transmisi bergantung pada sejumlah faktor, yang meliputi jenis alat elektronik yang digunakan, jenis data yang dikirimkan, tingkat efektivitas pengiriman data, serta ukuran data yang ditransmisikan (Ryan, 2018). Faktor-faktor lain yang mempengaruhi performa media transmisi mencakup:

1. **Bandwidth:** Bandwidth yang lebih besar memungkinkan pengiriman data dengan kapasitas lebih besar.
2. **Ketahanan terhadap gangguan:** Kemampuan media transmisi untuk mengatasi gangguan elektromagnetik dan magnetis yang berasal dari lingkungan sekitar sangat penting.

3. **Kemampuan melayani akses banyak (multiple access):** Media transmisi harus memungkinkan pengambilan data oleh banyak pengguna secara efisien.
4. **Keamanan data:** Aspek ini berkaitan dengan sejauh mana data yang dikirim dapat terlindungi dari gangguan atau penyadapan.

J. JENIS-JENIS MEDIA TRANSMISI

Media transmisi dapat dibagi menjadi dua kategori utama, yaitu media transmisi terpandu (guided) dan media transmisi tidak terpandu (unguided) (Purbawanto, 2021). Berikut adalah penjelasan lebih lanjut mengenai kedua jenis media tersebut:

1. Media Transmisi Terpandu (Guided Transmission Media)

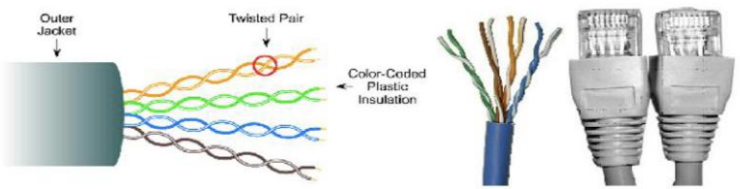
Media transmisi terpandu adalah media yang secara fisik memandu gelombang elektromagnetik menuju tujuan tertentu. Beberapa jenis kabel yang termasuk dalam kategori ini adalah sebagai berikut:

a. Kabel Twisted Pair

Kabel twisted pair adalah jenis kabel yang paling sederhana dan terjangkau, sering digunakan dalam jaringan komputer. Kabel ini terdiri dari dua kawat tembaga yang dipilin bersama, dengan pola spiral. Ada dua jenis utama kabel twisted pair, yaitu:

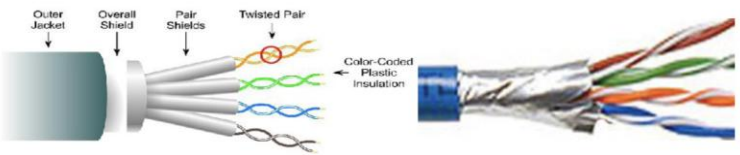
1) Unshielded Twisted Pair (UTP): Tidak dilengkapi pelindung, sering digunakan untuk jaringan lokal (LAN).

Keuntungannya adalah pemasangan yang mudah dan biaya rendah, namun rentan terhadap interferensi elektromagnetik.



Gambar 3.6 Ilustrasi Unshielded Twisted Pair

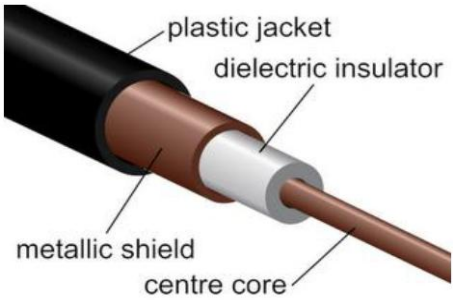
2) Shielded Twisted Pair (STP): Dilengkapi dengan pelindung untuk mengurangi gangguan elektromagnetik. Kabel ini lebih tahan terhadap interferensi, namun lebih mahal dan lebih sulit dipasang.



Gambar 3.7 Ilustrasi Shielded Twisted Pair

b. Kabel Koaksial

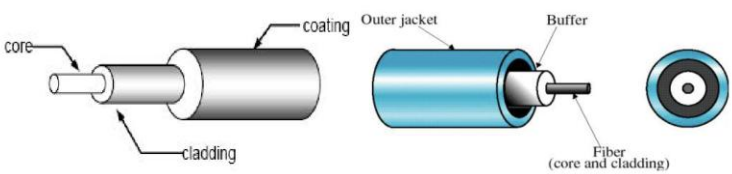
Kabel koaksial terdiri dari dua konduktor, satu di tengah (inti) dan satu di sekelilingnya (pelindung). Kabel ini digunakan untuk transmisi frekuensi tinggi dan sering digunakan pada sistem televisi, telekomunikasi jarak jauh, dan LAN. Keuntungan utama kabel koaksial adalah kemampuannya untuk mentransfer data pada kecepatan tinggi dan jarak jauh, namun pemasangannya lebih sulit dan mudah disadap.



Gambar 3.8 Ilustrasi Kabel Koaksial

c. Kabel Serat Optik

Kabel serat optik terbuat dari bahan dielektrik seperti kaca atau plastik yang mampu menyalurkan data dengan kecepatan sangat tinggi, bahkan dalam urutan gigabit per detik (Gb/s). Sinyal yang ditransmisikan dalam kabel serat optik berbentuk cahaya. Keunggulan dari kabel serat optik adalah bandwidth yang sangat lebar, redaman yang rendah, dan ketahanan terhadap interferensi elektromagnetik. Namun, instalasi kabel serat optik membutuhkan peralatan khusus dan kabelnya rentan terhadap tekanan fisik yang berlebihan.



Gambar 3.9 Ilustrasi Kabel Serat Optik

2. Media Transmisi Tidak Terpandu (Unguided Transmission Media)

Media transmisi tidak terpandu tidak memerlukan saluran fisik untuk mentransmisikan data. Sinyal data dapat bergerak melalui udara atau ruang bebas, menggunakan gelombang elektromagnetik. Beberapa jenis media transmisi tidak terpandu meliputi:

a. Antena

Antena digunakan untuk radiasi elektromagnetik dan penerimaan sinyal. Terdapat dua jenis antena utama:

1) Antena transmisi: Mengubah energi radio menjadi gelombang elektromagnetik untuk disiarkan.
2) Antena penerima: Menangkap gelombang elektromagnetik dan mengubahnya kembali menjadi sinyal listrik.

b. Gelombang Mikro

Gelombang mikro merupakan bentuk gelombang radio yang menggunakan frekuensi tinggi (dalam gigahertz). Gelombang mikro banyak digunakan dalam sistem komunikasi jarak menengah (MAN), layanan internet, dan sistem komunikasi nirkabel. Keuntungan penggunaan gelombang mikro adalah kemampuannya untuk membawa data dalam jumlah besar dengan biaya yang lebih rendah dibandingkan dengan sistem kabel, serta fleksibilitas karena tidak memerlukan tanah yang luas untuk menempatkan

menara antena. Namun, gelombang mikro rentan terhadap gangguan cuaca dan interferensi pesawat terbang.

c. Satelit

Satelit geostasioner berfungsi untuk menerima dan meneruskan sinyal antar stasiun bumi. Keuntungan penggunaan satelit adalah biaya yang lebih rendah dibandingkan pemasangan kabel antar benua, serta kemampuan untuk menjangkau wilayah terpencil dengan populasi rendah. Namun, penggunaan satelit juga menghadapi tantangan seperti keterbatasan teknologi antena besar dan biaya tinggi untuk peluncuran dan pemeliharaan satelit.

d. Gelombang Radio

Gelombang radio digunakan dalam berbagai aplikasi komunikasi, seperti radio FM dan televisi. Keuntungan utama gelombang radio adalah kemampuannya untuk mentransmisikan sinyal tanpa harus dalam jalur lurus, memungkinkan transmisi melalui berbagai rintangan. Namun, transmisi gelombang radio dapat terganggu oleh interferensi dari sumber eksternal.

e. Inframerah

Gelombang inframerah adalah radiasi elektromagnetik dengan panjang gelombang lebih panjang daripada cahaya tampak namun lebih pendek dari gelombang radio.

Komunikasi inframerah digunakan dalam aplikasi seperti remote control dan komunikasi data jarak dekat antara perangkat seperti telepon genggam dan komputer.

BAGIAN 4
PERANGKAT JARINGAN KOMPUTER

A. PENDAHULUAN

Perangkat jaringan komputer adalah sekumpulan perangkat keras, perangkat lunak, dan infrastruktur yang bekerja bersama untuk memungkinkan komunikasi data antara perangkat dalam suatu jaringan. Jaringan komputer sendiri merupakan kumpulan perangkat komputer yang terhubung satu sama lain untuk berbagi informasi, data, atau protokol komunikasi. Dengan adanya jaringan, perangkat dapat saling bertukar data dan informasi secara efisien

B. JENIS – JENIS PERANGKAT JARINGAN KOMPUTER

1. Network Adapter Card (Wired dan Wireless)

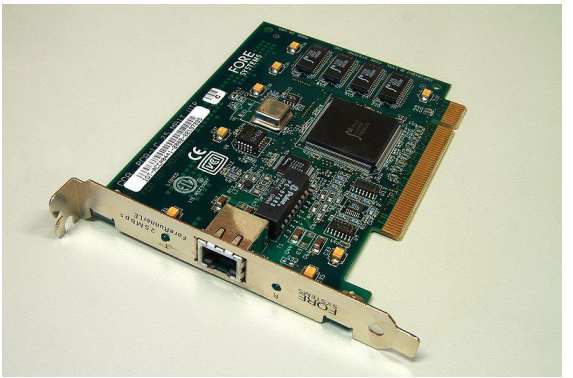
Agar dapat terhubung ke jaringan komputer, sebuah komputer harus dilengkapi dengan perangkat yang dikenal sebagai kartu jaringan atau *network adapter*, atau juga disebut sebagai *network interface card* (NIC). Perangkat ini memungkinkan komputer untuk terhubung dengan jaringan eksternal dan berkomunikasi dengan perangkat jaringan lainnya. Dan berikut jenis-jenis *network adapter card* :

a. Kartu Jaringan Untuk Kabel (Wired Network Card)

Kartu jaringan untuk kabel, atau *wired network card*, adalah perangkat keras tambahan yang digunakan untuk menghubungkan komputer atau perangkat lain ke jaringan kabel (LAN) melalui *port Ethernet*, Terdapat dua jenis kartu jaringan untuk kabel yaitu kartu jaringan internal yang terpasang langsung di *motherboard* maupun dalam bentuk kartu tambahan yang terpasang di *slot PCI* seperti ditunjukan pada gambar 4.1.

Selain kartu jaringan yang terpasang secara internal, tersedia juga pilihan kartu jaringan eksternal yang dapat digunakan untuk menghubungkan komputer ke jaringan. Salah satu perangkat jaringan external yang dapat digunakan adalah melalui *port USB*, atau yang kita kenal dengan *USB to Ethernet Network Adapter* seperti ditunjukan pada gambar 5.2, yang memungkinkan perangkat ini untuk dipasang dan dilepas dengan mudah sesuai kebutuhan. Kartu jaringan eksternal ini menjadi solusi praktis bagi komputer yang tidak memiliki kartu jaringan bawaan atau bagi pengguna yang ingin menambahkan koneksi tambahan tanpa perlu membuka casing komputer. Sebelum digunakan, kartu jaringan eksternal umumnya memerlukan instalasi perangkat lunak atau *driver*, meskipun banyak di antaranya yang mendukung fitur *plug-and-play*, sehingga dapat langsung dikenali oleh sistem operasi dan digunakan. Selain memiliki

kemudahan dalam pemasangan, perangkat ini juga menawarkan fleksibilitas dalam pemakaian, karena dapat digunakan pada berbagai perangkat, baik komputer *desktop* maupun laptop, tanpa memerlukan instalasi dan konfigurasi tambahan.



Gambar 4.1 Kartu Jaringan Internal Untuk Kabel

Gambar 4.2 *USB to Ethernet Network Adapter*

b. Kartu Jaringan Untuk Nirkabel (Wireless Network Cards)

Wireless network card, atau sering disebut kartu jaringan nirkabel, adalah perangkat keras yang memungkinkan komputer atau perangkat lain terhubung ke jaringan tanpa menggunakan kabel, dengan memanfaatkan gelombang radio. Kartu jaringan ini digunakan untuk mengakses jaringan Wi-Fi, yang termasuk dalam teknologi jaringan lokal nirkabel (Wireless Local Area Network / WLAN). Perangkat ini tidak memerlukan kabel jaringan untuk menghubungkan ke perangkat jaringan lainnya, sehingga memberikan fleksibilitas dalam instalasi jaringan maupun penggunaannya. Seperti hal nya pada kartu jaringan untuk kabel, pada kartu jaringan jenis ini juga memiliki dua jenis yaitu kartu jaringan internal dan external. Untuk jenis kartu jaringan nirkabel internal biasanya sudah terintegrasi pada *motherboard* seperti contoh pada perangkat laptop seperti ditunjukan pada gambar 5.3, sehingga memungkinkan pengguna untuk mengakses koneksi jaringan dimanapun dan kapanpun, selama terdapat sinyal jaringan nirkabel di sekitar.

Gambar 4.3 Kartu Jaringan Nirkabel Internal Untuk Laptop

Gambar 4.4 Kartu Jaringan Nirkabel Internal Untuk PC

2. HUB

HUB adalah perangkat jaringan yang berfungsi untuk menghubungkan beberapa komputer dalam satu jaringan lokal (LAN), bekerja pada layer 1 (*Physical Layer*) dari model OSI. HUB dikenal sebagai perangkat *non-inteligent* karena tidak dapat menentukan tujuan data yang dikirim, sehingga semua data yang masuk akan diteruskan ke semua *port* yang tersedia, tanpa memperdulikan siapa penerima sebenarnya (Crystal Panek, 2020). Terdapat dua jenis HUB yaitu *active* dan *passive* HUB (Ambedkar, 2015), berikut penjelasan dari kedua perangkat tersebut :

a. ***Active* Hub** : Jenis ini lebih canggih dibandingkan *passive* hub. Selain menjadi jalur pengiriman data, *active* hub juga memiliki kemampuan untuk memperkuat, mengonsentrasikan, dan meregenerasi sinyal sebelum diteruskan ke tujuan. Karena kemampuannya ini, *active* hub juga dikenal sebagai *repeater*.

b. *Passive* Hub : Jenis ini hanya berfungsi sebagai titik sambungan fisik antar kabel dalam jaringan. *Passive* hub tidak memiliki kemampuan untuk memperbaiki atau memodifikasi sinyal yang dilewatkannya.

