JARINGAN KOMPUTER

Wahyuddin S
Wirawan Istiono
Arief Yanto Rukmana
James Philip
Angga Aditya Permana
Suwito Pomalingo
Johni S Pasaribu
Rudi Sutomo
Danang Haryo Sulaksono
Iwan Adhicandra
Yuniansyah
Amna
Purnawarman Musa
Erick Fernando

GET PRESS INDONESIA

JARINGAN KOMPUTER

Penulis :
Wahyuddin S
Wirawan Istiono
Arief Yanto Rukmana
James Philip
Angga Aditya Permana
Suwito Pomalingo
Johni S Pasaribu
Rudi Sutomo
Danang Haryo Sulaksono
Iwan Adhicandra
Yuniansyah
Amna
Purnawarman Musa
Erick Fernando

ISBN :

Editor : Diana Purnama Sari,. S.E M.E
Penyunting : Tri Putri Wahyuni,S.Pd
Desain Sampul dan Tata Letak : Atyka Trianisa, S.Pd

Penerbit : GET PRESS INDONESIA
Anggota IKAPI No. 033/SBA/2022

Redaksi :
Jln. Palarik Air Pacah No 26 Kel. Air Pacah
Kec. Koto Tangah Kota Padang Sumatera Barat
Website : www. getpress.co.id
Email : adm.getpress@gmail.com

Cetakan pertama, September 2023

KATA PENGANTAR

Segala Puji dan syukur atas kehadirat Allah SWT dalam segala kesempatan. Sholawat beriring salam dan doa kita sampaikan kepada Nabi Muhammad SAW. Alhamdulillah atas Rahmat dan Karunia-Nya penulis telah menyelesaikan Buku Jaringan Komputer ini.

Buku ini membahas Pengantar Jaringan Komputer, Model Referensi OSI dan TCP/IP, Teknologi Jaringan Nirkabel, Infrastruktur Jaringan, Protokol Jaringan, Keamanan Jaringan, Pengalamatan IP dan Subnetting, Jaringan Area Lokal (LAN) dan Jaringan Area Luas (WAN), Virtualisasi Jaringan, Pengelolaan Jaringan, *Cloud Computing* dan Jaringan, *Internet of Things* (IoT) dan Jaringan, Jaringan Sensor dan Aktuator, Penggunaan Jaringan dalam Bisnis.

Proses penulisan buku ini berhasil diselesaikan atas kerjasama tim penulis. Demi kualitas yang lebih baik dan kepuasan para pembaca, saran dan masukan yang membangun dari pembaca sangat kami harapkan.

Penulis ucapkan terima kasih kepada semua pihak yang telah mendukung dalam penyelesaian buku ini. Terutama pihak yang telah membantu terbitnya buku ini dan telah mempercayakan mendorong, dan menginisiasi terbitnya buku ini. Semoga buku ini dapat bermanfaat bagi masyarakat Indonesia.

Padang, September 2023

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB 1
PENGANTAR JARINGAN KOMPUTER

Oleh Wahyuddin S

1.1 Pendahuluan

Jaringan komputer atau jejaring komputer (*computer network*) adalah jaringan telekomunikasi yang memungkinkan komputer dapat saling berkomunikasi melalui pertukaran data. Jaringan komputer mengacu pada perangkat komputer yang terhubung satu sama lain dan dapat bertukar data dan berbagi sumber daya satu sama lain. Perangkat jaringan ini menggunakan sistem aturan yang disebut protokol komunikasi untuk mengirimkan informasi melalui teknologi fisik atau nirkabel. Tujuan dari jaringan komputer adalah untuk memungkinkan setiap bagian dari jaringan komputer meminta dan memberikan layanan (*service*) untuk mencapai tujuannya. Pihak yang meminta/menerima jasa disebut *client* dan pihak yang memberikan/mengirimkan jasa disebut *server*. Desain ini disebut sistem *client-server* dan digunakan di hampir semua aplikasi jaringan komputer (Iskandar et al., 2022).

Dalam beberapa dekade terakhir, perkembangan jaringan komputer telah mengubah dunia dan memberikan dampak besar terhadap perubahan cara berkomunikasi, bekerja dan menjalani kehidupan sehari-hari mulai dari komunikasi secara jarak jauh hingga adanya revolusi internet yang memungkinkan pengguna dapat mengirim pesan dalam sekejap, mengakses file dari mana saja di dunia dan menghubungkan miliaran perangkat untuk dapat bekerja sama. Jaringan komputer telah menjadi jembatan digital yang menghubungkan pikiran, ide, bisnis dan kehidupan masyarakat digital saat ini.

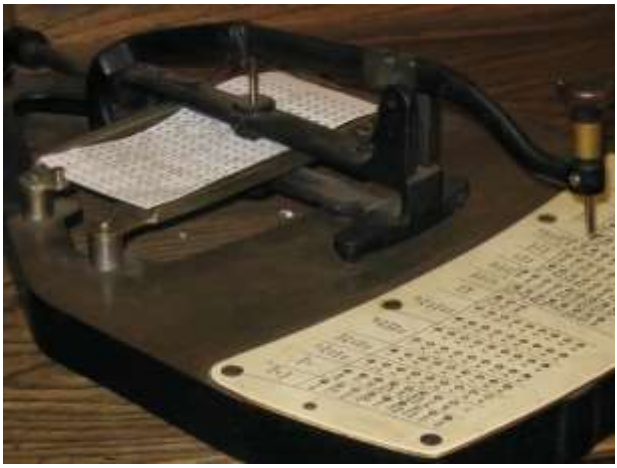
Seiring berjalannya waktu, jaringan komputer telah mengalami perubahan yang menakjubkan. Jaringan komputer, yang pada awalnya dimulai sebagai eksperimen di laboratorium akademik, telah menjadi fenomena global yang memasuki hampir setiap aspek kehidupan. Dari generasi ARPANET (*Advanced Research Project Agency Network*) yang penuh harapan hingga pada era Internet (Yudianto & Noor, 2014).

1.2 Sejarah Perkembangan Jaringan Komputer

1.2.1 Jaringan Komputer Pra-1960

Jaringan komputer sebelum tahun 1960 adalah konsep yang sangat awal dan terbatas, jauh sebelum munculnya teknologi modern seperti internet. Periode pra-1960 adalah periode eksperimen dan pengembangan awal yang membentuk dasar untuk perkembangan jaringan komputer selanjutnya. Berikut ini adalah penjelasan mengenai jaringan komputer pada periode tersebut:

1. Komputer Awal
   Pada awalnya, komputer adalah mesin yang besar dan mahal yang digunakan untuk perhitungan ilmiah dan proyek-proyek khusus. Mereka beroperasi secara terisolasi, dan data dimasukkan dan dikeluarkan melalui kartu punch.

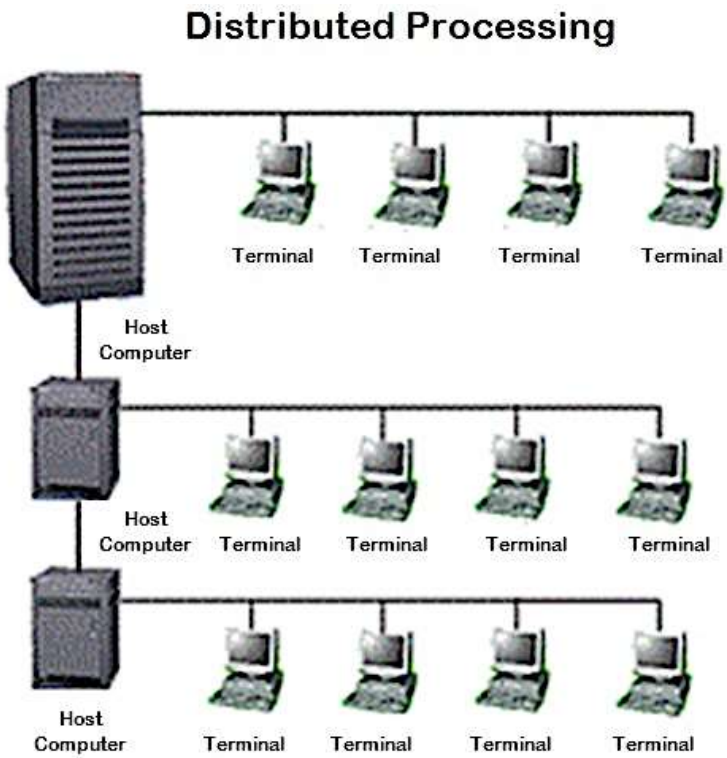


Gambar 1.1. Mesin sensus CTR yang menggunakan sistem kartu pons.