Gambar 4.5 HUB

3. SWITCH

Switch merupakan perangkat jaringan yang beroperasi pada lapisan kedua dalam model referensi OSI, yaitu *Data Link Layer*. Meskipun secara fungsi dasar menyerupai hub, *switch* memiliki kemampuan untuk mengenali dan memproses *Media Access Control* (MAC) *Address* guna mengidentifikasi dan memfilter data yang akan diteruskan ke tujuan yang tepat (Mutoffar et al., 2024). Perangkat ini menyimpan tabel yang memetakan alamat MAC dengan *port* pada *switch*, sehingga dapat menentukan arah pengiriman paket secara selektif, yang pada akhirnya dapat mengurangi beban lalu lintas data di jaringan. Selain itu, *switch* mendukung komunikasi *full-duplex*, di mana jalur transmisi dan penerimaan data berjalan secara terpisah. Mekanisme ini memungkinkan proses komunikasi dua arah secara simultan dan secara signifikan mengurangi kemungkinan terjadinya *colluision*

pada jaringan, meskipun potensi tersebut belum sepenuhnya dihilangkan (Madcoms, 2010).

Secara umum, *switch* dapat diklasifikasikan ke dalam dua jenis utama, yaitu *Switch Layer-2* dan *Switch Layer-3*. *Switch Layer-2* beroperasi pada lapisan *Data Link* dalam model OSI dan melakukan proses pengalihan data berdasarkan alamat MAC. Jenis *switch* ini umum digunakan untuk membagi jaringan lokal menjadi beberapa segmen yang lebih kecil, sehingga dapat meningkatkan efisiensi lalu lintas data dalam jaringan. Sementara itu, *Switch Layer-3* bekerja pada lapisan *network* dan menggunakan alamat IP untuk menentukan jalur pengiriman paket. *Switch* jenis ini memiliki kemampuan *routing* yang memungkinkan menghubungkan antar jaringan yang berbeda (*internetworking*), dan oleh karena itu sering disebut sebagai *multilayer switch* karena menggabungkan fungsi *switching* dan *routing* dalam satu perangkat (Ambedkar, 2015).

Gambar 4.5 *Switch*

4. ROUTER

Router adalah perangkat jaringan yang berfungsi untuk menghubungkan beberapa jaringan yang berbeda. *Router* bekerja pada lapisan jaringan (*Network Layer*) dalam model

referensi OSI dan bertugas meneruskan paket data dari satu jaringan ke jaringan lainnya berdasarkan alamat IP tujuan. Dengan kemampuannya menentukan jalur terbaik untuk pengiriman data, *router* dapat memastikan bahwa paket data mencapai tujuan yang tepat secara efisien (Syafrizal, 2020). *Router* memberikan beberapa manfaat penting dalam pengelolaan jaringan komputer, salah satu keuntungannya adalah kemampuannya dalam membagi jaringan menjadi beberapa segmen jaringan (segmentasi), yang berdampak pada pengurangan beban lalu lintas data. Dengan segmentasi ini, data tidak akan diteruskan ke seluruh jaringan, tetapi hanya dikirim ke jaringan yang menjadi tujuan, sehingga jaringan menjadi lebih efisien. Selain itu, *router* juga memiliki kemampuan untuk mengisolasi masalah jaringan. Jika terjadi gangguan pada salah satu segmen jaringan, *router* dapat mencegah gangguan tersebut menyebar ke seluruh jaringan. (Ahmad Yani, 2008).

Gambar 4.6 *Router*

5. ACCESS POINT

Access Point merupakan salah satu perangkat jaringan komputer yang memiliki fungsi sebagai perangkat penghubung antar perangkat di dalam jaringan *Wireless Local Area Network*

(WLAN). *Access Point* akan mengubah sinyal radio yang diterima menjadi sinyal digital yang kemudian ditransmisikan melalui perangkat WLAN lainnya. Selanjutnya, sinyal digital tersebut akan dikonversi kembali menjadi sinyal radio oleh perangkat penerima (Jumadi M.Parenreng et al., 2022). *Access Point* memiliki dua komponen utama yaitu antena dan *transceiver* dimana kedua komponen ini memiliki fungsi untuk memancarkan dan menerima sinyal jaringan dari perangkat nirkabel lainnya (Muhammad Haris et al., 2025)

Gambar 4.7 *Access Point*

6. FIREWALL

Firewall merupakan perangkat jaringan, baik berbentuk fisik maupun perangkat lunak, yang berfungsi mengatur dan membatasi lalu lintas data antar jaringan yang memiliki tingkat keamanan berbeda. Fungsinya tidak terbatas hanya pada koneksi internet, melainkan juga digunakan dalam jaringan internal organisasi, seperti membatasi akses ke bagian yang menangani data sensitif seperti keuangan atau kepegawaian. Pada arsitektur *firewall*, umumnya terdapat dua antarmuka utama yang berperan dalam pengelolaan lalu lintas jaringan,

yaitu antarmuka eksternal (*external interface*) dan antarmuka internal (*internal interface*). Antarmuka eksternal berfungsi sebagai titik koneksi ke jaringan luar atau jaringan yang tidak dipercaya (*untrusted network*), seperti internet. Sementara itu, antarmuka internal mengarah ke jaringan lokal atau *trusted network* yang mengandung aset-aset sensitif dan memerlukan tingkat perlindungan yang lebih tinggi. Kedua antarmuka ini berfungsi sebagai basis implementasi kebijakan kontrol akses dan inspeksi paket data yang diterapkan oleh *firewall* dalam menjaga integritas serta keamanan komunikasi jaringan (Scarfone & Hoffman, 2009).

Gambar 4.8 Perangkat Keras *Firewall*

7. MODEM

Modem, singkatan dari *Modulator-Demodulator*, merupakan perangkat elektronik yang berfungsi sebagai penghubung antara perangkat komputasi seperti komputer, laptop, *tablet* dan *smartphone* dengan jaringan Internet. Perangkat ini bekerja dengan mengubah (modulasi) sinyal data digital yang berasal dari perangkat komputasi menjadi sinyal analog agar dapat

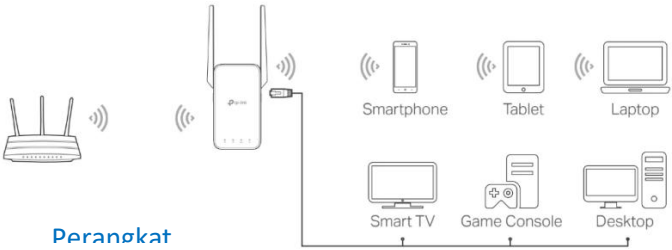
ditransmisikan melalui media komunikasi, seperti jaringan telepon atau sistem transmisi lainnya. Sebaliknya, saat sinyal analog diterima kembali, modem akan melakukan proses demodulasi untuk mengubah sinyal tersebut menjadi data digital yang dapat diproses oleh perangkat tujuan. Proses ini memungkinkan komunikasi dua arah antara pengguna dan jaringan secara efisien. Meskipun pada awalnya modem banyak digunakan pada saluran telepon konvensional, perkembangan teknologi telah memperluas penggunaannya ke berbagai media lain, seperti jaringan nirkabel (*wireless*) dan jaringan serat optik. (Wibowo et al., 2022).

Gambar 4.9 Modem

8. REPEATER

Repeater atau penguat sinyal, merupakan salah satu perangkat jaringan komputer yang berfungsi untuk menerima dan memancarkan kembali sinyal dengan daya yang telah diperkuat, sehingga memungkinkan sinyal tersebut menjangkau area yang lebih luas (Wibowo et al., 2022) seperti ditunjukan pada

gambar 5.10. Tujuan utama penggunaan *repeater* adalah untuk meningkatkan kualitas layanan komunikasi nirkabel, sehingga pengguna dapat menikmati konektivitas yang lebih stabil dan kuat. Dalam konteks jaringan Wi-Fi, *repeater* bekerja dengan dua perangkat utama: satu untuk menerima sinyal dari sumber (seperti *router* utama) dan satu lagi untuk memancarkan ulang sinyal tersebut ke area yang lebih luas. Meskipun demikian, penggunaan *repeater* di jaringan nirkabel tetap memiliki tantangan, seperti potensi interferensi antar perangkat, yang dapat mempengaruhi kualitas transmisi data (Achmad et al., 2016).



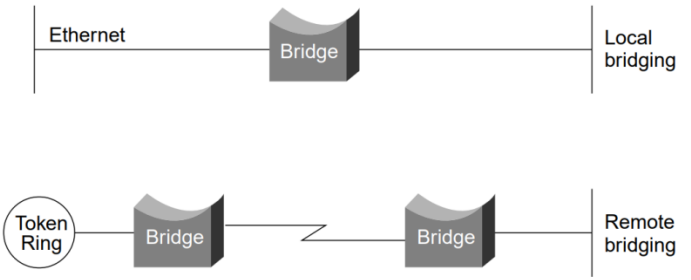
Gambar 4.10 Contoh Topologi Jaringan Menggunakan *Repeater*

Gambar 4.11 *Repeater*

9. BRIDGE

merupakan perangkat komunikasi data yang beroperasi pada lapisan *data link* (Layer 2) dalam model referensi OSI. Pada awal kemunculannya di tahun 1980-an, bridge digunakan untuk menghubungkan serta meneruskan data antar segmen jaringan lokal (LAN) yang memiliki karakteristik teknis yang sama, sebagai contoh dua segmen jaringan yang sama-sama menggunakan teknologi *Ethernet*. Seiring berkembangnya kebutuhan konektivitas dalam lingkungan jaringan yang lebih kompleks, bridge kemudian dirancang untuk menjembatani komunikasi antara jaringan yang menggunakan teknologi berbeda—contohnya, menghubungkan jaringan *Ethernet* dengan jaringan *Token Ring.*

Bridge dapat diklasifikasikan ke dalam beberapa kategori berdasarkan karakteristik dan fungsionalitas produk yang dimilikinya. Salah satu klasifikasi yang umum digunakan membagi *bridge* menjadi dua jenis utama, yaitu *local bridge* dan *remote bridge* seperti ditunjukan pada gambar 5.12. *Local bridge* digunakan untuk menghubungkan beberapa segmen LAN yang berada dalam area fisik yang berdekatan, dan biasanya tidak melibatkan media transmisi jarak jauh. Sebaliknya, *remote bridge* berfungsi untuk menghubungkan segmen-segmen LAN yang tersebar secara geografis dan dipisahkan oleh jarak yang cukup jauh, biasanya melalui saluran komunikasi seperti *leased line* atau jaringan WAN (Cisco System, 2003).

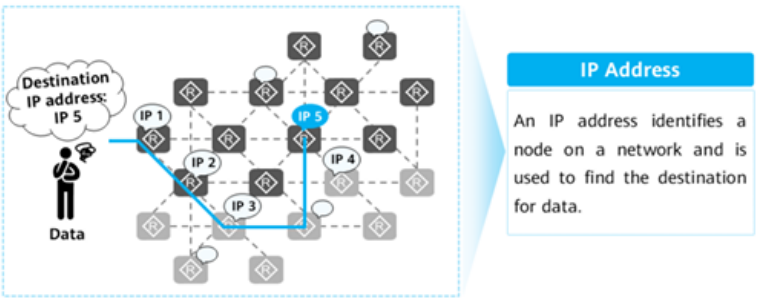


Gambar 4.12 Klasifikasi Bridge

BAGIAN 5
IP ADDRESSING dan SUBNETTING

A. IP ADDRESS

Dalam dunia jaringan komputer, IP Address (Internet Protocol Address) merupakan salah satu komponen paling penting dalam berkomunikasi. Komunikasi data antar perangkat merupakan tulang punggung dari berbagai sistem informasi dan jaringan komputer modern. IP Address berfungsi sebagai alamat identifikasi yang unik bagi setiap perangkat yang terhubung ke jaringan, baik jaringan lokal (LAN) maupun internet (Edition et al., 2011). Layaknya alamat rumah yang digunakan untuk mengirimkan surat, IP Address digunakan untuk mengirim dan menerima data antar perangkat di jaringan.



Gambar 5.1 Ilustrasi IP Address (Huawei Technologies Co, 2020)

IP Address memungkinkan perangkat untuk berkomunikasi satu sama lain, baik dalam jaringan tertutup maupun secara global melalui internet. IP Address beroperasi pada layer 3 dari model

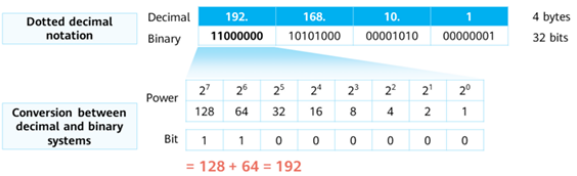
referensi OSI, yaitu Network Layer. Layer ini bertanggung jawab atas pengalamatan logis, routing antar jaringan, dan pengiriman paket dari sumber ke tujuan yang bisa jadi berada dalam jaringan berbeda. Berbeda dengan MAC address yang bersifat fisik dan tetap (beroperasi pada Data Link Layer), IP Address bersifat logis dan dapat dikonfigurasi, serta digunakan untuk pengiriman data lintas jaringan melalui perangkat seperti Router.

Terdapat dua versi IP Address yang umum digunakan saat ini, yaitu IPv4 dan IPv6 (Steinke, 2020). IPv4 menggunakan sistem bilangan biner 32-bit yang ditulis dalam format desimal (contoh : 10.0.0.1, 172.16.1.1, 192.168.1.1), sedangkan IPv6 merupakan pengembangan dari IPv4 dengan panjang 128-bit dan ditulis dalam format heksadesimal (contoh : 2001:0db8:85a3:0000:0000:8a2e:0370:7334). Melalui IPv4 dan IPv6, Network Layer membungkus data ke dalam bentuk paket IP dan menentukan jalur terbaik untuk mengirimkan paket tersebut dengan bantuan Routing Protocol seperti OSPF, BGP, atau RIP.

B. IPV4 ADDRESSING

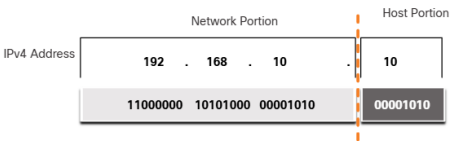
IPv4 address memiliki panjang 32 bit dan terdiri dari 4 byte. Ditulis dalam notasi desimal bertitik (dotted decimal) (Postel, 1981), yang memudahkan pembacaan dan penulisan. Format IPv4 Address dirancang untuk mempermudah manusia dalam menggunakan dan mengkonfigurasi jaringan komputer. Oleh karena itu, alamat IP

dituliskan dalam notasi desimal bertitik (dotted decimal) yang terdiri dari empat angka desimal, masing-masing berkisar dari 0 hingga 255 (contoh : 192.168.10.1). Namun, perangkat komunikasi dalam jaringan tidak membaca angka-angka ini sebagai desimal, melainkan memprosesnya dalam bentuk biner, karena komputer hanya memahami bit 1 dan 0. Untuk memahami bagaimana perangkat jaringan seperti router, switch, dan komputer melakukan proses pengalamatan, konversi antara desimal dan biner sangatlah penting. Hal ini menjadi dasar dalam menentukan bagian jaringan (Network Portion) dan bagian Host (Host Portion) berdasarkan subnet mask.