Kartu pons, Punch card, kartu IBM, atau kartu Hollerith adalah selembar kertas kaku yang berisi baik perintah untuk mengendalikan mesin otomatis atau data untuk aplikasi pengolahan data. Kedua perintah dan data diwakili oleh ada atau tidak adanya lubang di posisi yang telah ditentukan.

2. Telegraph dan Teleprinter
   Sebelum komputer modern, teknologi komunikasi jarak jauh seperti telegraf dan teleprinter digunakan untuk mengirim pesan dan data antara lokasi yang berjauhan. Ini bukanlah jaringan komputer, tetapi merupakan contoh awal komunikasi jarak jauh. Telegrafi adalah pengiriman jarak jauh dari pesan yang ditulis tanpa pengiriman fisik suatu surat. Definisi ini mencakup bentuk pengiriman data yang sekarang dipakai seperti faks, email, dan jaringan komputer.

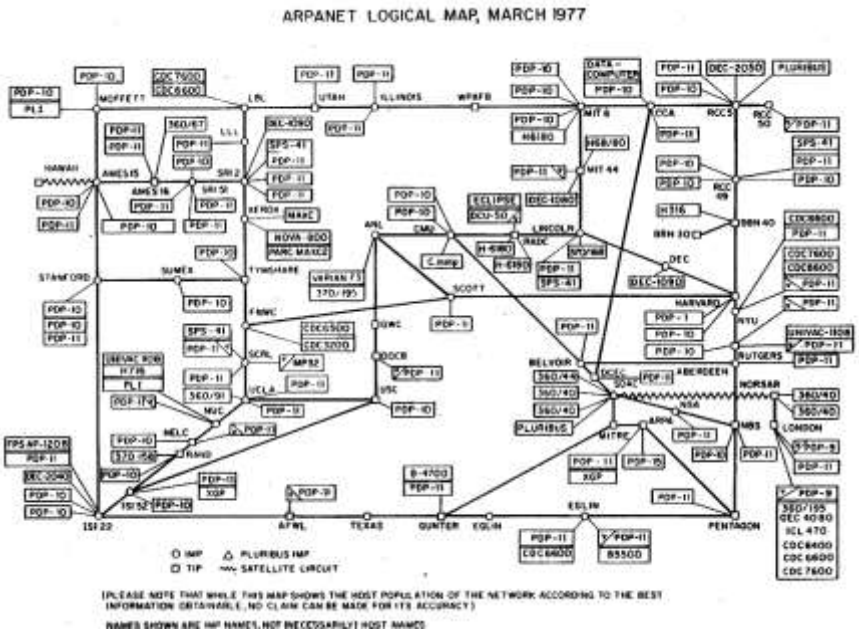
3. Pionir Kalkulator dan Komputer
   Beberapa ilmuwan dan insinyur di awal abad ke-20, seperti Charles Babbage dan Alan Turing, menciptakan mesin-mesin kalkulasi yang menjadi nenek moyang komputer modern. Namun, pada saat itu, gagasan tentang menghubungkan komputer tidak menjadi perhatian utama.
4. Proyek Kalkulator ENIAC
   Selama Perang Dunia II, proyek pembuatan komputer besar pertama, yaitu ENIAC (Electronic Numerical Integrator and Computer), mengalami perkembangan. Ini adalah komputer yang sangat besar dan rumit yang digunakan untuk menghitung tabel tembakau artileri. Namun, ENIAC tidak terhubung ke jaringan eksternal.
5. Penggunaan Pada Militer dan Penelitian Ilmiah
   Komputer di awal tahun 1960-an digunakan terutama oleh militer dan lembaga penelitian ilmiah. Mereka berfungsi sebagai alat bantu perhitungan dan simulasi untuk proyek-proyek khusus, tetapi belum ada konsep jaringan komputer seperti yang kita kenal sekarang.
6. Perkembangan Teori Jaringan
   Pada periode ini, beberapa teori tentang jaringan komputer mulai muncul, terutama melalui penelitian dan pemikiran para ilmuwan komputer seperti J.C.R. Licklider. Meskipun belum ada implementasi yang nyata, gagasan tentang komunikasi antar-komputer mulai berkembang (Sukaridhoto & ST Ph, 2014).



Gambar 1.2. Jaringan komputer model *distibuted processing*

1.2.2 Jaringan Komputer ARPANET: Akhir 1960an

ARPANET (*Advanced Research Projects Agency Network*) adalah jaringan komputer eksperimental yang dikembangkan pada akhir tahun 1960-an oleh Departemen Pertahanan Amerika Serikat, yang bertujuan untuk menghubungkan beberapa komputer di berbagai lokasi. ARPANET dianggap sebagai salah satu tonggak penting dalam sejarah jaringan komputer karena menjadi cikal bakal bagi perkembangan internet modern.



Gambar 1.3. Peta logika ARPNET pada maret 1977

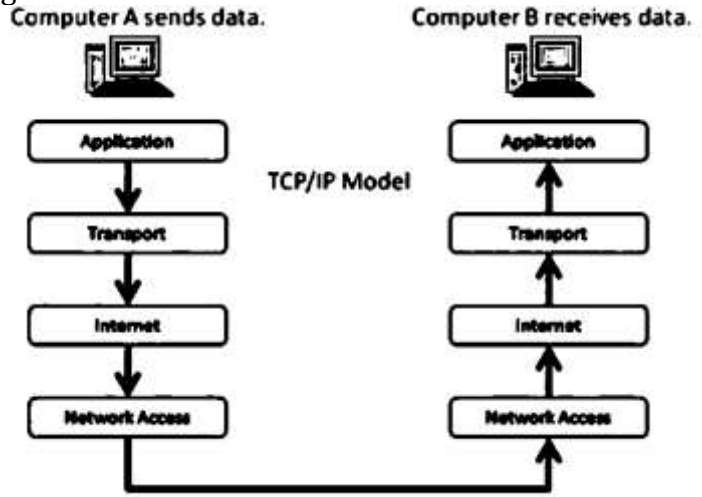
Pada tahun 1969, ARPANET mulai dikembangkan oleh Badan Proyek Penelitian Lanjutan (ARPA, sekarang DARPA). Laporan pertama yang mengusulkan konsep ARPANET, ditulis oleh J.C.R. Licklider dari MIT, pada tahun 1962, menjadi dasar pengembangan jaringan ini. Tujuan utama ARPANET adalah untuk menghubungkan komputer-komputer yang tersebar geografis, memungkinkan mereka untuk berbagi sumber daya, termasuk perangkat keras dan perangkat lunak. Ini juga bertujuan untuk menciptakan jaringan yang tahan banting dalam menghadapi serangan atau kegagalan komponen (Al Amien & Mukhtar, 2020).

1.2.3 Pertumbuhan Protokol TCP/IP: 1970

Pertumbuhan protokol TCP/IP (*Transmission Control Protocol/Internet Protocol*) pada tahun 1970-an adalah salah satu

tonggak penting dalam perkembangan jaringan komputer. TCP/IP adalah rangkaian protokol yang memungkinkan komputer untuk berkomunikasi satu sama lain di jaringan, dan saat ini merupakan dasar dari internet modern.

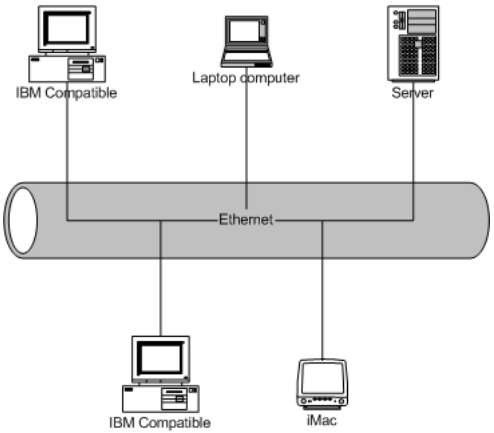
Protokol TCP/IP dikembangkan pada akhir dekade 1970-an hingga awal 1980-an sebagai sebuah protokol standar untuk menghubungkan komputer-komputer dan jaringan untuk membentuk sebuah jaringan yang luas (WAN). TCP/IP merupakan sebuah standar jaringan terbuka yang bersifat independen terhadap mekanisme transport jaringan fisik yang digunakan, sehingga dapat digunakan di mana saja (Pujowati & Harianto, 2021). Protokol ini menggunakan skema pengalamatan yang sederhana yang disebut sebagai alamat IP (IP Address) yang mengizinkan hingga beberapa ratus juta komputer untuk dapat saling berhubungan satu sama lainnya di Internet. Protokol ini juga bersifat routable yang berarti protokol ini cocok untuk menghubungkan sistem-sistem berbeda (seperti Microsoft Windows dan keluarga UNIX) untuk membentuk jaringan yang heterogen.



Gambar 1.4. Cara kerja protokol TCP/IP

1.2.4 Pengembangan Ethernet: 1970

Pengembangan Ethernet pada tahun 1970an adalah salah satu langkah penting dalam perkembangan jaringan komputer lokal (LAN) yang kemudian menjadi bagian integral dari jaringan komputer modern. Ethernet, yang dikembangkan oleh Robert Metcalfe, menghadirkan cara efisien untuk menghubungkan komputer di dalam area lokal, seperti di dalam gedung atau kantor.



Gambar 1.5. Diagram konseptual dari jaringan area lokal menggunakan topologi jejaring bus

Pengembangan Ethernet dimulai pada tahun 1973 di Xerox Corporation oleh Robert Metcalfe dan rekannya David Boggs. Proyek ini awalnya disebut "Ethernet" karena mereka menganggapnya sebagai cara untuk mengukur jarak di dalam lab mereka, bukan sebagai nama jaringan. Salah satu inovasi utama dalam Ethernet adalah penggunaan metode akses CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*). Ini adalah cara yang efisien untuk mengatur akses berbagi ke saluran komunikasi di antara beberapa komputer. CSMA/CD memungkinkan komputer untuk berbagi saluran komunikasi

secara adil dan menghindari tabrakan (collision) saat mengirimkan data (Tantriawan et al., 2023).

Pada tahun 1980, IEEE (Institute of Electrical and Electronics Engineers) mengadopsi teknologi Ethernet sebagai standar yang dikenal sebagai IEEE 802.3. Standar ini mendefinisikan berbagai aspek Ethernet, seperti protokol fisik (seperti kabel dan konektor) dan protokol data (seperti format frame data). Ethernet pertama kali diimplementasikan secara praktis di Xerox PARC (*Palo Alto Research Center Incorporated*) di California pada tahun 1974. Xerox PARC kemudian menjadi salah satu pusat penelitian utama yang mengembangkan teknologi komputer seperti mouse, antarmuka grafis, dan jaringan komputer. Ethernet tumbuh dengan pesat dan segera menjadi teknologi standar untuk jaringan lokal di berbagai sektor, termasuk pendidikan, bisnis, dan industri. Ini memungkinkan komputer di dalam organisasi atau di lokasi yang berdekatan untuk berkomunikasi dan berbagi sumber daya dengan efisien. Seiring berjalannya waktu, Ethernet mengalami perkembangan yang signifikan dalam hal kecepatan dan standar. Awalnya, Ethernet beroperasi pada kecepatan 10 Mbps (megabit per detik). Namun, dengan kemajuan teknologi, kecepatan Ethernet meningkat menjadi 100 Mbps (*Fast Ethernet*), 1 Gbps (*Gigabit Ethernet*), dan bahkan 10 Gbps dan 100 Gbps dalam perkembangan selanjutnya (Romindo et al., n.d.).

Pengembangan Ethernet pada tahun 1970an memainkan peran kunci dalam memungkinkan pertumbuhan dan adopsi jaringan komputer lokal di seluruh dunia. Ini menciptakan dasar bagi konektivitas di dalam gedung, kampus, dan tempat kerja, dan Ethernet tetap menjadi teknologi yang sangat relevan dan dominan dalam jaringan komputer hingga saat ini.

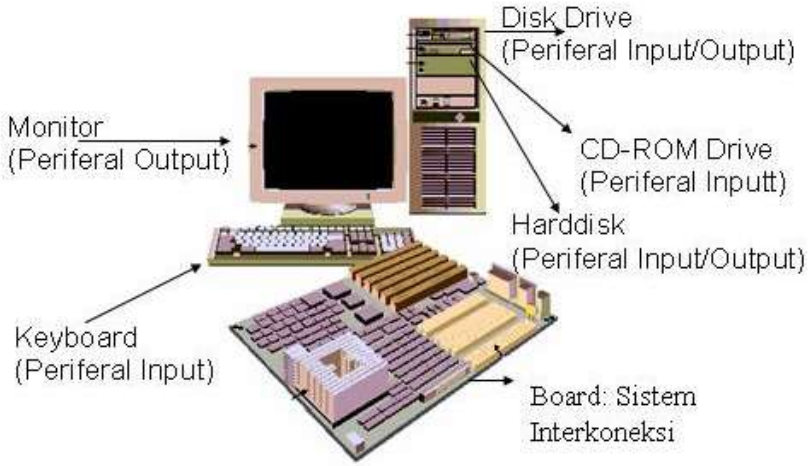
1.2.5 Kemunculan Mikrokomputer: 1970-1980an

Kemunculan mikrokomputer pada tahun 1970-an hingga 1980-an adalah salah satu peristiwa paling penting dalam sejarah komputasi dan jaringan komputer (Andriyani et al., 2023). Ini membuka pintu bagi penggunaan komputer di tingkat individu dan di dalam bisnis, serta memungkinkan perkembangan jaringan komputer lokal (LAN) yang lebih terjangkau dan mudah diakses.

Sebelum era mikrokomputer, komputer adalah mesin besar yang mahal dan hanya tersedia di laboratorium penelitian, universitas, dan perusahaan-perusahaan besar. Mereka digunakan untuk perhitungan ilmiah, penelitian, dan tugas-tugas khusus lainnya. Pada tahun 1971, Intel memperkenalkan mikroprosesor pertama, Intel 4004, yang merupakan komponen utama dalam komputer mikro. Ini menjadi tonggak penting dalam perkembangan komputer karena memungkinkan pengembangan komputer yang lebih kecil dan lebih terjangkau.

Pada tahun 1975, Altair 8800, salah satu komputer mikro pertama yang berbasis mikroprosesor Intel 8080, dirilis oleh MITS (*Micro Instrumentation and Telemetry Systems*). Altair 8800 menjadi komputer mikro pertama yang tersedia secara komersial dan dijual sebagai kit. Ini menjadi populer di kalangan penghobi komputer. Steve Wozniak dan Steve Jobs memperkenalkan Apple I pada tahun 1976 dan kemudian Apple II pada tahun 1977. Apple II adalah salah satu komputer mikro pertama yang memiliki antarmuka grafis dan layar berwarna, yang membuatnya populer di kalangan pengguna rumahan dan pendidik (Nuraini et al., 2023).

Pada tahun 1981, IBM memasuki pasar komputer mikro dengan merilis IBM PC. Ini adalah komputer yang menggunakan arsitektur terbuka, dan keberhasilannya membuka pintu bagi berbagai produsen untuk membuat perangkat keras dan perangkat lunak yang kompatibel dengan IBM PC. Ini menjadi landasan bagi komputer pribadi modern.



Gambar 1.6. Sistem Mikrokomputer

1.2.6 Internet Awal: 1980an

Pada tahun 1980-an, internet awal mengalami perkembangan yang signifikan, yang membentuk dasar bagi internet modern yang kita kenal saat ini. Meskipun masih dalam tahap eksperimental, banyak perkembangan penting dan proyek-proyek yang mengarah ke pembentukan internet sebagai salah satu jaringan komputer terbesar dan paling berpengaruh di dunia. Berikut adalah penjelasan lebih lanjut tentang internet awal pada dekade 1980-an:

1. Peralihan ke TCP/IP
   Salah satu peristiwa kunci pada awal 1980-an adalah peralihan dari protokol NCP (*Network Control Protocol*) ke protokol TCP/IP (*Transmission Control Protocol/ Internet Protocol*) sebagai standar komunikasi di ARPANET dan jaringan-jaringan lainnya. Ini adalah langkah penting dalam pengembangan internet.