Gambar 5.2 Notasi dan Konversi IPv4 Address (Huawei Technologies Co., Ltd., 2023)

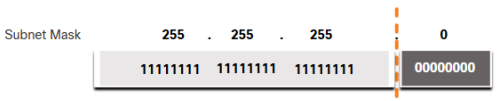
Struktur IPv4 address terdiri dari dua bagian yaitu bagian jaringan (Network Portion) dan bagian Host (Host Portion) seperti terlihat pada gambar 5.3



Gambar 5.3 Struktur IPv4 Address (Cisco Networking Academy, 2020)

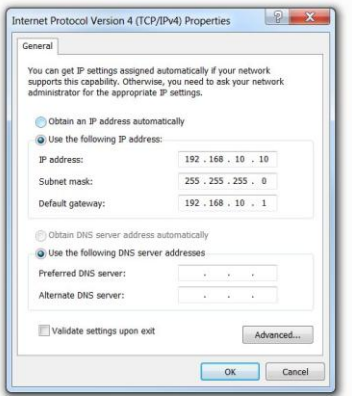
Bagian jaringan menunjukkan jaringan tempat sebuah perangkat (host) berada, sedangkan bagian host digunakan untuk mengidentifikasi perangkat tertentu dalam jaringan tersebut. Bagian host inilah yang membedakan satu perangkat dengan perangkat lainnya di dalam jaringan yang sama.

Subnet Mask digunakan untuk mengetahui berapa bit dari 32-bit alamat IPv4 address yang digunakan untuk bagian jaringan dan bagian host. Memiliki panjang 32-bit, yang juga direpresentasikan dalam notasi desimal bertitik, seperti bit dalam IPv4 address. Terdiri dari angka 1 yang berurutan diikuti oleh angka 0 yang berurutan dalam notasi biner. Umumnya, jumlah angka 1 menunjukkan panjang subnet mask (contoh : panjang subnet mask 255.0.0.0 adalah 8, panjang subnet mask 255.255.0.0 adalah 16, panjang subnet mask 255.255.255.0 adalah 24). Bit 1 digunakan untuk identifikasi bagian jaringan, sedangkan bit 0 digunakan untuk identifikasi bagian host.



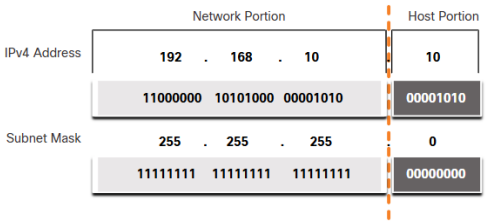
Gambar 5.4 Subnet Mask (Cisco Networking Academy, 2020)

Subnet mask umumnya digunakan bersama-sama dengan IPv4 address seperti pada gambar 5.5 berikut ini



Gambar 5.5 Konfigurasi IPv4 Address (Cisco Networking Academy, 2020)

Untuk mengidentifikasi bagian jaringan dan host dari alamat IPv4 pada gambar 5 tersebut diatas, subnet mask dibandingkan dengan alamat IPv4 bit demi bit, dari kiri ke kanan seperti yang ditunjukkan pada gambar 6 berikut ini

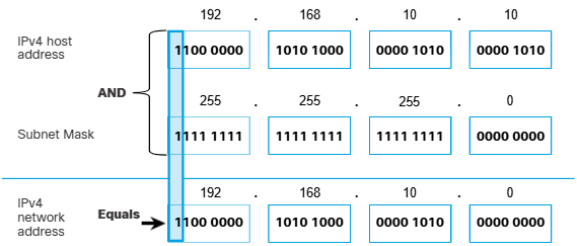


Gambar 5.6 Subnet Mask dalam notasi desimal (Cisco Networking Academy, 2020)

Perlu diperhatikan bahwa subnet mask sebenarnya tidak memuat bagian jaringan atau host dari alamat IPv4 address, subnet mask hanya memberi tahu komputer tempat mencari bagian alamat IPv4

yang merupakan bagian jaringan dan bagian mana yang merupakan bagian host. Proses sebenarnya yang digunakan untuk mengidentifikasi bagian jaringan dan bagian host disebut ANDing

Untuk mengidentifikasi alamat jaringan dari host IPv4, IPv4 address tersebut di AND secara logika, bit demi bit, dengan subnet mask. AND antara alamat dan subnet mask menghasilkan alamat jaringan. Untuk mengilustrasikan bagaimana AND digunakan untuk menemukan alamat jaringan, sebagai contoh host dengan IPv4 address 192.168.10.10 dan subnet mask 255.255.255.0, seperti yang ditunjukkan pada gambar 7



Gambar 5.7 Proses ANDing (Cisco Networking Academy, 2020)

Dengan menggunakan urutan bit pertama sebagai contoh, perhatikan bahwa operasi AND dilakukan pada bit ke-1 alamat host dengan bit ke-1 subnet mask. Ini menghasilkan bit ke-1 untuk alamat jaringan. 1 AND 1 = 1 (Boolean Operations). Operasi AND antara alamat host IPv4 dan subnet mask menghasilkan alamat jaringan IPv4 untuk host ini. Dalam contoh ini, operasi AND antara alamat host 192.168.10.10 dan subnet mask 255.255.255.0, menghasilkan

alamat jaringan IPv4 192.168.10.0. Ini adalah operasi IPv4 yang penting, karena memberi tahu host jaringan tempat ia berada.

Jenis komunikasi pada IPv4 address terdiri dari :

1. **Unicast** : Mengacu kepada satu perangkat yang mengirim pesan ke satu perangkat lain dalam komunikasi satu-ke-satu. Paket unicast memiliki IP address tujuan yang merupakan alamat unicast yang ditujukan ke satu penerima. IP address sumber hanya dapat berupa alamat unicast, karena paket hanya dapat berasal dari satu sumber.
2. **Broadcast :** Mengacu pada perangkat yang mengirim pesan ke semua perangkat di jaringan dalam komunikasi satu-ke-semua. Paket broadcast memiliki IP address tujuan dengan semu angka 1 di bagian host, atau 32 bit satu (255.255.255.255). Paket broadcast harus diproses oleh semua perangkat dalam domain broadcast yang sama.
3. **Multicast :** Mengacu pada perangkat yang mengirim pesan ke sekumpuan host terpilih yang berlangganan ke grup multicast. Paket multicast adalah paket dengan IP address tujuan yang merupakan alamat multicast. IPv4 telah menyediakan alamat 244.0.0.0 hingga 239.255.255.255 sebagai rentang multicast.

Tipe IPv4 address terdiri dari Private dan Public IP address (Lammle, 2016)

1. **Private IP Address :** Alamat yang hanya digunakan dalam jaringan lokal (LAN) dan tidak dapat diakses langsung dari internet. Alamat ini digunakan untuk identifikasi perangkat-

perangkat dalam satu jaringan privat, seperti di rumah, kantor, atau sekolah.

Network Address and Prefix	RFC 1918 Private Address Range
10.0.0.0/8	10.0.0.0 - 10.255.255.255
172.16.0.0/12	172.16.0.0 - 172.31.255.255
192.168.0.0/16	192.168.0.0 - 192.168.255.255

Gambar 5.8 blok Private IP Address (Salamatian et al., 2023)

2. **Public IP Address** : Alamat yang dapat diakses langsung dari internet global. Alamat ini diberikan oleh ISP (Internet Service Provider) dan digunakan untuk mengidentifikasi perangkat di luar jaringan lokal.

   Alamat IPv4 publik adalah alamat yang dirutekan secara global melalui internet. Alamat IPv4 publik harus unik. Baik alamat IPv4 maupun IPv6 dikelola oleh Internet Assigned Numbers Authority (IANA) (Jennings & Gurbani, 2008). IANA mengelola dan mengalokasikan blok alamat IP ke Regional Internet Registries (RIR) (Kuusisto, 2015). Kelima RIR ditunjukkan pada gambar 5.9 berikut ini

Gambar 5.9 Regional Internet Registries (RIR)

RIR bertanggung jawab untuk mengalokasikan IP Address ke ISP yang menyediakan blok IPv4 Address ke organisasi dan ISP yang lebih kecil. Organisasi juga dapat memperoleh alamat mereka secara langsung dari RIR (tunduk pada kebijakan RIR tersebut).

Pada awal pengembangan Internet, IP Address dibagi ke dalam beberapa kelas (classes) berdasarkan ukuran jaringan dan jumlah host. Sistem ini disebut Classful Addressing (Postel, 1981). Meskipun saat ini sudah jarang digunakan secara langsung (karena digantikan oleh CIDR), konsep ini masih penting untuk pemahaman dasar jaringan.

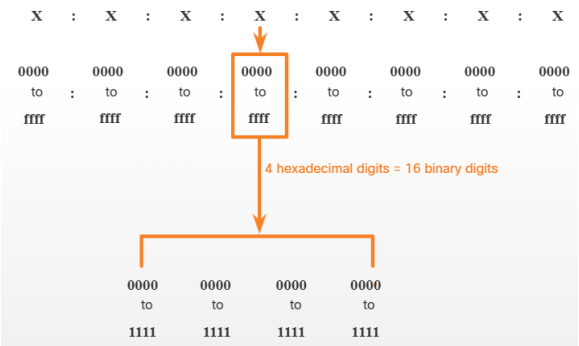
1. Kelas A, 1.0.0.0 s.d 126.255.255.255, Subnet Mask 255.0.0.0 (/8), untuk jaringan besar.
2. Kelas B, 128.0.0.0 s.d 191.255.255.255, Subnet Mask 255.255.0.0 (/16), untuk jaringan menengah.
3. Kelas C, 192.0.0.0 s.d 223.255.255.255, Subnet Mask 255.255.255.0, untuk jaringan kecil
4. Kelas D, 224.0.0.0 s.d 239.255.255.255, untuk jaringan multicast
5. Kelas E, 240.0.0.0 s.d 255.255.255.255, untuk eksperimen/riset

C. IPV6 ADDRESSING

IPv6 dirancang sebagai penerus dari IPv4. IPv6 memiliki ruang alamat yang jauh lebih besar, yaitu 128-bit, yang menyediakan 340 undecillion (yaitu angka 340 diikuti oleh 36 nol) kemungkinan

alamat (Siddiqui, 2017). Namun, IPv6 bukan hanya soal ukuran alamat yang lebih besar. Kelangkaan IPv4 address telah menjadi faktor pendorong utama dalam peralihan ke IPv6. Seiring dengan semakin terkoneksinya kawasan seperti Afrika, Asia, dan wilayah lainnya ke internet, IPv4 address tidak lagi mencukupi untuk mengakomodasi pertumbuhan tersebut.

IPv6 address memiliki panjang 128 bit dan ditulis sebagai rangkaian nilai heksadesimal. Setiap empat bit direpresentasikan oleh satu digit heksadesimal, sehingga secara keseluruhan terdiri dari 32 digit heksadesimal, seperti yang ditunjukkan dalam gambar. IPv6 address tidak peka huruf besar-kecil (case-insensitive) dan bisa ditulis menggunakan huruf kecil maupun huruf kapital.



Gambar 5.10 Representasi IPv6 Hexadecimal (Cisco Networking Academy, 2020)

Penulisan IPv6 address memang bisa sangat panjang dan rumit, tetapi untungnya dapat disederhanakan menggunakan dua aturan utama yaitu Leading Zeros dan Double Colon (::)

1. Leading Zeros : Nol di depan (leading zeros) dalam setiap blok boleh dihapus. Contoh 2001:0db8:0000:0000:0000:ff00:0042:8329 menjadi 2001:db8:0:0:0:ff00:42:8329.
2. Double Colon : Jika ada dua atau lebih blok "0000" secara berurutan, kitab isa menggantinya dengan ::, akan tetapi hanya boleh sekali dalam satu Alamat. Contoh 2001:db8:0:0:0:ff00:42:8329 menjadi 2001:db8::ff00:42:8329

Sama seperti pada IPv4, terdapat beberapa jenis IPv6 address. Bahkan, IPv6 memiliki tiga kategori utama alamat :

1. Unicast : IPv6 address unicast digunakan untuk mengidentifikasi secara unik satu antarmuka (interface) pada perangkat yang mendukung IPv6.
2. Multicast : Alamat IPv6 multicast digunakan untuk mengirim satu paket IPv6 ke beberapa tujuan sekaligus.
3. Anycast : Alamat IPv6 anycast adalah alamat unicast yang bisa ditetapkan ke beberapa perangkat.

Berbeda dengan IPv4, IPv6 tidak memiliki alamat broadcast. Namun, sebagai gantinya, IPv6 memiliki alamat multicast all-nodes, yang memberikan fungsi serupa dengan broadcast, yaitu mengirim pesan ke semua node dalam jaringan.

Dalam IPv4, bagian prefix atau bagian jaringan dari sebuah IP address dapat diidentifikasi menggunakan subnet mask dalam format desimal bertitik (dotted-decimal) atau dengan panjang

prefix dalam notasi garis miring (slash notation). Misalnya, IPv4 address 192.168.1.10 dengan subnet mask 255.255.255.0 setara dengan 192.168.1.10/24.

Dalam IPv6, hanya digunakan istilah panjang prefix (prefix length). IPv6 tidak menggunakan notasi subnet mask desimal bertitik seperti IPv4. Sama seperti pada IPv4, panjang prefix dalam IPv6 juga ditulis menggunakan notasi garis miring untuk menunjukkan bagian jaringan dari sebuah alamat IPv6.

Panjang prefix dalam IPv6 dapat berkisar dari 0 hingga 128. Panjang prefix yang direkomendasikan untuk jaringan LAN dan sebagian besar jenis jaringan lainnya adalah /64, seperti yang ditunjukkan pada gambar.

Gambar 5.11 IPv6 prefix length (Cisco Networking Academy, 2020)

IPv6 unicast address secara unik mengidentifikasi sebuah antarmuka (interface) pada perangkat yang mendukung IPv6. Sebuah paket yang dikirim ke alamat unicast akan diterima oleh antarmuka yang diberikan alamat tersebut. Mirip seperti pada IPv4, alamat sumber (source address) dalam IPv6 harus berupa alamat unicast.