2. Pembentukan Domain Name System (DNS)
   Pada tahun 1983, Paul Mockapetris mengembangkan *Domain Name System* (DNS), yang memungkinkan pengguna internet untuk menggunakan nama domain (seperti www.example.com) alih-alih alamat IP numerik. Ini membuat internet lebih mudah diakses dan dipahami oleh pengguna.
3. Pembentukan Usenet:
   Usenet adalah sistem forum diskusi berbasis tekstual yang muncul pada tahun 1980. Ini adalah salah satu layanan awal yang memungkinkan pengguna untuk berbagi informasi dan berdiskusi tentang berbagai topik. Usenet menjadi salah satu asal mula dari grup berita internet.
4. Proyek NSFNET
   National Science Foundation (NSF) di Amerika Serikat meluncurkan proyek NSFNET pada tahun 1985. Ini adalah jaringan berkecepatan tinggi yang menghubungkan universitas dan pusat penelitian di seluruh negara bagian AS. NSFNET menjadi tulang punggung utama internet awal.
5. Pengembangan MUDs dan MUSHes
   Multi-User Dungeons (MUDs) dan *Multi-User Shared Hallucinations* (MUSHes) adalah game dan lingkungan virtual awal yang muncul pada tahun 1980-an. Mereka memungkinkan pengguna untuk berinteraksi secara real-time dalam lingkungan virtual yang berbagi.
6. Pertumbuhan Pengguna Internet
   Selama tahun 1980-an, pengguna internet mulai berkembang secara signifikan, terutama di kalangan akademisi, peneliti, dan komunitas teknologi. Meskipun masih jauh dari mencapai tingkat penggunaan yang meluas seperti saat ini, internet mulai meresap ke berbagai sektor.

7. Standarisasi Email dan Protokol Internet Lainnya
   Standarisasi protokol email, seperti SMTP (*Simple Mail Transfer Protocol*), POP (*Post Office Protocol*), dan IMAP (*Internet Message Access Protocol*), memungkinkan pengiriman dan pengelolaan email yang efisien. Ini merupakan langkah penting dalam pengembangan komunikasi internet.
8. Munculnya Web Browser
   Meskipun web browser modern seperti Mozilla Firefox atau Google Chrome belum ada pada tahun 1980-an, proyek-proyek seperti WorldWideWeb (WWW) yang dikembangkan oleh Tim Berners-Lee pada awal 1990-an telah membuka jalan bagi pengembangan World Wide Web.

1.2.7 Revolution Mobile: 2000an

Revolusi mobile pada tahun 2000an merujuk pada perkembangan pesat dalam teknologi komunikasi nirkabel, terutama dalam hal perangkat seluler (ponsel) dan jaringan seluler. Periode ini ditandai oleh inovasi dalam perangkat seluler, peningkatan kecepatan data, dan munculnya aplikasi mobile yang mengubah cara kita berinteraksi dengan dunia digital. Berikut adalah penjelasan lebih lanjut tentang revolusi mobile pada tahun 2000an:

1. Perkembangan Ponsel Cerdas
   Pada awal tahun 2000, ponsel cerdas atau smartphone mulai menjadi populer. Ponsel cerdas memiliki kemampuan untuk menjalankan aplikasi, menjelajahi web, mengirim pesan teks, dan melakukan berbagai fungsi lainnya. iPhone yang dirilis oleh Apple pada tahun 2007 adalah salah satu perangkat yang mengubah permainan dan memulai tren smartphone modern.

2. Jaringan Seluler Generasi Ketiga (3G)
   Perkembangan teknologi jaringan seluler dari 2G ke 3G membawa peningkatan signifikan dalam kecepatan data. Ini memungkinkan pengguna untuk mengakses internet dengan lebih cepat dan mulai menggunakannya untuk streaming video, bermain game online, dan aplikasi berat data lainnya.
3. Proliferasi Aplikasi Mobile
   Penyebaran smartphone memungkinkan pengembangan dan adopsi aplikasi mobile yang luas. Aplikasi seperti WhatsApp, Facebook, Instagram, dan Twitter menjadi populer, mengubah cara kita berkomunikasi dan berbagi informasi.
4. Jaringan Seluler Generasi Keempat (4G)
   4G, yang diperkenalkan pada tahun 2009, memberikan kecepatan internet yang lebih tinggi daripada 3G, memungkinkan streaming video berkualitas tinggi, video konferensi, dan penggunaan aplikasi yang lebih lancar di perangkat seluler.
5. Munculnya Internet Mobile
   Akses internet mobile yang lebih cepat dan lebih stabil membuka pintu bagi pengguna untuk menjelajahi web, membaca berita, berbelanja online, dan melakukan berbagai aktivitas online di perangkat seluler.
6. Kecerdasan Buatan dalam Mobile
   Kecerdasan buatan semakin diintegrasikan dalam aplikasi mobile, seperti asisten virtual seperti Siri (Apple) dan Google Assistant. Ini membuat pengalaman pengguna menjadi lebih personal dan responsif.
7. *Internet of Things* (IoT) Mobile
   Internet of Things (IoT) berkembang pesat pada tahun 2000an, dan banyak perangkat IoT terhubung melalui jaringan seluler. Contohnya termasuk mobil pintar,

perangkat rumah pintar, dan perangkat medis terhubung yang memanfaatkan koneksi mobile untuk berkomunikasi.

8. Jaringan Seluler Generasi Kelima (5G)
   Pengembangan jaringan seluler 5G menjadi pusat perhatian pada akhir tahun 2010an dan awal 2020an. 5G menjanjikan kecepatan internet yang sangat tinggi, keterlambatan rendah, dan kapasitas yang lebih besar. Ini membuka peluang baru, seperti kendaraan otonom dan realitas virtual yang diperbaiki (Wibowo et al., 2023).

1.2.8 Jaringan 5G dan Masa Depan

Jaringan 5G adalah generasi terbaru dalam teknologi jaringan seluler yang memberikan peningkatan signifikan dalam kecepatan, kapasitas, dan kinerja jaringan dibandingkan dengan generasi sebelumnya (4G) (Muttaqin et al., 2023). Ini membawa perubahan besar dalam berbagai aspek, termasuk konektivitas, industri, dan gaya hidup. Di masa depan, 5G memiliki dampak yang signifikan:

1. Realitas Virtual dan Augmented Reality
   5G akan memungkinkan pengembangan lebih lanjut dalam VR dan AR. Ini akan memungkinkan pengalaman yang lebih mendalam dalam gaming, pelatihan, pendidikan, dan hiburan.
2. Smart Cities
   Pengembangan kota pintar (smart cities) akan dipercepat oleh 5G. Ini mencakup pemantauan lalu lintas, manajemen limbah, tata kota yang efisien, dan penggunaan sensor untuk meningkatkan kualitas hidup di kota-kota besar.
3. IoT yang Lebih Besar
   Dengan kapasitas yang lebih besar, 5G akan mendukung pertumbuhan besar dalam IoT. Ini akan menghubungkan lebih banyak perangkat di rumah, industri, dan lingkungan kota.

4. Keamanan dan Privasi
   Seiring dengan peningkatan konektivitas, perhatian akan semakin diberikan pada keamanan dan privasi data. Perlindungan terhadap serangan siber dan pengelolaan data yang aman akan menjadi fokus penting.
5. Pemanfaatan AI
   5G akan memungkinkan aplikasi kecerdasan buatan (AI) yang lebih kuat dan responsif. Ini akan berdampak pada berbagai industri, termasuk layanan pelanggan, manufaktur, dan otomasi.
6. Kerja Jarak Jauh yang Lebih Lanjut
   Kemampuan 5G untuk menyediakan konektivitas tingkat tinggi di mana saja akan memungkinkan lebih banyak pekerjaan jarak jauh dan kolaborasi tim yang lebih efisien.

Jaringan 5G memiliki potensi untuk mengubah cara kita menjalani hidup, bekerja, dan berinteraksi dengan teknologi. Dengan kemampuan yang lebih besar dan konektivitas yang lebih cepat, kita dapat mengantisipasi terobosan teknologi yang lebih besar dan perubahan signifikan dalam berbagai aspek kehidupan di masa yang akan datang.

DAFTAR PUSTAKA

Al Amien, J., & Mukhtar, H. 2020. *Implementasi Jaringan Komputer*. Deepublish.

Andriyani, W., Sacipto, R., Susanto, D., Vidiati, C., Kurniawan, R., & Nugrahani, R. A. G. 2023. *Technology, Law And Society*. Tohar Media.

Iskandar, A., Geni, B. Y., Prabiantissa, C. N., Kurnaedi, D., Wahyuddin, S., Samosir, K., … Supriyadi, A. 2022. *Pengantar Jaringan Komputer*. Get Press.

Muttaqin, M., Simarmata, J., AKP, A. M., Nurzaenab, N., Ashari, I. F., Wahyuddin, S., … Arifin, S. R. 2023. *Cloud Computing: Konsep dan Implementasi*. Yayasan Kita Menulis.

Nuraini, R., Komalasari, R., Kurniawan, F. S., Rachmat, Z., Wahyuddin, S., Munawar, Z., … Firgia, L. 2023. *Organisasi Dan Arsitektur Komputer*. Global Eksekutif Teknologi.

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

Romindo, R. M., Yusnanto, T., Heryana, N., Jamaludin, A. P. A., Permana, A. A., Aisa, S., … Sihombing, F. A. H. (n.d.). *Rekayasa Perangkat Lunak*.

Sukaridhoto, S., & ST Ph, D. 2014. Buku Jaringan Komputer I. *Surabaya: Politeknik Elektronika Negeri Surabaya*.

Tantriawan, H., Sasongko, D., Rizal, M., Lumbanraja, O. M., Suryani, S., Halid, A., … Sirwan, S. 2023. *Komunikasi Data dan Jaringan*. Yayasan Kita Menulis.

Wibowo, S. H., Wahyuddin, S., Permana, A. A., Sembiring, S., Wahidin, A. J., Nugroho, J. W., … Adhicandra, I. 2023. *Teknologi Digital Di Era Modern*. Global Eksekutif Teknologi.

Yudianto, M. J. N., & Noor, J. 2014. Jaringan komputer dan Pengertiannya. *Ilmukomputer. Com*, *1*, 1–10.

BAB 2
MODEL REFRENSI OSI DAN TCIP

Oleh Wirawan Istiono

2.1 Apa itu Model OSI?

Model *Open Systems Interconnection* (model OSI) adalah model konseptual yang dikembangkan oleh Organisasi Internasional untuk Standardisasi (ISO) yang "menyediakan dasar bersama untuk koordinasi pengembangan standar untuk tujuan interkoneksi sistem." Model referensi OSI membagi komunikasi antara sistem komputasi menjadi tujuh lapisan abstraksi: physics, Data link, network, transportation, session, dan presentation (*model OSI*, 2023).

Model tersebut membagi aliran data dalam sistem komunikasi menjadi tujuh lapisan abstraksi untuk menggambarkan komunikasi jaringan dari implementasi fisik pengiriman bit melalui media komunikasi hingga representasi data tingkat tertinggi dari aplikasi terdistribusi. Setiap lapisan perantara menyediakan kelas fungsionalitas ke lapisan di atasnya dan menerima kelas fungsionalitas dari lapisan di bawahnya. Kelas fungsionalitas diimplementasikan melalui semua protokol komunikasi standar di semua pengembangan perangkat lunak.

Setiap lapisan model OSI memiliki fungsi yang terdefinisi dengan baik, dan setiap metode lapisan berkomunikasi dan berinteraksi dengan lapisan tepat di atas dan di bawah, sebagaimana mestinya.

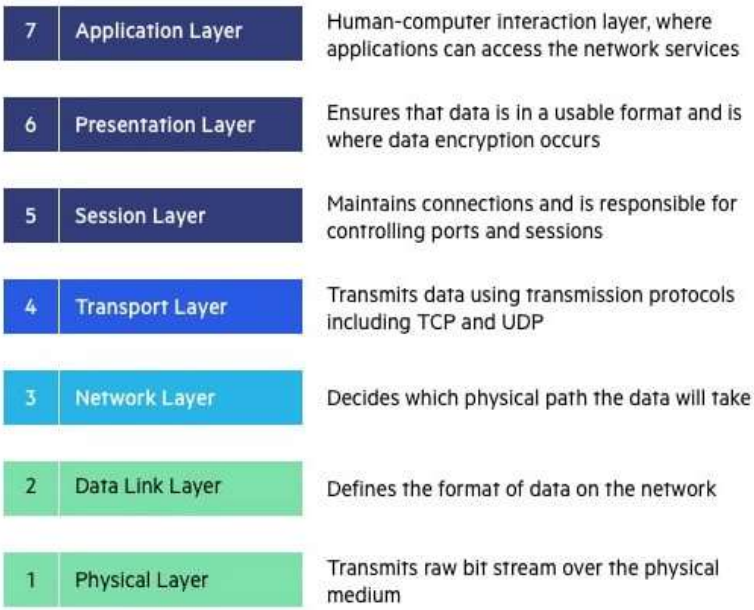
Rangkaian protokol Internet, sebagaimana didefinisikan dalam RFC 1122 dan RFC 1123, adalah model jaringan yang dikembangkan bersamaan dengan model OSI, dan sebagian besar didanai oleh Departemen Pertahanan Amerika Serikat. Itu adalah

fondasi di mana Internet dibangun. Itu mengasumsikan adanya koneksi fisik generik dan berfokus terutama pada lapisan komunikasi perangkat lunak, dengan struktur yang sebanding dengan model OSI tetapi jauh lebih ketat (*model OSI*, 2023).

Beberapa model jaringan telah berusaha untuk membuat kerangka intelektual untuk menjelaskan konsep dan aktivitas jaringan, [rujukan?] Tetapi tidak ada yang sesukses model referensi OSI dalam membangun dirinya sebagai model standar untuk berdiskusi dan mengajar jaringan di bidang teknologi informasi. . Melalui jaringan peer-to-peer (juga dikenal sebagai komunikasi peer-to-peer), model ini memungkinkan komunikasi transparan antara dua peserta melalui pertukaran unit data protokol (PDU) yang setara. Karena sebagian besar kerangka kerjanya yang ramah pengguna diterima secara luas, model referensi OSI telah menjadi komponen penting tidak hanya di kalangan profesional dan non-profesional, tetapi juga di semua jaringan antara satu pihak atau lebih.

Paradigma Open System Interconnection (OSI) menggambarkan tujuh lapisan yang digunakan sistem komputer untuk komunikasi jaringan. Itu adalah model standar pertama untuk komunikasi jaringan, diadopsi pada awal 1980-an oleh semua perusahaan komputer dan telekomunikasi besar. Internet modern tidak didasarkan pada OSI, melainkan pada model TCP/IP yang lebih mudah. Namun, model OSI 7-lapisan masih banyak digunakan karena membantu dalam memvisualisasikan dan mengkomunikasikan bagaimana jaringan beroperasi dan dalam mengisolasi dan menyelesaikan masalah jaringan (Imperva.com, 2023).

OSI diperkenalkan oleh perwakilan perusahaan komputer dan telekomunikasi terbesar pada tahun 1983, dan ISO mengadopsinya sebagai standar internasional pada tahun 1984 (Imperva.com, 2023).



Gambar 2.1. Penjelasan Model OSI: OSI 7 Layers
(Sumber: Imperva.com, 2023)

2.1.1 Application Layer

Perangkat lunak pengguna akhir seperti browser web dan program email memanfaatkan lapisan aplikasi. Ini menyediakan protokol yang memungkinkan perangkat lunak untuk mengirim dan menerima data dan menyajikan informasi yang berarti kepada pengguna. *Hypertext Transfer Protocol* (HTTP), *File Transfer Protocol (*FTP), *Post Office Protocol* (POP), *Simple Mail Transfer Protocol* (SMTP), dan Domain Name System (DNS) adalah contoh protokol lapisan aplikasi.

2.1.2 Presentation Layer

Data disiapkan untuk lapisan aplikasi oleh lapisan presentasi. Ini menentukan bagaimana dua perangkat harus menyandikan, mengenkripsi, dan memampatkan data agar

perangkat lain menerimanya secara akurat. Lapisan presentasi menyiapkan data lapisan aplikasi untuk transmisi melalui lapisan sesi.

2.1.3 Session Layer

Lapisan sesi menetapkan saluran komunikasi antar perangkat, yang dikenal sebagai sesi. Ini bertanggung jawab untuk membuka sesi, memastikan bahwa mereka tetap terbuka dan berfungsi saat data dikirim, dan menutupnya setelah komunikasi selesai. Lapisan sesi juga dapat mengatur pos pemeriksaan selama transfer data, yang memungkinkan perangkat melanjutkan transfer data dari pos pemeriksaan terakhir jika sesi terganggu.

2.1.4 Transportation Layer

Lapisan transport membagi data yang ditransmisikan dalam lapisan sesi menjadi "segmen" di ujung pengiriman. Ini bertanggung jawab untuk memasang kembali segmen di ujung penerima, mengubahnya kembali menjadi data yang dapat digunakan oleh lapisan sesi. Lapisan transport bertanggung jawab untuk kontrol aliran, yang melibatkan pengiriman data pada kecepatan yang sesuai dengan kecepatan koneksi perangkat penerima, dan kontrol kesalahan, yang melibatkan penentuan apakah data diterima secara akurat dan memintanya kembali jika tidak.