Sedangkan alamat tujuan (destination address) dapat berupa alamat unicast maupun alamat multicast.

IPv6 unicast address terdiri dari :

1. Global Unicast Address (GUA) : Mirip dengan IPv4 publik. Alamat ini unik secara global dan dapat dirutekan melalui internet. Dapat dikonfigurasi secara statis atau diberikan secara dinamis.
2. Link Local Address (LLA) : Alamat ini diperlukan untuk setiap perangkat yang mendukung IPv6. Digunakan untuk berkomunikasi dengan perangkat lain dalam jaringan lokal yang sama (link). Dalam konteks IPv6, istilah link merujuk kepada subnet. Hanya berlaku dalam satu link saja.
3. Loopback : Alamat khusus (::1) yang digunakan oleh perangkat untuk mengirim paket ke dirinya sendiri.
4. Unique Local : Alamat ini digunakan untuk komunikasi lokal dalam satu organisasi. Mirip dengan Private Address pada IPv4
5. Unspesified Address : Alamat ini ditulis sebagai :: dan digunakan Ketika perangkat belum memiliki Alamat IPv6 (misalnya saat proses pengalamatan otomatis dimulai.

D. SUBNETTING

Dalam jaringan LAN Ethernet, perangkat menggunakan broadcast dan Address Resolution Protocol (ARP) untuk menemukan perangkat lain. ARP mengirimkan broadcast pada Layer 2 ke IPv4

address yang diketahui di jaringan lokal untuk menemukan alamat MAC yang sesuai. Perangkat dalam jaringan Ethernet juga menemukan perangkat lain melalui layanan jaringan. Misalnya, sebuah host biasanya memperoleh konfigurasi alamat IPv4-nya menggunakan Dynamic Host Configuration Protocol (DHCP), yang mengirimkan broadcast ke jaringan lokal untuk menemukan server DHCP.

Broadcast domain yang besar adalah jaringan yang menghubungkan banyak host. Masalah dari broadcast domain yang besar adalah banyaknya host dapat menghasilkan broadcast berlebihan yang berdampak negatif terhadap jaringan. Misal, LAN 1 menghubungkan 400 pengguna yang berpotensi menghasilkan lalu lintas broadcast dalam jumlah besar. Hal ini dapat menyebabkan operasi jaringan menjadi lambat karena tingginya volume lalu lintas yang terjadi, serta kinerja perangkat menjadi menurun karena setiap perangkat harus menerima dan memproses setiap paket broadcast yang diterima.

Solusinya adalah dengan mengurangi ukuran jaringan untuk membuat broadcast domain yang lebih kecil melalui proses yang disebut subnetting. Ruang jaringan yang lebih kecil ini disebut subnet. Misal, 400 pengguna di LAN dengan alamat jaringan 172.16.0.0/16 telah dibagi menjadi dua subnet, masing-masing berisi 200 pengguna menggunakan 172.16.0.0/24 (LAN 1) dan 172.16.1.0/24 (LAN 2).

Subnetting adalah proses membagi sebuah jaringan besar menjadi jaringan-jaringan yang lebih kecil, yang disebut subnet (*subnetworks*) (Cisco Networking Academy, 2020; Huawei Technologies Co., Ltd., 2023). Teknik ini banyak digunakan dalam manajemen jaringan komputer untuk meningkatkan efisiensi penggunaan alamat IP, mengurangi kemacetan jaringan, serta meningkatkan keamanan dan keteraturan infrastruktur jaringan. Subnetting memungkinkan administrator jaringan untuk Menghemat dan mengelola IP address secara lebih efisien, Memisahkan lalu lintas jaringan berdasarkan departemen/fungsi/Lokasi, Mengurangi broadcast yang tidak diperlukan, dan Meningkatkan keamanan dengan membatasi akses antar subnet.

IPv4 address terdiri dari 32-bit yang ditulis dalam empat oktet decimal (misal : IP Address 192.168.10.1, Subnet Mask 255.255.255.0, Prefik /24). Subnet mask menunjukkan berapa bit yang digunakan untuk Network ID, dan sisanya digunakan untuk Host ID. Dari contoh tersebut kita memiliki alamat jaringan 192.168.10.0 dan ingin membuat 4 subnet, maka berikut ini Langkah subnettingnya :

1. Hitung jumlah bit yang dibutuhkan untuk membuat 4 subnet menggunakan rumus $2^n \geq$ jumlah subnet (n adalah bit 1). $2^2 \geq 4$, maka n = 2 (butuh 2 bit tambahan)
2. Tambahkan 2 bit ke prefik awal, /24 (255.255.255.0) + 2 = /26 (255.255.255.192)

3. Hitung jumlah host per subnet menggunakan rumus 2^(n-2) dimana n adalah bit 0 yang didapatkan dari 32 – 26 yaitu 6-bit 0. Sehingga didapatkan 2^(6-2) = 62 IPv4 Address
4. Maka hasil subnetnya adalah sebagai berikut :
   a. Subnet 1 (62 Host) → 192.168.10.0/26
   b. Subnet 2 (62 Host) → 192.168.10.64/26
   c. Subnet 3 (62 Host) → 192.168.10.128/26
   d. Subnet 4 (62 Host) → 192.168.10.192/26

BAGIAN 6
PROTOKOL JARINGAN

A. PENGERTIAN PROTOKOL JARINGAN

Protokol jaringan adalah sekumpulan aturan atau standar yang digunakan untuk mengatur komunikasi data antar perangkat dalam sebuah jaringan komputer. Protokol ini menentukan cara data dikemas, dikirim, diterima, dan diinterpretasikan, sehingga perangkat yang berbeda dapat berkomunikasi dengan efektif dan efisien.

Contoh sederhananya seperti manusia butuh bahasa untuk saling mengerti saat berbicara, komputer juga butuh "bahasa bersama" itulah fungsi protokol jaringan.

Berikut beberapa contoh protokol jaringan populer beserta fungsinya:

1. TCP (*Transmission Control Protocol*)
   Menjamin pengiriman data secara andal dan berurutan. Contoh penggunaan: browsing web, email, file transfer.
2. IP (*Internet Protocol*)
   Mengatur alamat dan rute data agar sampai ke tujuan yang benar di jaringan. Bekerja bersama TCP sebagai TCP/IP.
3. HTTP (*HyperText Transfer Protocol*)

Protokol utama untuk mengakses halaman web. Versi amannya: HTTPS, menggunakan enkripsi SSL/TLS.

4. FTP (*File Transfer Protocol*)
   Digunakan untuk mentransfer file antar komputer dalam jaringan.
5. DNS (*Domain Name System*)
   Menerjemahkan nama domain (seperti google.com) menjadi alamat IP.
6. DHCP (*Dynamic Host Configuration Protocol*)
   Memberikan alamat IP secara otomatis ke perangkat yang terhubung ke jaringan.
7. SMTP (*Simple Mail Transfer Protocol*)
   Digunakan untuk mengirim email.
8. POP3/IMAP
   Digunakan untuk mengambil email dari server.
9. UDP (*User Datagram Protocol*)
   Alternatif dari TCP, lebih cepat tapi tidak menjamin keandalan data. Cocok untuk streaming dan game online.

Berikut adalah definisi protokol jaringan menurut para ahli yang telah dikenal luas dalam bidang ilmu komputer dan jaringan:

1. Menurut Andrew S. Tanenbaum (Tanenbaum & Wetherall, 2010): "Protokol jaringan adalah seperangkat aturan yang mengatur komunikasi data antara perangkat-perangkat dalam jaringan komputer." Tanenbaum menjelaskan bahwa protokol mendefinisikan bagaimana data dikemas, ditransmisikan, dan

diterima, sehingga semua perangkat di jaringan dapat berkomunikasi secara efisien.

2. William Stallings (Stallings, 2013) mengatakan "Protokol adalah seperangkat aturan yang mendefinisikan format dan urutan pesan yang dipertukarkan antara entitas yang berkomunikasi, serta tindakan yang diambil saat terjadi transmisi atau kesalahan." Stallings menekankan struktur formal komunikasi dan respons terhadap gangguan, menjadikannya lebih dari sekadar aturan teknis, tapi juga sistem respon.
3. Douglas E. Comer (Comer, 2015) "*Network protocol is a set of rules and conventions that devices use to communicate on a network.*" Definisi ini menyoroti pentingnya kesepakatan (*convention*) dalam protokol sehingga berbagai jenis perangkat dan sistem dapat saling memahami.
4. Menurut Forouzan (B. Forouzan, 2006)**:** "Protokol adalah seperangkat aturan yang mengatur pertukaran data antar entitas dalam komunikasi data." Forouzan memfokuskan pada aspek komunikasi data dan pertukaran informasi yang teratur serta efisien.
5. James F. Kurose & Keith W. Ross (Kurose & Ross, 2012) berpendapat : "*A network protocol defines the format and the order of messages exchanged between two or more communicating entities, as well as the actions taken on the transmission and receipt of a message*." Definisi ini sangat teknis dan modern, mencakup struktur pesan dan reaksi sistem terhadap pesan yang dikirim dan diterima.

6. Behrouz A. Forouzan (B. A. Forouzan, 2013) mengatakan "*A protocol is a set of rules that governs data communications; it represents an agreement between the communicating devices*."

Protokol jaringan merupakan himpunan aturan atau prosedur yang memungkinkan perangkat dalam jaringan komputer berkomunikasi dengan benar dan efisien. Aturan ini meliputi:

1. Format data
2. Urutan transmisi
3. Tindakan bila terjadi kesalahan
4. Pengakuan dan respons antar perangkat

B. SISTEM PROTOKOL JARINGAN

Adalah kumpulan protokol yang bekerja secara terstruktur dalam lapisan-lapisan (*layers*) untuk mengatur komunikasi antar perangkat dalam jaringan komputer. Sistem ini memastikan bahwa proses komunikasi data berjalan dengan tertib, efisien, dan bisa diandalkan, mulai dari pengiriman hingga penerimaan data.

Sistem protokol biasanya mengacu pada dua model utama:

1. Model OSI (*Open Systems Interconnection*) – 7 lapisan:

a. *Physical* yaitu media fisik (kabel, sinyal)
b. *Data Link* yaitu pengalamatan MAC, deteksi error
c. *Network* yaitu pengalamatan IP, routing (contoh: IP)

d. *Transport* yaitu pengiriman data end-to-end (contoh: TCP, UDP)
e. *Session* yaitu manajemen sesi komunikasi
f. *Presentation* yaitu enkripsi, kompresi, format data
g. *Application* yaitu interaksi dengan aplikasi pengguna (contoh: HTTP, FTP)

2. Model TCP/IP – lebih sederhana, 4 lapisan:

a. *Network Access* (Link)
b. *Internet* (contoh: IP)
c. *Transport* (contoh: TCP, UDP)
d. *Application* (contoh: HTTP, FTP, SMTP)

Tabel 6.1. Contoh Protokol dalam Sistem

Lapisan	Protokol
Aplikasi	HTTP, FTP, SMTP
Transport	TCP, UDP
Internet	IP (IPv4/IPv6), ICMP
Link	Ethernet, Wi-Fi

Jadi, sistem protokol jaringan bekerja seperti tim kerja yang terorganisir, di mana setiap lapisan punya tugas tertentu, dan data diproses bertahap dari satu lapisan ke lapisan lain sampai sampai ke tujuan.

C. TUJUAN DAN MANFAAT PROTOKOL JARINGAN

Berikut adalah tujuan dan manfaat dari protokol jaringan secara jelas dan ringkas:

Tujuan Protokol Jaringan:

1. Mengatur komunikasi antar perangkat
   Supaya perangkat bisa saling "mengerti" dan bertukar data dengan benar.
2. Menstandarisasi proses pengiriman data
   Semua perangkat, walau berbeda jenis atau sistem operasi, bisa berkomunikasi karena mengikuti aturan yang sama.
3. Menjamin keandalan dan keamanan data
   Protokol seperti TCP memastikan data dikirim lengkap dan urut, sementara HTTPS memberi keamanan lewat enkripsi.
4. Mengelola koneksi antar perangkat
   Mengatur pembentukan, pemeliharaan, dan pemutusan koneksi.
5. Mengoptimalkan kinerja jaringan
   Menghindari bentrokan data, mengatur alokasi alamat IP, dan memperlancar lalu lintas data.

Manfaat Protokol Jaringan:

1. Komunikasi antar perangkat menjadi mungkin
   Tanpa protokol, komputer tidak bisa saling bertukar data.
2. Memungkinkan jaringan global (seperti internet)
   Protokol seperti TCP/IP memungkinkan koneksi lintas negara dan sistem.

3. Memastikan data dikirim dengan benar
   Deteksi dan koreksi error selama pengiriman.
4. Mendukung berbagai jenis layanan jaringan
   Seperti browsing (HTTP), email (SMTP), transfer file (FTP), dan lainnya.
5. Meningkatkan efisiensi dan keamanan
   Protokol membantu menjaga agar jaringan tidak mudah disusupi dan tetap optimal digunakan.

D. KOMPONEN PROTOKOL JARINGAN

Berikut adalah komponen utama dalam protokol jaringan yang membuat proses komunikasi data antar perangkat bisa berjalan dengan baik:

Komponen Protokol Jaringan:

1. *Syntax* (Sintaksis)
   a. Menjelaskan struktur atau format data yang ditransmisikan.
   b. Termasuk urutan bit, byte, header, dan field data.
   c. Contoh: Dalam protokol HTTP, struktur data terdiri dari metode, URL, versi, dan header.
2. *Semantics* (Semantik)
   a. Menjelaskan arti dari setiap bagian data.
   b. Apa fungsi atau makna dari setiap bagian dalam protokol.
   c. Contoh: Bit tertentu dalam header IP menunjukkan apakah paket itu bisa dipecah atau tidak.

3. *Timing* (Waktu)
    a. Menjelaskan kapan data dikirim dan seberapa cepat.
    b. Termasuk kecepatan pengiriman, urutan pengiriman, dan kontrol aliran data.
    c. Contoh: Protokol seperti TCP menggunakan sistem timing untuk memastikan data sampai secara berurutan dan tanpa kehilangan.
4. Prosedur (Rules/Aturan)
    a. Aturan bagaimana dua atau lebih perangkat membangun koneksi, mengirim data, dan mengakhiri koneksi.
    b. Contoh: Protokol TCP menggunakan proses "*3-way handshake*" untuk memulai koneksi.

Sehingga dapat disimpulkan bahwa:
Komponen protokol = bagaimana bentuk data (*syntax*) + apa artinya (*semantics*) + kapan dan bagaimana dikirimnya (*timing* + prosedur).

Contoh sederhananya dua orang yang sedang berkirim surat atau bertelepon. Ini akan mempermudah kamu memahami komponen protokol jaringan:

1. *Syntax* (Sintaksis) sama dengan Format Surat
    Bayangkan anda menulis surat. Ada format yang harus diikuti:
    a. Nama pengirim
    b. Alamat penerima
    c. Isi pesan
    d. Tanda tangan di akhir

Kalau anda mengacak formatnya, maka penerima bisa bingung.

Di jaringan, syntax adalah aturan format data, seperti struktur header, urutan bit, dll.

2. *Semantics* (Semantik) sama dengan Arti Pesan

   Dalam surat kamu tulis, misalnya: "Tolong datang jam 3 sore."

   Kalimat itu punya makna tertentu. Jika penerima salah paham, maka dia dapat datang pada jam 3 pagi.

   Di jaringan, semantics menjelaskan arti setiap bagian data, seperti arti dari kode tertentu di header.

3. *Timing* (Waktu) sama dengan kapan dan seberapa cepat kita berbicara.

   Contohnya pada saat anda menelepon kepada teman:

   a. Anda berbicara terlalu cepat, maka teman anda akan bingung.
   b. Jika anda berbicara berbarengan maka akan saling tumpang tindih pembicaraaannya.

   Timing mengatur kapan harus mengirim, berapa cepat, dan urutan data agar tidak bentrok atau salah paham.

4. Prosedur sama dengan aturan Main Komunikasi

   Sama halnya pada saat anda mulai telepon dengan:

   "Halo, bisa dengar suara saya?"

   Lalu diakhiri dengan:

   "Oke, terima kasih, sampai jumpa."

   Dalam jaringan, prosedur mengatur pembukaan, pengiriman, dan penutupan koneksi (seperti "*3-way handshake*" di TCP).

Sehingga dapat disimpulkan bahwa Komunikasi manusia butuh aturan supaya pesan jelas dan lancar, begitu juga komunikasi antar komputer di jaringan. Protokol jaringan adalah "aturan tata krama" versi digital.

E. TINGKATAN APLIKASI PROTOKOL JARINGAN

Lapisan paling atas dalam sistem komunikasi jaringan, tempat di mana pengguna dan aplikasi berinteraksi langsung dengan jaringan. Tingkatan Aplikasi (*Application Layer*) dalam Protokol Jaringan adalah lapisan aplikasi pada lapisan ke-7 dalam model OSI atau lapisan ke-4 dalam model TCP/IP. Berfungsi untuk menyediakan layanan jaringan langsung kepada pengguna akhir atau aplikasi.

Fungsi Utama Lapisan Aplikasi:

1. Menyediakan antarmuka bagi aplikasi untuk mengakses jaringan.
2. Menyediakan layanan komunikasi untuk berbagai aktivitas seperti *browsing*, email, transfer file, dan sebagainya.
3. Mengatur format data agar bisa dimengerti oleh pengguna dan sistem penerima.

Tabel 6.2 Contoh Protokol pada Tingkatan Aplikasi

Protokol	Fungsi	Contoh Penggunaan
HTTP / HTTPS	Transfer halaman web	Membuka website di browser
FTP / SFTP	Transfer file	Mengirim/unduh file ke

Protokol	Fungsi	Contoh Penggunaan
		server
SMTP	Mengirim email	Proses pengiriman email
POP3 / IMAP	Mengambil email	Mengakses email masuk
DNS	Menerjemahkan domain ke IP	Mengetik “google.com” di browser
Telnet / SSH	Akses remote ke komputer lain	Mengelola server dari jarak jauh

Analoginya:

Jika anda membuka aplikasi browser seperti Chrome dan mengetik alamat web. Maka:

1. Aplikasi anda meminta layanan ke jaringan via HTTP.
2. Protokol HTTP bekerja di lapisan aplikasi, meneruskan permintaan itu ke lapisan-lapisan bawah untuk diproses.

Dengan demikian Tingkatan aplikasi adalah tempat di mana protokol "bertemu" dengan pengguna. Tanpa lapisan ini, aplikasi seperti browser, email, atau game online tidak bisa menggunakan jaringan.

F. DASAR PENGGUNAAN PROTOKOL JARINGAN

Protokol jaringan digunakan karena komputer dan perangkat jaringan membutuhkan aturan bersama agar dapat saling

berkomunikasi, bertukar data, dan memahami satu sama lain, meskipun berasal dari sistem atau vendor yang berbeda.

Alasan dan Dasar Utamanya:

1. Standarisasi Komunikasi
   Semua perangkat menggunakan "bahasa" yang sama dalam pertukaran data.
2. Interoperabilitas Perangkat
   Komputer Windows, Mac, Linux, bahkan *smartphone* bisa saling terhubung karena menggunakan protokol yang sama.
3. Keamanan Komunikasi
   Protokol seperti HTTPS atau SSH membantu mengenkripsi data agar tidak mudah disadap.
4. Efisiensi dan Keandalan
   Protokol seperti TCP menjamin data sampai secara lengkap dan berurutan.
5. Pengendalian dan Manajemen Jaringan
   Protokol seperti DHCP, DNS, dan ICMP membantu mengatur alamat IP, nama domain, serta diagnostik jaringan.
6. Dukungan terhadap Aplikasi dan Layanan
   Aplikasi seperti browser, email, dan *video call* bisa berjalan karena memanfaatkan protokol jaringan yang sesuai.

Sehingga dapat disimpulkan bahwa Protokol jaringan adalah fondasi utama komunikasi digital tanpa protokol, internet dan jaringan lokal tidak akan bisa berjalan sebagaimana mestinya.

Gambar 6.1. Protokol Jaringan

Sumber: https://jagad.id/pengertian-protokol/

BAGIAN 7
KEAMANAN JARINGAN KOMPUTER

A. KONSEP DASAR KEAMANAN JARINGAN

Keamanan jaringan komputer merupakan disiplin yang berfokus pada perlindungan infrastruktur, perangkat, data, dan komunikasi dalam jaringan dari berbagai ancaman yang dapat membahayakan sistem. Dengan semakin tingginya ketergantungan pada teknologi informasi dalam beragam bidang dari bisnis, pemerintahan, krpendidikan juga prlayanan kesehatan, keamanan jaringan menjadi aspek krusial yang tidak dapat diabaikan. Peningkatan penggunaan internet dan sistem berbasis *cloud* memperluas cakupan jaringan komputer, namun di sisi lain juga meningkatkan risiko serangan siber yang bisa merugikan secara individual ataupun organisasi. Konsep dasar keamanan jaringan harus dipahami dan diterapkan secara menyeluruh supaya bisa memberi perlindungan sistem atas beragam masalah yang terus berkembang.

Keamanan jaringan bertumpu pada tiga prinsip utama yang dikenal sebagai *Confidentiality, Integrity, and Availability* (*CIA Triad*). Kerahasiaan (*confidentiality*) mengacu pada perlindungan data serta informasi terhadap akses ilegal. Dalam dunia digital ancaman terhadap kerahasiaan sering muncul dalam bentuk pencurian data, seperti serangan *phishing*, *man-in-the-middle attack*, atau peretasan basis data. Integritas (*integrity*) memastikan bahwa data yang

tersimpan maupun yang dikirim melalui jaringan tidak diubah, dihapus, atau dimanipulasi pihak yang tidak berwenang. Serangan terhadap integritas data dapat berupa *data tampering* di mana informasi yang dikirim melalui jaringan diubah tanpa sepengetahuan pengirim maupun penerima. Ketersediaan (*availability*) menjamin agar pelayanan jaringan tetap dapat diakses oleh pemakai sah tanpa gangguan. Serangan seperti *Distributed Denial-of-Service* (DDoS) dapat mengancam ketersediaan layanan dengan membanjiri jaringan atau server dengan lalu lintas palsu hingga sistem menjadi tidak dapat merespons pengguna sah (Kumar & Shukla, 2021).

Seiring perkembangan teknologi, konsep keamanan jaringan terus berkembang menyesuaikan dengan ancaman yang semakin kompleks. Pendekatan tradisional dalam keamanan jaringan lebih menitikberatkan pada pengamanan perimeter jaringan, di mana lapisan perlindungan ditempatkan untuk mencegah akses tidak sah dari luar sistem. Namun dengan meningkatnya model kerja jarak jauh, layanan berbasis *cloud*, dan penggunaan perangkat *Internet of Things* (IoT), pendekatan keamanan berbasis perimeter menjadi kurang efektif. Muncul konsep keamanan modern seperti *Zero Trust Architecture* (ZTA) yang mengadopsi prinsip bahwa tidak ada entitas yang dapat dipercaya secara *default* baik yang berasal dari dalam maupun luar jaringan organisasi. Model ini mengharuskan setiap permintaan akses untuk diverifikasi secara ketat berdasarkan

identitas pengguna, lokasi, perangkat, dan pola perilaku sebelum diizinkan mengakses sumber daya jaringan (Brown et al., 2024).

Dalam praktik keamanan jaringan komputer selain tergantung terhadap teknologi, juga terhadap kebijakan, regulasi, dan kesadaran pengguna. Banyak negara dan organisasi internasional menetapkan standar dan regulasi ketat untuk memastikan sistem keamanan jaringan yang lebih kuat. *General Data Protection Regulation* (GDPR) yang diterapkan di Uni Eropa mewajibkan perusahaan untuk memberi perlindungan data pribadi pengguna dengan standar keamanan tinggi. Di Amerika Serikat regulasi seperti *Cybersecurity Information Sharing Act* (CISA) mendorong berbagi informasi mengenai ancaman siber antara perusahaan dan pemerintah untuk meningkatkan respons terhadap serangan. Regulasi ini menekankan bahwa keamanan jaringan selain menjadi tanggung jawab tim teknologi informasi (TI), juga seluruh elemen dalam organisasi yang terlibat dalam pemrosesan dan pengelolaan data digital (Singh & Sharma, 2022).

Ancaman terhadap keamanan jaringan komputer bisa bersumber dari beragam sebab dari dalam organisasi ataupun pihak eksternal. Ancaman internal sering disebabkan oleh kelalaian atau kesalahan manusia seperti penggunaan kata sandi yang lemah, pengunduhan perangkat lunak berbahaya, atau kurangnya pemahaman terhadap protokol keamanan. Sekitar 60% insiden keamanan siber terjadi akibat kelalaian pengguna, termasuk dalam penggunaan perangkat dan akses jaringan yang tidak sesuai dengan kebijakan keamanan

(M. Johnson et al., 2020). Pelatihan dan kesadaran keamanan bagi karyawan menjadi faktor penting dalam memperkuat pertahanan jaringan organisasi.

Ancaman eksternal dapat berupa serangan yang dilakukan oleh peretas, kelompok kriminal siber, atau bahkan aktor negara yang memiliki kepentingan politik atau ekonomi. Contoh serangan eksternal yang terkenal adalah serangan *ransomware* di mana peretas melakukan enkripsi data pengguna serta menuntut tebusan bila mendapatkan kembali akses terhadap data dimaksud. Serangan *WannaCry* pada tahun 2017 menjadi s contoh serangan *ransomware* yang menyebar secara global dan menyebabkan kerugian miliaran dolar. Serangan siber juga dapat berbentuk eksploitasi celah keamanan perangkat lunak, pencurian identitas, atau manipulasi informasi yang beredar di jaringan (Rahman et al., 2021).

Untuk mengatasi berbagai ancaman tersebut, organisasi perlu mengadopsi strategi keamanan jaringan berlapis yang mencakup pengamanan perangkat keras, perangkat lunak, serta kebijakan keamanan ketat. Teknologi seperti *firewall*, sistem deteksi dan pencegahan intrusi (IDS/IPS), serta enkripsi data menjadi komponen utama dalam perlindungan jaringan. *Firewall* berfungsi sebagai penyaring lalu lintas jaringan yang hanya mengizinkan komunikasi yang disetujui berdasarkan aturan keamanan yang ditetapkan. IDS dan IPS bekerja dengan cara mendeteksi serta mencegah serangan sebelum mencapai sistem utama. Enkripsi data digunakan untuk

mengamankan informasi yang dikirim melalui jaringan hingga tak bisa diakses pihak yang tak autoritatif meskipun berhasil mencegat data tersebut (Mishra et al., 2019).

Strategi keamanan jaringan yang efektif juga mencakup perencanaan respons terhadap insiden siber. Berbagai organisasi kini mempunyai *Computer Security Incident Response Team* (CSIRT) yang bertanggung jawab dalam menangani dan merespons insiden keamanan secara cepat. CSIRT berperan mengidentifikasi serangan, mengisolasi dampak, serta memulihkan sistem yang terdampak dengan seminimal mungkin gangguan terhadap operasional organisasi. Organisasi yang memiliki strategi respons insiden yang baik dapat mengurangi waktu pemulihan pasca serangan hingga 50% (Al-Hadhrami et al., 2023).

Keamanan jaringan komputer merupakan bidang yang terus berkembang dan membutuhkan pendekatan komprehensif. Dengan kombinasi teknologi, kebijakan regulasi, serta peningkatan kesadaran dan edukasi pengguna, ancaman siber dapat diminimalkan secara efektif. Dalam lingkungan digital yang semakin kompleks, penguatan keamanan jaringan selain menjadi tanggung jawab tim TI, juga seluruh individu yang terlibat dalam ekosistem digital.

B. JENIS SERANGAN DALAM JARINGAN KOMPUTER

Jaringan komputer menjadi target utama bagi berbagai serangan siber yang bertujuan untuk mengakses, merusak, atau mencuri informasi yang tersimpan dalam sistem. Kemajuan teknologi informasi dan komunikasi secara cepat berdampak nyata pada infrastruktur jaringan, namun di sisi lain juga meningkatkan risiko keamanan. Serangan jaringan komputer dapat berasal dari berbagai sumber dari individu peretas (*hackers*), kelompok kriminal siber, hingga aktor negara yang memiliki kepentingan tertentu. Beragam metode digunakan oleh pelaku serangan untuk mengeksploitasi celah keamanan dari pencurian kredensial, penyusupan sistem, hingga sabotase layanan digital. Memahami jenis serangan dalam jaringan komputer menjadi langkah awal yang penting dalam upaya pencegahan dan mitigasi ancaman siber.

Jenis serangan yang sangat umum yaitu *Denial-of-Service* (DoS) serta *Distributed Denial-of-Service* (DDoS). Serangan tersebut ditujukan agar membuat layanan atau sistem tak bisa diakses pemakai sah dengan cara membanjiri *server* dengan lalu lintas data dalam jumlah besar. Dalam serangan DoS pelaku menggunakan satu sumber untuk mengirimkan permintaan yang berlebihan ke *server* target sehingga menyebabkan *overload* dan menghambat kinerja. Sementara dalam serangan DDoS serangan dilakukan secara terdistribusi menggunakan berbagai perangkat yang telah dikompromikan pelaku. Serangan jenis ini sering memanfaatkan *botnet* yaitu kumpulan perangkat yang telah diinfeksi *malware* dan

dikendalikan peretas untuk melancarkan serangan secara bersamaan (Jiang et al., 2021).