2.1.5 Network Layer

Lapisan jaringan melayani dua tujuan utama. Salah satunya adalah menguraikan segmen menjadi paket jaringan dan memasangnya kembali di sisi penerima. Yang lainnya adalah perutean paket dengan menentukan jalur optimal melintasi jaringan fisik. Untuk merutekan paket ke node tujuannya, lapisan jaringan menggunakan alamat jaringan (biasanya alamat Protokol Internet).

2.1.6 Data Link Layer

Lapisan tautan data bertanggung jawab untuk membangun dan mengakhiri koneksi antara dua elemen jaringan yang terhubung secara fisik. Ini membagi paket menjadi bingkai sebelum mengirimkannya dari sumber ke tujuan. Lapisan ini terdiri dari dua bagian: LLC, yang mengidentifikasi protokol jaringan, melakukan pemeriksaan kesalahan, dan menyinkronkan bingkai, dan MAC, yang menggunakan alamat MAC untuk menghubungkan perangkat dan menentukan izin untuk mengirim dan menerima data.

2.1.7 Physics Layer

Lapisan fisik bertanggung jawab atas koneksi nyata antara node jaringan melalui sarana kabel atau nirkabel. Ini mendefinisikan konektor, kabel listrik atau teknologi nirkabel yang menghubungkan perangkat dan bertanggung jawab untuk transmisi data mentah, yang terdiri dari serangkaian 0 dan 1, serta kontrol laju bit (Imperva.com, 2023).

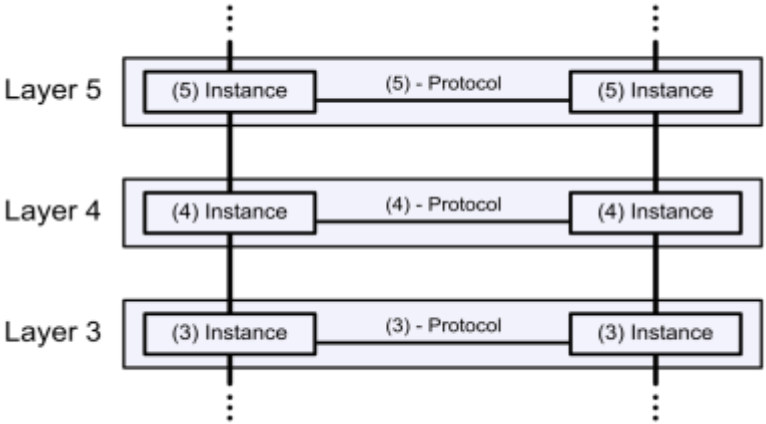
2.2 Sejarah Model OSI

Model OSI dibuat pada akhir 1970-an untuk mendukung proliferasi beragam metode jaringan komputer yang bersaing untuk aplikasi di inisiatif jaringan nasional terbesar di dunia (lihat Protokol OSI dan Perang Protokol). Pada 1980-an, kelompok Interkoneksi Sistem Terbuka dari Organisasi Internasional untuk Standardisasi (ISO) mengembangkan versi model yang berfungsi. Sementara berusaha untuk memberikan gambaran yang komprehensif tentang jaringan, model ini gagal mendapatkan dukungan selama desain Internet, sebagaimana dibuktikan oleh Internet Protocol Suite yang kurang preskriptif, yang terutama disponsori oleh *Internet Engineering Task Force* (IETF) (*model OSI*, 2023).

Awal dan pertengahan 1970-an jaringan terutama disponsori pemerintah (jaringan NPL di Inggris Raya, ARPANET di

Amerika Serikat, dan CYCLADES di Prancis) atau dikembangkan vendor dengan standar kepemilikan, seperti Arsitektur Jaringan Sistem IBM dan DECnet Digital Equipment Corporation. Pada akhir 1970-an, jaringan data publik pertama kali mengadopsi protokol X.25.

Di Inggris antara tahun 1973 dan 1975, Sistem Pengalih Paket Eksperimental mengidentifikasi kebutuhan untuk mendefinisikan protokol tingkat yang lebih tinggi. Why Distributed Computing, sebuah publikasi dari UK National Computing Center berdasarkan penelitian ekstensif tentang konfigurasi sistem komputer di masa depan, menghasilkan kasus di Inggris untuk komite standar internasional untuk membahas area ini pada pertemuan ISO di Sydney pada bulan Maret 1977.



Gambar 2.2. Komunikasi dalam model OSI (contoh dengan layer 3 sampai 5)
(Sumber: *model OSI*, 2023)

ISO memprakarsai sebuah program untuk mengembangkan standar dan protokol jaringan umum pada tahun 1977. Komite Konsultatif Telegraf dan Telepon Internasional (CCITT, dari bahasa Prancis: Comité Consultatif International Téléphone et Télégraphe)

mengalami evolusi serupa. Kedua organisasi menghasilkan dokumen yang mendefinisikan model jaringan yang sebanding. Departemen Perdagangan dan Industri Inggris berfungsi sebagai sekretariat organisasi, dan universitas di Inggris merancang prototipe standar.

Model OSI awalnya didefinisikan dalam bentuk yang belum dimurnikan di Washington, D.C., pada bulan Februari 1978 oleh insinyur perangkat lunak Perancis Hubert Zimmermann, dan ISO menerbitkan standar draf yang disempurnakan namun belum selesai pada tahun 1980. Pencipta model referensi harus menyeimbangkan banyak prioritas dan kepentingan yang saling bersaing. . Alih-alih standarisasi prosedur setelah fakta, tingkat perubahan teknologi memerlukan standar mendefinisikan dimana sistem baru bisa berkumpul, yang merupakan kebalikan dari pendekatan tradisional untuk mengembangkan standar. Meskipun bukan standar itu sendiri, itu memberikan kerangka kerja untuk definisi standar masa depan (*model OSI*, 2023).

Dokumen CCITT dan ISO digabungkan pada Mei 1983 untuk membuat Model Referensi Dasar untuk Interkoneksi Sistem Terbuka, juga dikenal sebagai Model Referensi Interkoneksi Sistem Terbuka, Model Referensi OSI, atau model OSI. Itu diterbitkan pada tahun 1984 oleh ISO dan berganti nama CCITT (sekarang dikenal sebagai Sektor Standardisasi Telekomunikasi dari International Telecommunication Union atau ITU-T) sebagai standar X.200.

OSI terdiri dari dua komponen utama: model jaringan abstrak yang dikenal sebagai Model Referensi Dasar atau model tujuh lapis, dan kumpulan protokol khusus. Model referensi OSI mewakili langkah maju yang signifikan dalam standarisasi konsep jaringan. Ini mempromosikan konsep paradigma yang konsisten dari lapisan protokol, mendefinisikan perangkat jaringan dan interoperabilitas perangkat lunak.

Konsep paradigma tujuh lapis dikembangkan oleh Charles Bachman dari Honeywell Information Systems. Desain OSI

dipengaruhi oleh jaringan NPL, ARPANET, CYCLADES, EIN, dan Kelompok Kerja Jaringan Internasional (IFIP WG6.1) dalam berbagai cara. Sistem jaringan disegmentasi menjadi beberapa lapisan dalam model ini. Dalam setiap strata, satu atau lebih entitas bertanggung jawab untuk mengimplementasikan fungsinya. Setiap entitas hanya berinteraksi langsung dengan lapisan di bawahnya dan memberikan fasilitas bagi lapisan di atasnya.

ITU-T menawarkan dokumen standar OSI sebagai seri rekomendasi X.200.[16] Beberapa spesifikasi protokol juga disertakan dalam seri ITU-T X. ISO menyediakan standar ISO/IEC yang setara untuk model OSI. Tidak semuanya bebas biaya. OSI adalah inisiatif industri yang mencoba membuat peserta industri menyetujui standar jaringan umum untuk memfasilitasi interoperabilitas di antara banyak vendor. Itu adalah hal yang umum bagi jaringan besar untuk mendukung beberapa rangkaian protokol jaringan, dan kurangnya protokol umum mencegah banyak perangkat untuk beroperasi. Pada akhir 1980-an dan awal 1990-an, para insinyur, organisasi, dan negara terpecah atas standar mana, model OSI atau rangkaian protokol Internet, yang akan menghasilkan jaringan komputer yang paling efektif dan tangguh. Namun demikian, sementara OSI mengembangkan standar jaringannya pada akhir 1980-an, TCP/IP untuk internetworking pada jaringan multi-vendor diterima secara luas.*model OSI*, 2023).