Jenis serangan lain yang sangat merugikan adalah *malware* yaitu piranti lunak berbahaya yang didesain menginfeksi, merusak, ataupun mengambil alih kendali sistem komputer tanpa sepengetahuan pengguna. Beberapa jenis *malware* yang lazim mencakup virus, *worm*, *trojan*, *spyware*, serta *ransomware*. Virus dan *worm* memiliki kemampuan untuk menyebar secara otomatis melalui jaringan, sementara *trojan* sering menyamar sebagai aplikasi yang sah untuk mengelabui pengguna. *Spyware* digunakan untuk mengumpulkan informasi rahasia dari sistem yang terinfeksi seperti *credential login* atau data keuangan. *Ransomware* yang menjadi ancaman besar dalam beberapa tahun terakhir mengenkripsi data korban dan meminta tebusan agar data tersebut dapat dipulihkan (Alazab et al., 2022).

Phishing adalah jenis serangan siber yang mengandalkan rekayasa sosial untuk menipu korban agar memberi informasi sensitif semisal kata sandi ataupun data kartu kredit. Serangan *phishing* biasanya dilakukan melalui e-mail yang berisi tautan atau lampiran berbahaya yang mengarahkan korban ke situs web palsu yang menyerupai situs resmi. Begitu pengguna memasukkan informasi pribadi di situs tersebut, data tersebut langsung jatuh ke tangan penyerang. *Phishing* semakin berkembang dengan adanya teknik seperti *spear phishing* yang menargetkan individu tertentu dengan pesan yang lebih personal dan meyakinkan, serta *whaling* yang

bersasaran eksekutif perusahaan atau tokoh penting organisasi (Verma & Das, 2020).

Man-in-the-middle (MitM) *Attack* adalah serangan dengan peretas menyusup pada komunikasi antar dua pihak tanpa diketahui sehingga dapat mencuri atau memanipulasi data yang dikirimkan. Bentuk umum serangan MitM adalah penyadapan lalu lintas jaringan di Wi-Fi publik yang tidak dilindungi dengan enkripsi kuat. Serangan ini juga bisa terjadi dalam komunikasi berbasis protokol HTTP yang tidak dienkripsi, memungkinkan pelaku mengubah isi pesan atau mengarahkan pengguna ke situs palsu berbahaya (Kshetri, 2021).

Eksploitasi celah keamanan dalam perangkat lunak juga merupakan metode yang lazim dipakai pada serangan jaringan komputer yang dikenal sebagai *Zero-Day Attack* di mana pelaku memakai kerentanan piranti lunak yang tidak diidentifikasi pengembang ataupun tidak mendapat *patch* keamanan. Serangan jenis ini sangat berbahaya karena tidak ada perlindungan yang tersedia pada tahap awal serangan. Banyak kelompok peretas yang menjual atau memperdagangkan informasi mengenai celah keamanan ini di pasar gelap untuk dimanfaatkan pihak lain dalam melancarkan serangan (Bilge & Dumitras, 2019).

SQL Injection (SQLi) merupakan teknik serangan yang menargetkan basis data dalam suatu sistem. Serangan ini dilakukan dengan menyisipkan kode SQL berbahaya ke dalam formulir input di situs

web yang tidak memiliki validasi kuat. Jika berhasil, peretas dapat mengakses, mengubah, atau menghapus data dalam basis data yang ditargetkan. *SQL Injection* sering digunakan untuk mencuri informasi sensitif, seperti data pelanggan atau informasi keuangan yang tersimpan dalam sistem (Pavur & Hutchings, 2020).

Di era digital yang semakin terkoneksi, *Internet of Things* (IoT) juga menjadi target utama serangan siber. Banyak perangkat IoT seperti kamera keamanan, *smart home devices*, dan perangkat medis, memiliki tingkat keamanan rendah dan sering menggunakan kata sandi bawaan yang mudah ditebak. Serangan terhadap IoT dapat mendukung peretas mengambil alih kendali perangkat, mengakses data pengguna, atau menjadikan perangkat tersebut bagian dari *botnet* melancarkan serangan DDoS skala besar (Kumar et al., 2021).

Dengan berbagai jenis serangan yang semakin kompleks dan canggih, upaya perlindungan jaringan komputer harus terus diperbarui dan ditingkatkan. Organisasi perlu menerapkan strategi keamanan yang mencakup penggunaan *firewall*, enkripsi data, sistem deteksi intrusi, serta pelatihan kesadaran keamanan bagi pengguna. Memahami pola dan teknik serangan yang berkembang menjadi langkah awal dalam membangun pertahanan yang lebih kuat terhadap ancaman siber.

C. TEKNIK DAN TEKNOLOGI KEAMANAN JARINGAN

Keamanan jaringan komputer merupakan aspek yang sangat krusial dalam era digital masa kini. Kemajuan teknologi informasi secara cepat menaikkan ketergantungan individu, organisasi, dan pemerintah pada jaringan komputer untuk komunikasi, transaksi keuangan, maupun penyimpanan data sensitif. Namun kemajuan ini juga diiringi ancaman siber yang semakin kompleks dan canggih. Untuk mengatasi ancaman tersebut, diperlukan teknik dan teknologi keamanan jaringan yang efektif guna melindungi infrastruktur digital dari serangan yang merusak atau mencuri informasi penting.

Teknologi pokok pada keamanan jaringan adalah *firewall* dengan fungsi menjadi penghambat antara jaringan internal secara aman dengan jaringan eksternal yang belum terpercaya semisal internet. *Firewall* dapat dikonfigurasi memfilter lalu lintas data berdasarkan aturan yang ditetapkan sehingga hanya paket data yang memenuhi kriteria tertentu yang diizinkan masuk atau keluar dari jaringan. *Firewall* modern terdiri dari berbagai jenis seperti *packet-filtering firewall*, *stateful inspection firewall*, dan *next-generation firewall* (NGFW) yang menawarkan perlindungan lebih canggih dengan fitur tambahan seperti deteksi ancaman berbasis kecerdasan buatan dan analisis lalu lintas jaringan secara mendalam.

Sistem deteksi dan pencegahan intrusi (*Intrusion Detection System*/IDS serta *Intrusion Prevention System*/IPS) juga merupakan

komponen penting dalam keamanan jaringan. IDS mempunyai fungsi melakukan deteksi kegiatan mencurigakan atau serangan pada jaringan dan memberikan peringatan kepada administrator, sementara IPS selain melakukan deteksi, juga mencegah serangan melalui pemblokiran lalu lintas berbahaya sebelum mencapai target. IDS dan IPS bekerja dengan metode berbasis tanda (*signature-based detection*) yang mengidentifikasi ancaman berdasar pola serangan yang dikenal, serta metode berbasis anomali (*anomaly-based detection*) yang mendeteksi aktivitas tidak biasa dalam jaringan yang mengindikasikan serangan baru (H. Nguyen et al., 2022).

Enkripsi juga berperan fundamental menjaga kerahasiaan dan integritas data yang ditransmisikan melalui jaringan. Dengan menerapkan teknik enkripsi, data ditransformasikan dalam format yang tak bisa dibaca tanpa kunci dekripsi yang sesuai. Protokol enkripsi yang umum dipakai dalam jaringan adalah *Secure Sockets Layer* (SSL) serta *Transport Layer Security* (TLS), yang melakukan pengamanan komunikasi *server* dengan klien semisal dalam transaksi perbankan dan *e-commerce*. Algoritma enkripsi *Advanced Encryption Standard* (AES) dan *Rivest-Shamir-Adleman* (RSA) digunakan luas dalam memberi perlindungan data atas akses ilegal.

Teknologi *Virtual Private Network* (VPN) juga lazim dipakai dalam menaikkan keamanan jaringan dengan cara mengenkripsi koneksi antara perangkat pengguna dan *server* sehingga data yang dikirimkan melalui jaringan publik tetap terlindungi. VPN memungkinkan pengguna untuk mengakses jaringan pribadi dengan

aman dari lokasi mana pun, menjadikannya solusi ideal bagi pekerja jarak jauh atau organisasi yang membutuhkan akses terenkripsi ke sumber daya internal. Beberapa protokol yang digunakan dalam VPN meliputi IPSec (*Internet Protocol Security*), *OpenVPN*, dan *WireGuard* yang masing-masing menawarkan tingkat keamanan berbeda sesuai kebutuhan (López et al., 2019).

Dalam konteks perlindungan dari *malware*, teknologi antivirus dan anti*malware* sangat penting untuk mendeteksi, mencegah, dan menghapus piranti lunak berbahaya yang bisa mengacaukan sistem ataupun mencuri data. Perangkat lunak ini bekerja dengan berbagai metode seperti pemindaian berbasis tanda yang membandingkan file dengan *database malware* yang sudah dikenal, serta pemindaian heuristik yang mengidentifikasi pola perilaku mencurigakan yang mengindikasikan adanya ancaman baru. Teknologi *sandboxing* juga digunakan dalam solusi keamanan modern di mana file atau program yang mencurigakan dijalankan dalam lingkungan terisolasi untuk menganalisis apakah file tersebut berbahaya sebelum dieksekusi dalam sistem utama (Alotaibi et al., 2021).

Keamanan jaringan juga ditingkatkan dengan teknologi segregasi jaringan dan segmentasi mikro (*micro-segmentation*). Dengan konsep ini jaringan dibagi menjadi beberapa segmen lebih kecil yang masing-masing memiliki aturan akses ketat. Jika satu segmen jaringan dikompromikan oleh serangan, dampaknya dapat diminimalkan karena segmen lainnya tetap terlindungi. Teknologi ini sangat berguna dalam lingkungan *cloud* dan data *center* di mana

banyak layanan dan aplikasi berjalan secara bersamaan dan memerlukan perlindungan berbeda-beda (Sharma & Jain, 2020).

Keamanan berbasiskan kecerdasan buatan (AI) serta pembelajaran mesin (ML) semakin banyak diadopsi dalam strategi pertahanan jaringan modern. AI dan ML dapat digunakan untuk mendeteksi pola serangan baru secara otomatis dengan menganalisis data lalu lintas jaringan dalam jumlah besar. Dengan model pembelajaran berbasis anomali, sistem keamanan mengidentifikasi aktivitas mencurigakan yang tidak sesuai dengan pola normal dan secara proaktif mencegah serangan sebelum menyebabkan kerusakan besar. Contoh penerapan AI dalam keamanan jaringan adalah sistem yang dapat mengenali pola serangan *phishing* secara otomatis dengan menganalisis e-mail atau situs web berbahaya (Hu et al., 2023).

Untuk meningkatkan otentikasi dan akses aman ke sistem, teknologi *Multi-Factor Authentication* (MFA) semakin banyak digunakan. MFA mewajibkan pemakai memberi lebih dari satu format verifikasi identitas untuk mendapat akses. Faktor yang digunakan MFA dapat berupa kombinasi dari sesuatu yang dikenal pengguna (kata sandi), sesuatu yang dipunyai pengguna (token ataupun *smartphone*), serta sesuatu yang melekat di pengguna (sidik jari ataupun pengenalan muka). Dengan menerapkan MFA, risiko akses ilegal akibat kredensial yang dicuri dapat dikurangi signifikan (Reddy et al., 2022).

Teknologi terbaru yang semakin banyak dipakai keamanan jaringan adalah *blockchain* yang menawarkan solusi keamanan berbasis desentralisasi. Dengan struktur *ledger* yang tidak dapat diubah dan sistem verifikasi berbasis kriptografi, *blockchain* dapat digunakan untuk meningkatkan integritas data, terutama dalam transaksi digital, penyimpanan data, dan sistem identitas terdesentralisasi. *Blockchain* mulai diterapkan dalam berbagai solusi keamanan jaringan termasuk dalam mengamankan komunikasi antar perangkat IoT dan memastikan bahwa data yang disimpan dalam sistem *cloud* tak bisa dimanipulasi pihak ilegal (Dinh et al., 2021).

Dengan semakin peningkatan ancaman siber, teknik dan teknologi keamanan jaringan harus selalu diperbarui menghadapi tantangan baru. Implementasi strategi keamanan komprehensif dari pemakaian *firewall*, IDS/IPS, enkripsi, hingga pemanfaatan AI dan *blockchain*, menjadi kunci utama menjaga keamanan jaringan komputer.

D. *BEST PRACTICES* DALAM KEAMANAN JARINGAN

Keamanan jaringan komputer adalah aspek sangat krusial dalam ekosistem teknologi informasi modern. Dengan peningkatan ancaman siber, organisasi dan individu harus mengadopsi pendekatan komprehensif guna melindungi infrastruktur digital dari serangan yang menyebabkan pencurian data, gangguan layanan, serta kerusakan sistem. Untuk memastikan keamanan

jaringan yang optimal, diperlukan serangkaian praktik terbaik (*best practices*) yang mencakup aspek teknis, kebijakan, serta kesadaran pengguna.

Praktik terbaik keamanan jaringan adalah penerapan kebijakan keamanan kuat. Kebijakan ini mencakup pedoman penggunaan jaringan, prosedur akses, serta aturan terkait manajemen identitas dan autentikasi. Setiap organisasi harus memiliki dokumen kebijakan keamanan yang jelas dan diperbarui secara berkala untuk menyesuaikan perkembangan ancaman siber terbaru. Kebijakan ini juga harus mencakup prosedur penanganan insiden keamanan agar menjamin tanggapan cepat serta efektif pada serangan yang terjadi (T. Johnson et al., 2021).

Manajemen akses berbasis prinsip *least privilege* juga merupakan langkah penting melindungi jaringan dari ancaman internal maupun eksternal. Konsep ini mengharuskan setiap pengguna atau sistem hanya diberikan akses yang benar-benar diperlukan menjalankan tugasnya. Dengan membatasi hak akses secara ketat, organisasi dapat mengurangi risiko eskalasi hak istimewa yang dapat digunakan peretas untuk mendapatkan kendali penuh sistem (Brown & Wilson, 2022). Implementasi teknologi seperti *Role-Based Access Control* (RBAC) dan *Multi-Factor Authentication* (MFA) juga dapat memperkuat strategi manajemen akses dalam jaringan.

Pembaruan perangkat lunak dan *patching* berkala merupakan langkah krusial mengurangi risiko eksploitasi celah keamanan. Banyak serangan siber terjadi karena sistem yang tidak diperbarui sehingga rentan terhadap eksploitasi peretas. Administrator jaringan harus memastikan bahwa sistem operasi, aplikasi, dan perangkat jaringan selalu dalam kondisi terbaru dengan menerapkan pembaruan keamanan secara berkala (L. Nguyen & Lee, 2020). Penggunaan sistem manajemen *patch* otomatis membantu organisasi memastikan semua piranti tetap terlindungi dari ancaman terbaru.

Keamanan *endpoint* juga menjadi aspek penting strategi perlindungan jaringan. Dengan semakin banyaknya perangkat yang terhubung ke jaringan, seperti laptop, *smartphone*, dan perangkat IoT, setiap *endpoint* harus dilindungi dengan solusi keamanan kuat, termasuk antivirus, anti*malware*, dan deteksi ancaman berbasis AI. Kebijakan *Bring Your Own Device* (BYOD) harus diatur ketat untuk memastikan perangkat pribadi yang digunakan dalam lingkungan kerja tidak menjadi titik masuk serangan siber (Patel et al., 2023).

Selain melindungi perangkat penerapan enkripsi data juga menjadi langkah esensial menjaga kerahasiaan informasi yang dikirim melalui jaringan. Data yang tidak dienkripsi berisiko tinggi disadap pihak tidak bertanggung jawab, terutama dalam komunikasi melalui internet. Penggunaan protokol *Transport Layer Security* (TLS) dan *Virtual Private Network* (VPN) membantu melindungi data saat

dalam transmisi. Organisasi juga harus mempertimbangkan implementasi *end-to-end encryption* layanan komunikasi internal untuk meningkatkan tingkat keamanan (Miller & Singh, 2021).

Segmentasi jaringan juga menjadi salah satu praktik terbaik dalam keamanan jaringan. Dengan membagi jaringan menjadi beberapa segmen berdasarkan fungsi atau tingkat sensitivitas data, organisasi dapat mengurangi risiko penyebaran serangan. Jika satu segmen jaringan disusupi, dampaknya dapat diminimalkan karena akses ke segmen lain dibatasi secara ketat. *Zero Trust Architecture* (ZTA) merupakan konsep terbaru dalam segmentasi jaringan yang mengharuskan setiap permintaan akses diverifikasi sebelum diizinkan masuk ke sistem, meskipun berasal dari dalam jaringan organisasi (Taylor et al., 2022).

Kesadaran dan pelatihan keamanan bagi pengguna berperan sangatlah krusial pula untuk mempertahankan keamanan jaringan. Banyak serangan siber yang berhasil karena adanya kelalaian manusia, semisal melakukan klik tautan berbahaya ataupun memakai kata sandi yang rentan. Organisasi harus secara rutin mengadakan pelatihan keamanan siber bagi karyawan guna meningkatkan pemahaman terhadap ancaman seperti *phishing*, *social engineering*, dan serangan berbasis *malware*. Pelatihan ini dapat dilakukan melalui simulasi serangan dan penyuluhan mengenai praktik terbaik dalam keamanan digital (Henderson & Clark, 2023).

Monitoring dan deteksi ancaman *real-time* merupakan langkah penting lainnya dalam strategi keamanan jaringan. Organisasi harus menggunakan solusi seperti *Intrusion Detection System* (IDS) dan *Security Information and Event Management* (SIEM) untuk melakukan analisis lalu lintas jaringan serta deteksi aktivitas mencurigakan secara cepat. Penggunaan AI dan *Machine Learning* dalam analisis ancaman siber semakin populer karena kemampuan dalam mengidentifikasi pola serangan baru secara otomatis dan memberikan respons proaktif sebelum serangan menyebabkan dampak lebih besar (Garcia et al., 2021).

Penerapan kebijakan cadangan data (*backup*) yang teratur juga menjadi bagian penting strategi keamanan jaringan. Dengan cadangan data yang tersimpan di lokasi aman, organisasi dapat dengan cepat memulihkan sistem jika terjadi serangan *ransomware* atau kegagalan sistem. *Backup* data harus dilakukan secara berkala dan disimpan dalam beberapa lokasi yang berbeda termasuk *cloud storage* dan perangkat fisik yang tidak terhubung langsung ke jaringan utama. Penerapan strategi 3-2-1 *Backup* (tiga salinan data, dua media penyimpanan berbeda, satu lokasi *offsite*) merupakan pendekatan yang direkomendasikan oleh para ahli keamanan siber (Anderson & Reed, 2020).

Seiring berkembangnya teknologi dan semakin kompleksnya ancaman siber, organisasi dan individu harus terus menerapkan serta memperbarui praktik terbaik dalam keamanan jaringan. Pendekatan yang mencakup kombinasi antara kebijakan, teknologi,

serta kesadaran pengguna akan memastikan bahwa infrastruktur digital tetap aman dari berbagai ancaman yang dapat merusak atau mencuri informasi sensitif. Dengan menerapkan *best practices* ini secara konsisten, keamanan jaringan dapat terus ditingkatkan dan risiko serangan siber dapat diminimalkan secara signifikan.

DAFTAR PUSTAKA

Abdullah, D. (2015). Jaringan Komputer: Data Link, Network & Issue. Universitas Malikussaleh Press (Unimal Press).

Achmad, A. D., Achmad, A., & Anggreni, D. R. (2016). Perancangan antena mikrotrip untuk repeater jaringan 4G yang beroperasi pada frekuensi 1800 Mhz. Prosiding Seminar Teknik Elektro & Informatika.

Agustini, K. (2021). Komunikasi Data dan Jaringan Komputer serta Analoginya dalam Konsep Subak. PT. RajaGrafindo Persada.

Ahmad Yani. (2008). Panduan Membangun Jaringan Komputer (Cetakan Ke). Penerbit PT Kawan Pustaka.

Ahmad, S. (2023). Types of computer network. https://www.slideshare.net/Shahbaz15/types-of-computer-network-104202832

Ahmed, F., Butt, Z. U. A., & Siddiqui, U. A. (2016). MPLS based VPN Implementation in a Corporate Environment. In Journal of Information Technology & Software Engineering (Vol. 6, Issue 5). OMICS Publishing Group. https://doi.org/10.4172/2165-7866.1000193

Alazab, M., Tang, M., & Cross, J. (2022). Evolution of ransomware attacks: Strategies, impact, and countermeasures. Journal of Cybersecurity Research, 18(3), 215–230.

Al-Hadhrami, A., Gupta, R., & Singh, P. (2023). Security challenges in IoT networks: An overview and future directions. Journal of Cybersecurity Research, 15(2), 134–150.

Alotaibi, S., Almomani, A., & Salah, K. (2021). Advanced malware detection using machine learning and sandboxing techniques. Cybersecurity Journal, 19(2), 132–150.

Ambedkar, B. (2015). Fundamentals of Computer Networking (FCN) PGDCA 201 BLOCK 1: NETWORKING CONCEPT.

Anderson, J., & Reed, M. (2020). Cybersecurity strategies for data protection and backup management. Journal of Information Security, 18(3), 155–172.

Arius, D. (2020). Komunikasi Data. Penerbit Andi.

Bilge, L., & Dumitras, T. (2019). Before we knew it: An empirical study of zero-day attacks in the real world. IEEE Transactions on Security and Privacy, 16(2), 50–65.

Brown, K., & Wilson, L. (2022). Role-Based Access Control: Enhancing network security through access management. Cybersecurity Advances, 22(1), 77–90.

Brown, K., Wilson, T., & Carter, J. (2024). Implementing Zero Trust Architecture for enhanced network security. Cybersecurity & Digital Protection Journal, 19(1), 45–62.

Campbell-Kelly, M., & Garcia-Swartz, D. D. (2013). The History of the Internet: The Missing Narratives. In Journal of Information Technology (Vol. 28, Issue 1). https://doi.org/10.1057/jit.2013.4

Cisco Networking Academy. (2020). CCNAv7: Introduction to Networks (ITN) Companion Guide). Cisco Press.

Cisco System, I. (2003). Internetworking Technologies Handbook, Fourth Edition. In Review Literature And Arts Of The Americas.

Comer, D. E. (2015). Internetworking with TCP/IP Volume one. https://www.amazon.com/Internetworking-TCP-one-Douglas-Comer/dp/9332550107/ref=sr_1_3?crid=3Q4SMQVWLU01Y&dib=eyJ2IjoiMSJ9.j4kElVoyS_VyQq-PRqz4wHZcY53_bS9R-nP-ZH2mjaLkkLrQ0IuyLBFKR-JfxzmKo7zQPh215RpYUZS-gSTStNMVfo34RZNjz48mzdKDJNwVtHro1i-HIhXx-3nka0jagWEBj

Crystal Panek. (2020). Networking Fundamentals (1st Editio). John Wiley & Sons, Inc.

Dinh, T., Wang, L., & Zhang, Y. (2021). Blockchain-based security solutions for IoT networks. Journal of Emerging Technologies in Security, 22(4), 198–215.

Edition, E., Systems, O., Edition, S., & Communications, B. D. (2011). the William Stallings Books on Computer Data and Computer Communications , Eighth Edition. In Network (Vol. 139, Issue 3). https://doi.org/10.1007/11935070

Forouzan, B. (2006). Data Communications and Networking (McGraw-Hill Forouzan Networking) (4th ed.). McGraw-Hill Science/Engineering/Math. https://www.amazon.com/Data-Communications-Networking-McGraw-Hill-Forouzan/dp/0073250325

Forouzan, B. A. (2007). Data Communications and Networking (4th ed.). McGraw-Hill.

Forouzan, B. A. (2013). TCP/IP Protocol Suite (4th ed.). McGraw Hill. https://www.amazon.com/Protocol-Suite-Mcgraw-hill-Forouzan-Networking/dp/0073376043

Garcia, M., Smith, R., & Patel, S. (2021). AI-powered threat detection in modern networks. Journal of Cybersecurity Research, 19(4), 200–217.

Henderson, J., & Clark, P. (2023). The importance of cybersecurity training in organizational security. International Journal of Information Security Awareness, 25(2), 98–115.

Hu, Q., Wang, H., & Liu, M. (2023). AI-driven phishing detection: Methods and challenges. Cyber Threat Intelligence Review, 20(3), 112–130.

Huawei Technologies Co, L. (2020). HCIA-Datacom V1.0 Training Material.pdf. Huawei Technologies Co, Ltd.

Huawei Technologies Co., Ltd. (2023). Data Communications and Network Technologies. In Data Communications and Network Technologies. https://doi.org/10.1007/978-981-19-3029-4

Irawati, I. D., Yovita, L. V., & Wibowo, T. A. (2018). Jaringan Komputer dan Data Lanjut. Deepublish.

Jalil, M. A. B. (2022). A Brief Overview: Computer Network Based on Physical and Logical Topology. In International Journal for Research in Applied Science and Engineering Technology (Vol. 10, Issue 3, p. 1154). International Journal for Research in Applied Science and Engineering Technology (IJRASET). https://doi.org/10.22214/ijraset.2022.40833

Jennings, C., & Gurbani, V. (2008). The Internet Assigned Number Authority (IANA) tel Uniform Resource Identifier (URI) Parameter Registry. In Network Working Group.

Jiang, M., Yang, C., & Liu, X. (2021). A deep learning approach for DDoS attack detection. Cybersecurity & AI Journal, 15(4), 103–120.

Johnson, M., Roberts, L., & Chang, H. (2020). The role of human factors in cybersecurity breaches. Information Security Journal, 13(4), 289–305.

Johnson, T., Cooper, B., & Lee, H. (2021). The role of security policies in mitigating cyber threats. Journal of Network Security & Policy, 17(2), 120–138.

Jumadi M.Parenreng, Abdul Wahid, Sanatang, & A.Yusmalasari. (2022). Pengantar Jaringan Komunikasi Nirkabel (Indika (ed.); Pertama). Zahira Media Publisher.

Kshetri, N. (2021). Man-in-the-middle attacks and countermeasures in modern networks. Journal of Information Security, 14(2), 147–161.

Kumar, S., & Shukla, R. (2021). Confidentiality, Integrity, and Availability: The foundation of cybersecurity. Journal of Network Security, 14(3), 89–105.

Kumar, S., Patel, P., & Jha, A. (2021). Securing the Internet of Things: Challenges and future directions. IoT Security Journal, 12(1), 89–105.

Kurose, J. F., & Ross, K. W. (2012). Computer Networking: A Top-Down Approach. Pearson Education. https://www.amazon.com/Computer-Networking-James-Kurose-Keith/dp/0273768964

Kurose, J. F., & Ross, K. W. (2017). Computer Networking: A Top-Down Approach (7th ed.). Pearson.

Kuusisto, F. (2015). IP addresses. XRDS: Crossroads, The ACM Magazine for Students, 22(2). https://doi.org/10.1145/2859010

Lammle, T. (2016). CCNA Routing and Switching Complete Study Guide. In Cisco Certified Network Associate.

López, P., Suárez, F., & Martínez, R. (2019). VPN security and performance analysis: A comparative study. Journal of Network Security & Cryptography, 15(1), 75–89.

Madcoms. (2010). Sistem Jaringan Komputer untuk Pemula. Penerbit ANDI Ygyakarta.

Miller, D., & Singh, A. (2021). Encryption techniques for securing data in transit. Cybersecurity & Encryption Review, 20(1), 89–104.

Mishra, P., Verma, S., & Dutta, B. (2019). Encryption techniques for data security: A comparative analysis. International Journal of Computer Science & Security, 11(2), 200–215.

Muhammad Haris, Hevlie Winda Nazry S, Okvi Nugroho, Farid Akbar Siregar, & Rizaldy Khair. (2025). Komunikasi Data & Jaringan Komputer (Fatma Sari Hutagulung (ed.); Pertama).

Mutoffar, M. M., Gunawan, A. A. N., Negara, A. A. N. F. C., Gunantara, N., & Musril, H. A. (2024). Jaringan Komputer: Konsep dan Aplikasi Modern (Vol. 1, Issue June).

Nguyen, H., Tran, P., & Chen, J. (2022). Intrusion detection and prevention systems: Trends and future directions. Cybersecurity Advances Journal, 17(1), 89–105.

Nguyen, L., & Lee, H. (2020). Patch management strategies for enterprise security. Information Security Management Journal, 15(3), 65–79.

Open-E, I. (2023). Solutions for data storage management and centralization. https://www.open-

e.com/solutions/article/solutions-for-data-storage-management-and-centralization/

Patel, D. (2024). A Research Paper on Basic of Computer Network. In International Journal for Research in Applied Science and Engineering Technology (Vol. 12, Issue 2). https://doi.org/10.22214/ijraset.2024.58481

Patel, R., Kumar, N., & Sharma, V. (2023). Endpoint security in modern organizations: Challenges and solutions. Cyber Defense Journal, 28(1), 135–152.