Model OSI masih digunakan sebagai referensi untuk pengajaran dan dokumentasi, tetapi protokol OSI yang awalnya dirancang untuk model tersebut belum diterima secara luas. Insinyur tertentu menegaskan bahwa model referensi OSI masih berlaku untuk komputasi awan. [24] Yang lain berpendapat bahwa model OSI asli tidak kompatibel dengan protokol jaringan modern dan mengusulkan pendekatan yang disederhanakan.

2.3 Manfaat Model OSI

Model OSI membantu konsumen dan administrator jaringan dengan (Imperva.com, 2023):

1. Tentukan perangkat keras dan perangkat lunak yang diperlukan untuk membangun jaringan mereka.
2. Memahami dan mengkomunikasikan proses yang diikuti oleh komponen jaringan saat berkomunikasi.
3. Lakukan pemecahan masalah dengan menentukan lapisan jaringan mana yang menjadi sumber masalah dan memfokuskan upaya pada lapisan tersebut.

Model OSI membantu produsen perangkat jaringan dan vendor perangkat lunak jaringan dengan cara berikut:

1. Kembangkan perangkat dan perangkat lunak yang dapat berkomunikasi dengan produk dari produsen lain mana pun, memungkinkan interoperabilitas terbuka.
2. Tentukan komponen jaringan mana yang harus kompatibel dengan produk mereka.
3. Beri tahu konsumen tentang lapisan jaringan tempat produk Anda beroperasi, seperti lapisan aplikasi atau keseluruhan tumpukan.

2.4 Apa itu Model TCP/IP?

Transmission Control Protocol/Internet Protocol (TCP/IP) adalah kumpulan protokol komunikasi yang memfasilitasi interkoneksi perangkat jaringan di dalam internet. Protokol TCP/IP umumnya digunakan sebagai protokol komunikasi dalam jaringan komputer pribadi, seperti intranet dan ekstranet.

TCP/IP, juga dikenal sebagai Protokol Kontrol Transmisi/Protokol Internet, mengacu pada perangkat lunak lengkap yang mencakup kumpulan aturan dan prosedur. *Transmission Control Protocol* (TCP) dan *Internet Protocol* (IP) sering dianggap sebagai dua protokol terpenting dalam jaringan

komputer, meskipun ada protokol tambahan yang berperan dalam domain ini. Rangkaian protokol TCP/IP berfungsi sebagai lapisan konseptual abstraksi yang memediasi interaksi antara aplikasi internet dan infrastruktur routing dan switching yang mendasarinya.

Paket protokol TCP/IP menetapkan pedoman untuk transmisi data melalui internet, yang mencakup seluruh proses komunikasi end-to-end. Ini termasuk penggambaran data ke dalam paket, penetapan alamat, transmisi dan perutean paket ini, dan penerimaannya di tujuan yang dituju. Rangkaian protokol TCP/IP menunjukkan struktur terdesentralisasi, meminimalkan kebutuhan akan kontrol terpusat. Desainnya bertujuan untuk meningkatkan keandalan jaringan melalui mekanisme pemulihan otonom jika terjadi kegagalan perangkat.

Paket *Internet Protocol* (IP) terdiri dari dua protokol inti yang memenuhi peran terpisah. *Transmission Control Protocol* (TCP) mengatur prosedur dan mekanisme dimana aplikasi dapat membangun saluran komunikasi melalui jaringan. Selain itu, ia bertanggung jawab atas pengelolaan segmentasi pesan sebelum dikirim melalui internet, serta pemasangan kembali segmen ini selanjutnya di alamat tujuan yang ditentukan.

Protokol Internet (IP) bertanggung jawab untuk menentukan mekanisme pengalamatan dan perutean yang tepat untuk memastikan keberhasilan pengiriman setiap paket ke titik akhir yang ditentukan. Setiap komputer gateway dalam jaringan menjalani proses verifikasi alamat IP ini untuk memastikan tujuan yang sesuai untuk pengiriman pesan.

Subnet mask melayani tujuan menggambarkan komponen jaringan dan bagian host dari alamat IP, sehingga memungkinkan komputer atau perangkat jaringan lainnya untuk membedakan jaringan dan masing-masing komputer atau host dalam jaringan itu.

Terjemahan alamat jaringan (NAT) mengacu pada proses mengubah alamat IP. Network Address Translation (NAT) adalah mekanisme yang meningkatkan langkah-langkah keamanan dan mengurangi kebutuhan akan sejumlah besar alamat IP dalam konteks organisasi.

Protokol TCP/IP standar biasanya mencakup komponen-komponen berikut.

1. HTTP adalah protokol yang memfasilitasi pertukaran informasi antara web server dan web browser.
2. HTTP Secure (HTTPS) adalah protokol yang meningkatkan keamanan komunikasi antara web server dan web browser.
3. *File movement Protocol* (FTP) adalah protokol komputer yang memungkinkan perpindahan file antara beberapa komputer.

2.5 Sejarah TCP/IP

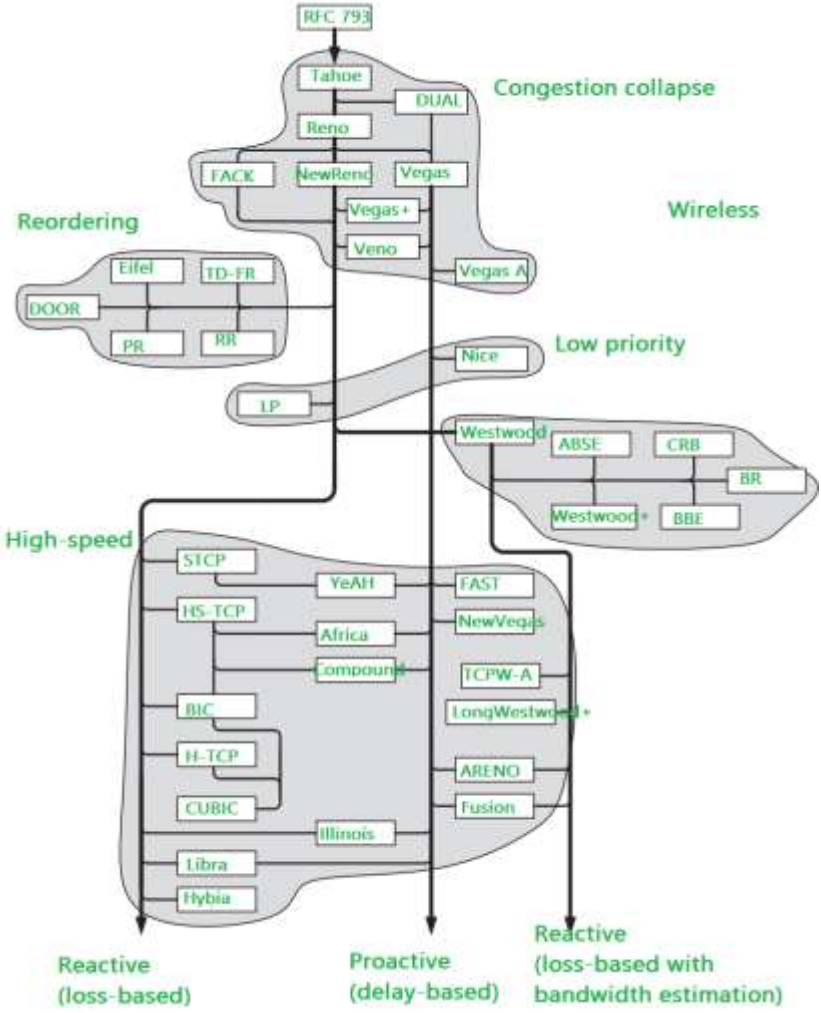
Format RFC (*Request for Comments*) diperkenalkan pada tahun 1969 sebagai bagian dari inisiatif ARPANET (*Advanced Research Projects Agency Network*). RFC adalah saluran publikasi resmi IETF, yang merupakan singkatan dari Internet Engineering Task Force. Satuan Tugas Rekayasa Internet (IETF) adalah Dewan Arsitektur Internet (IAB); itu adalah komunitas peneliti jaringan komputer di seluruh dunia (Pintusaini, 2022).