Pavur, J., & Hutchings, A. (2020). The role of SQL injection in cybercrime: Trends and mitigation strategies. International Journal of Network Security, 17(2), 121–136.

Postel, J. (1981). RFC 791: Internet Protocol. In Ietf Rfc 791.

Pujowati, S., & Harianto, B. B. (2021). Pengenalan Dasar Jaringan Komputer. Penerbit Pustaka Rumah C1nta.

Purbawanto, S. (2021). Media Transmisi Telekomunikasi. Deepublish.

Rahman, A., Islam, M. J., Islam, M., Aziz, A., Kundu, D., Sazzad, S., Karim, Md. R., Hasan, M., Rahman, Z., Elnaffar, S., & Band, S. S. (2022). Enhancing Data Security for Cloud Computing Applications through Distributed Blockchain-based SDN Architecture in IoT Networks. In arXiv (Cornell University). Cornell University. https://doi.org/10.48550/arXiv.2211.

Rahman, A., Lee, C., & Kim, D. (2021). Effectiveness of cybersecurity training programs in reducing human errors. Journal of Information Security & Applications, 17(2), 99–115.

Reddy, P., Krishna, R., & Mukherjee, S. (2022). Multi-factor authentication: Enhancing security in cloud computing. International Journal of Secure Computing, 21(2), 150–165.

Ryan, N. G. (2018). Basic Computer Networking. XP Solution Surabaya.

Salamatian, L., Arnold, T., Cunha, Í., Zhu, J., Zhang, Y., Katz-Bassett, E., & Calder, M. (2023). Who Squats IPv4 Addresses? In Computer Communication Review (Vol. 53, Issue 1). https://doi.org/10.1145/3594255.3594260

Scarfone, K., & Hoffman, P. (2009). Guidelines on Firewalls and Firewall Policy. NIST Special Publication.

Setiawan, A. A., Syaiful, & Arifin, Z. (2024). Buku Ajar Jaringan dan Komunikasi Data. Kaizen Media Publishing.

Sharma, N., & Jain, S. (2020). Network micro-segmentation for enhanced security in data centers. Journal of Computer Science & Security, 16(4), 97–120.

Siddiqui, A. (2017). RFC 8200 - IPv6 has been standardized | Internet Society. Internet Society.

Singh, R., & Sharma, T. (2022). Regulatory compliance and its impact on network security. Global Journal of Cyber Law & Policy, 16(1), 78–94.

Stallings, W. (2013). Data and Computer Communications (10th ed.). Pearson.

Steinke, S. (2020). The TCP/IP Protocol Suite. In Network Tutorial. https://doi.org/10.1201/9781482280876-41

Sudeep, J., Girish, S. C., Raghavendra, K., G, P. K., Srinidhi, H. R., & Anilkumar, K. M. (2022). Introduction to Cyber Security. In

Advances in information security, privacy, and ethics book series. https://doi.org/10.4018/978-1-6684-3991-3.ch001

Sunkari, S. (2021). A Brief Study on Data Communication and Computer Networks. In SSRN Electronic Journal. RELX Group (Netherlands). https://doi.org/10.2139/ssrn.3904826

Syafrizal, M. (2020). Pengantar Jaringan Komputer - Google Books. In CV. Andi Offset (Penerbit Andi).

Syafrizal, M., & Yogyakarta, U. A. (2020). Pengantar Jaringan Komputer. Penerbit Andi.

Tanenbaum, A. S., & Wetherall, D. J. (2011). Computer Networks (5th ed.). Pearson.

Tanenbaum, A., & Wetherall, D. (2010). Computer Networks (5th ed.). Pearson. https://www.amazon.com/Computer-Networks-5th-Andrew-Tanenbaum/dp/0132126958

Taylor, B., Adams, C., & Wilson, D. (2022). Zero Trust Architecture: A new paradigm in network security. Network Security Innovations, 23(3), 188–205.

Verma, S., & Das, A. (2020). Phishing attacks: Methods, countermeasures, and prevention techniques. Cybersecurity & Digital Forensics Journal, 14(3), 189–204.

Viehland, D., & Zhao, F. (2010). The Future of Personal Area Networks in a Ubiquitous Computing World. In International Journal of Advanced Pervasive and Ubiquitous Computing (Vol. 2, Issue 2, p. 30). IGI Global. https://doi.org/10.4018/japuc.-2010040102

Wibowo, S. H. (2023). Jaringan Komputer & Komunikasi Data. Deepublish.

Wibowo, S. H., Andesti, C. L., Suleman, Hendarsyah, D., Santoso, N. A., Dewantara, R., Wahidin, A. J., Santoso, L. W., Sihombing, F. A., & Saputra, H. (2022). Teknologi Jaringan Nirkabel (M. P. Ariyanto & S. P. Tri Putri Wahyuni (eds.); Pertama). PT GLOBAL EKSEKUTIF TEKNOLOGI.

Yeşil, F. (2023). Network Protocols: A Comprehensive Guide. https://medium.com/@fahriiyesill/demystifying-networking-protocols-a-comprehensive-guide-171c81ac07ae

TENTANG PENULIS

Penulis Bagian 1:

Ir.Ida Bagus Kerthyayana Manuaba, S.T., Ph.D

Seorang penulis, akademisi, peneliti, serta dosen pengajar pada Computer Science Departement, School of Computing and Creative Arts – Bina Nusantara (BINUS) University – Pada Program International. Penulis menamatkan pendidikan program Sarjana (S1 - Sarjana Teknik) di Universitas Udayana, Bali, pada Jurusan Teknik Elektro, dengan Penjurusan Sistem Komputer dan Informatika pada tahun 2009, serta telah menyelesaikan program Doktoral (Ph.D in Computer Science) di Australian National University pada tahun 2014, Canberra, Australia. Pada tahun 2024, Penulis juga menyelesaikan pendidikan profesi Insinyur (dengan gelar Ir.) pada universitas Atma Jaya Jakarta.

Penulis Bagian 2 :

Prof. Dr. Fahrul Agus, S.Si., M.T., MTA., MCE.

Guru Besar dengan keahlian Sistem Informasi Lingkungan-Kehutanan ini merupakan dosen tetap pada Program Studi Informatika Fakultas Teknik Universitas Mulawarman Samarinda. Saat ini juga aktif sebagai praktisi pada bidang pengembangan *E-Government* kabupaten di Kaltim. Lahir di Tenggarong-Kutai Kartanegara, 26 September 1969. Anak ketiga dari empat bersaudara, pasangan Baharuddin (alm) dan Bahariah (almh). Menamatkan pendidikan Program Sarjana (S1) di Statistika-IPB Bogor (S.Si), Program Magister (S2) di Teknik

Informatika-ITB Bandung (M.T) dan Program Doktor Ilmu Kehutanan Universitas Mulawarman. Pemegang Sertifikat kompetensi global dari Microsoft Technology Associate (MTA), Microsoft Certified Educator (MCE) dan AWS Academy Graduate. Berbagai penelitian telah dilakukan di bidang Sistem Informasi Geografis dan pengalahan data spasial serta dipublikasikan di jurnal/prosiding internasional bereputasi. Profil penulis dapat diakses pada ID-SCOPUS 56596806400, ID-SINTA 258424 dan ID-ORCID di https://orcid.org/0000-0003-2983-137X.

Penulis Bagian 3:

Ir. I Made Satrya Ramayu, S.Kom.,M.Kom

Seorang penulis dan dosen tetap Program Studi S1 Bisnis Digital, Institut Desain dan Bisnis Bali. Penulis mendapatkan gelar Sarjana Komputer pada tahun 2012 dari Institut Teknologi Dan Bisnis STIKOM Bali dan gelar Magister Komputer pada tahun 2018 dari Universitas Pendidikan Ganesha pada tahun 2018. Penulis berfokus pada bidang Pemrograman, Bisnis, Sistem Informasi dan Data Science. Beberapa mata kuliah yang pernah diampu oleh penulis adalah Pemrograman Dasar, Komputer Grafis, Interaksi Manusia Komputer, Desain Website, Desain Web, Analisis Data Bisnis dan Algoritma Pemrograman.

Penulis Bagian 4:

Vian Ardiyansyah Saputra, S.ST., M.Kom., adalah seorang profesional di bidang IT Infrastructure & Network dengan pengalaman luas dalam manajemen jaringan komputer, keamanan sistem, serta administrasi server. Beliau menyelesaikan pendidikan Diploma IV di Politeknik Negeri Semarang dengan fokus pada Teknik Telekomunikasi, kemudian melanjutkan studi Magister di Universitas Amikom Yogyakarta dalam bidang Teknologi Informasi dengan spesialisasi Technopreneurship. Saat ini, beliau aktif sebagai pengajar di Politeknik Astra Cikarang, dengan berbagai sertifikasi profesional di bidang jaringan dan keamanan sistem, seperti MikroTik Academy Trainer, Certified Network Administrator BNSP, EngGenius Certified Network Specialist, MikroTik Certified Engineer dan Omada Certified Network Administrator beliau terus berkontribusi dalam dunia IT, baik di industri maupun akademik. Selain itu, beliau juga aktif dalam penelitian dan publikasi ilmiah, khususnya di bidang jaringan nirkabel, keamanan sistem, serta implementasi teknologi modern dalam infrastruktur IT, dengan beberapa karya yang telah dipublikasikan di jurnal nasional.

Penulis Bagian 5:

Andy Victor Pakpahan, MT.

Seorang Penulis dan Dosen Prodi Teknik Informatika Institut Digital Ekonomi LPKIA Bandung. Lahir di Aek Raja, 12 Maret 1981, Tapanuli Utara Sumatera Utara. Penulis merupakan anak ketiga dari lima bersaudara dari pasangan bapak Syarifuddin Pakpahan dan Ibu Rospita Rajagukguk. Ia menamatkan

pendidikan program Sarjana (S1) di STMIK LPKIA Bandung prodi Teknik Informatika dan menyelesaikan program Pasca Sarjana (S2) di Universitas Telkom prodi Teknik Informatika. Beberapa sertifikasi kompetensi industri internasional yang dimiliki adalah *Microsoft Certified Professional (MCP), Microsoft Office Specialist (MOS), Mikrotik Certified Network Associate (MTCNA), Huawei Certified ICT Associate (HCIA)-Datacom, Huawei Certified ICT Associate (HCIA)-Cloud Service, dan Huawei Certified Academy Instructor (HCAI).* Sampai dengan saat ini, juga masih aktif sebagai instruktur di *Cisco Networking Academy* dan *Huawei Talent ICT Academy*. Berbagai Penelitian dan Pengabdian kepada Masyarakat sebagai narasumber/instruktur telah dilakukan baik pada instansi pemerintahan maupun instansi swasta dan dipublikasikan (Buku ber-ISBN & Artikel Ilmiah) pada Jurnal internasional bereputasi SCOPUS & Jurnal Nasional terakreditasi.

Penulis Bagian 6:

Julia R.Skawanti, S.Kom,M.Kom.

Dosen Tetap Prodi Perhotelan di Sekolah Tinggi Pariwisata Bogor, mengajar mata kuliah *Computer Application, Digital Marketing, Hotel Information System, Techology Information System*. Lahir dan besar di Bandung, menamatkan pendidikan Program Sarjana (S1) di STIMIK Indonesia Mandiri Bandung tahun 2006 pada Prodi Sistem Informasi dan Program Magister-S2 pada STIMIK LIKMI Bandung tahun 2013. Berbagai penelitian yang telah dilakukan dan dipublikasi Jurnal Nasional terindeks Sinta (tercantum di Google Scholar) serta menghasilkan beberapa buku antara lain Buku Ajar Pengantar Teknologi Informasi, The Amizing Of Corel Draw: Belajar Mudah Desain Grafis, Panduan Penulisan Karya Ilmiah Untuk Mahasiswa

Hospitality And Tourism, Basic English Grammar: Teori, Contoh & Penerapan, Buku Ajar Dasar Dasar Desain Grafis, dan lain-Lain.

Penulis Bagian 7:

Loso Judijanto adalah peneliti yang bekerja pada lembaga penelitian **IPOSS Jakarta**. Penulis dilahirkan di Magetan pada tanggal 19 Januari 1971. Penulis menamatkan pendidikan *Master of Statistics* di *the University of New South Wales*, Sydney, Australia pada tahun 1998 dengan dukungan beasiswa ADCOS (*Australian Development Cooperation Scholarship*) dari Australia. Sebelumnya penulis menyelesaikan Magister Manajemen di Universitas Indonesia pada tahun 1995 dengan dukungan beasiswa dari Bank Internasional Indonesia. Pendidikan sarjana diselesaikan di Institut Pertanian Bogor pada Jurusan Statistika – FMIPA pada tahun 1993 dengan dukungan beasiswa dari KPS-Pertamina. Penulis menamatkan Pendidikan dasar hingga SMA di Maospati, Sepanjang karirnya, Penulis pernah ditugaskan untuk menjadi anggota Dewan Komisaris dan/atau Komite Audit pada beberapa perusahaan/lembaga yang bergerak di berbagai sektor antara lain pengelolaan pelabuhan laut, telekomunikasi seluler, perbankan, pengembangan infrastruktur, sekuritas, pembiayaan infrastruktur, perkebunan, pertambangan batu bara, properti dan rekreasi, dan pengelolaan dana perkebunan. Penulis memiliki minat dalam riset di bidang kebijakan publik, ekonomi, keuangan, *human capital*, dan *corporate governance*. Penulis dapat dihubungi melalui e-mail di: losojudijantobumn@gmail.com.

Penerbit :

PT. Sonpedia Publishing Indonesia

Buku Gudang Ilmu, Membaca Solusi Kebodohan, Menulis Cara Terbaik Mengikat Ilmu. Everyday New Books

Redaksi :
Jl. Kenali Jaya No 166
Kota Jambi 36129
Tel +6282177858344
Email: sonpediapublishing@gmail.com
Website: www.sonpedia.com

SONPEDIA
Publishing Indonesia

SERTIFIKAT

PENGHARGAAN

NO:515/BC-SPI/V/2025

Penghargaan Sebesar-besarnya kami berikan kepada

Andy Victor Pakpahan, MT

Atas kontribusinya sebagai Penulis Buku
dengan nomor ISBN : **978-623-514-639-3**
di penerbit Sonpedia Publishing Indonesia dengan judul:
Jaringan Komputer

Jambi, 16 Mei 2025

PERPUSTAKAAN NASIONAL
REPUBLIK INDONESIA

Pimpinan Redaksi

IKAPI
IKATAN PENERBIT INDONESIA