Perkembangan TCP dan IP dimulai pada tahun 1970-an. Pada tahun 1974, Vinton Cerf dan Robert Kahn mempresentasikan makalah pertama di internet pada konferensi IEEE Transactions on Communications, berjudul "*A Protocol for Packet Network Intercommunication.*" Pada bulan Desember 1974, "Specification of Internet Transmission Control Program" (RFC 675) diterbitkan oleh Vinton Cerf, Yogen Dalal, dan Carl Sunshine. Pada tahun 1974, RFC 675 asli tidak berfungsi sepenuhnya, sehingga penulis diminta untuk merevisi dokumen tersebut. Akhirnya, pada tahun 1981, spesifikasi 'v4' dari TCP/IP diterbitkan setelah beberapa revisi. Kali ini, ada dua RFC yang berbeda (Pintusaini, 2022):

1. "Protokol Internet" adalah subjek dari RFC 791.
2. "Protokol Kontrol Transmisi" adalah RFC 793.

'v4' di IPv4 adalah warisan koneksinya ke TCP; tidak ada protokol IPv1, IPv2, atau IPv3 yang berdiri sendiri. Jadi, 'v4' dalam IPv4 mengacu pada iterasi keempat dari RFC Internet asli yang pernah diterbitkan. Oleh karena itu, Vinton Cerf, Yogen Dalal, dan Robert Kahn diakui sebagai bapak Internet. Yogen Dalal adalah lulusan IIT Bombay dan keturunan India.

Tahun 1994 menandai awal pengerjaan "*Internet Protocol next generation* (IPng)". Karena konvensi penamaan, IPng diganti namanya menjadi IPv6 (istilah resmi *Internet Protocoling*). IPng adalah singkatan dari IP next generation. Dalam setengah abad terakhir, TCP dan IP telah mengalami revisi yang signifikan. Sampai saat ini, lebih dari 100 varian TCP telah diusulkan dalam literatur. Kernel Linux mendukung 10+ varian TCP (CUBIC TCP adalah default). Sejak 2014, macOS telah menggunakan CUBIC secara default, dan sejak 2017, Microsoft Windows juga menggunakannya (Pintusaini, 2022).



Gambar 2.3. Evolusi TCP
(Sumber: Pintusaini, 2022)

RFC 793, Makalah ini adalah yang pertama membahas Internet dan TCP. Itu termasuk setiap fitur dengan pengecualian

kontrol kemacetan. Itu termasuk dimulai dengan varian berikutnya. Tidak diketahui pada saat itu bahwa internet akan menjadi begitu umum dan maju dalam dekade-dekade berikutnya. Header TCP akan menemui banyak kendala di masa depan. Oleh karena itu, bidang opsi ditambahkan ke tajuk TCP untuk persiapan pengoptimalan di masa mendatang.

TCP Tahoe adalah varian TCP pertama yang menggabungkan algoritma kontrol kemacetannya sendiri. Itu memiliki keterbatasan, kemudian TCP Reno mengembangkan solusi, dll.

TCP NewReno menguasai internet selama sepuluh tahun; sekarang menjadi TCP default di macOS; TCP CUBIC telah mendominasi dunia selama lima belas tahun terakhir.

Awalnya, TCP tidak mewakili apa yang diwakilinya saat ini. Awalnya, itu adalah aplikasi kontrol Transmisi. Itu dirancang untuk memungkinkan komunikasi antara dua komputer yang jauh dengan mengirimkan data dalam paket. TCP menjadi protokol komunikasi Internet standar. Tujuan penemunya adalah untuk membuat jaringan antara dua komputer yang, tidak seperti UDP, dapat menjamin pengiriman paket yang aman.

Saat ini, Internet menggunakan protokol TCP dan IP untuk tujuan yang berbeda untuk mencapai satu tujuan. IP adalah protokol tingkat jaringan, sedangkan TCP adalah protokol tingkat transportation menurut model OSI (*Open System Interconnection*) lima lapis. *Transmission Control Protocol* (TCP) adalah protokol lapisan atas. IP menambahkan alamat tujuan dari ujung penerima ke transmisi. TCP bertanggung jawab untuk membangun koneksi yang aman dan andal antara dua node yang berkomunikasi dan mentransmisikan data dari ujung pengirim ke ujung penerima. TCP bersifat dua arah dan mampu mengirim dan menerima paket secara bersamaan.

2.6 Bagaimana cara kerja TCP/IP?

Protokol TCP/IP menggunakan model komunikasi klien-server, di mana komputer di dalam jaringan (disebut sebagai server) menawarkan layanan, seperti mentransmisikan halaman web, ke komputer lain (disebut sebagai klien). Paket protokol TCP/IP diklasifikasikan sebagai stateless, menunjukkan bahwa setiap permintaan klien dianggap berbeda karena tidak memiliki koneksi atau korelasi dengan permintaan sebelumnya. Menurut Shacklett (2021), kondisi tanpa kewarganegaraan memungkinkan pemanfaatan jalur jaringan secara terus menerus.

Namun demikian, penting untuk dicatat bahwa lapisan transport memperlihatkan perilaku stateful. Proses transmisi melibatkan pengiriman pesan tunggal, dengan koneksi dipertahankan sampai semua paket individu yang terdiri dari pesan berhasil diterima dan dipasang kembali di tujuan yang dituju.

Model TCP/IP memiliki sedikit variasi jika dibandingkan dengan model *Open System Interconnection* (OSI), yang berfungsi sebagai kerangka dasarnya. Model referensi OSI menggambarkan cara di mana aplikasi jaringan dapat membangun komunikasi.

Pentingnya TCP/IP terletak pada kekritisannya. Paket protokol TCP/IP diklasifikasikan sebagai standar terbuka, sehingga menandakan bahwa itu tidak tunduk pada kontrol eksklusif oleh entitas tunggal mana pun. Oleh karena itu, *Internet Protocol suite* dapat dengan mudah dimodifikasi. Perangkat lunak ini menunjukkan kompatibilitas dengan banyak sistem operasi (OS), memfasilitasi komunikasi tanpa batas antara berbagai komputer. Selain itu, perlu dicatat bahwa suite IP menunjukkan interoperabilitas dengan berbagai perangkat keras dan jaringan komputer, seperti yang disoroti oleh Shacklett (2021).

TCP/IP adalah protokol yang dapat dirutekan yang menunjukkan tingkat skalabilitas tinggi dan memiliki kemampuan

untuk memastikan jalur jaringan yang optimal. Ini banyak digunakan dalam arsitektur internet modern.

Tujuan utama TCP/IP adalah untuk memfasilitasi transmisi data komputer antar perangkat. Prasyarat mendasar dari operasi ini adalah kebutuhan data untuk memiliki keandalan dan akurasi, memastikan bahwa penerima memperoleh informasi yang identik dengan yang diberikan oleh pengirim. Untuk menjamin pengiriman yang akurat dari setiap pesan, model TCP/IP menerapkan strategi membagi datanya ke dalam paket-paket. Paket-paket ini kemudian dipasang kembali di ujung penerima, dengan demikian menjaga integritas data yang dikirim (Jain, 2023).

2.7 4 Lapisan model TCP/IP

Fungsionalitas TCP/IP diatur ke dalam empat lapisan berbeda, yang masing-masing mencakup seperangkat protokol (Shacklett, 2021).

1. *Application layer* memungkinkan aliran data standar di berbagai aplikasi. Protokol yang digunakan oleh sistem termasuk HTTP, FTP, Post Office Protocol 3, Simple Mail Transfer Protocol, dan Simple Network Management Protocol. Muatan yang ada di lapisan aplikasi mengacu pada data aplikasi faktual.
2. Transportation layer bertanggung jawab untuk memastikan integritas dan keandalan komunikasi jaringan end-to-end. *Transmission Control Protocol* (TCP) bertanggung jawab atas manajemen komunikasi antar host, termasuk fungsi penting seperti kontrol aliran, multiplexing, dan ketergantungan. Protokol transport mencakup TCP dan *User Datagram Protocol* (UDP), dengan yang terakhir kadang-kadang digunakan sebagai pengganti TCP dalam konteks tertentu.
3. Network layer, biasanya disebut sebagai lapisan internet, bertanggung jawab untuk mengelola paket dan membangun koneksi antara jaringan yang berbeda untuk memfasilitasi

transmisi paket melewati batas jaringan. Protokol lapisan jaringan, yaitu IP dan *Internet Control Message Protocol* (ICMP), melayani tujuan pelaporan kesalahan.

4. *Physics layer*, sebagai alternatif disebut sebagai lapisan antarmuka jaringan atau lapisan tautan data, terdiri dari protokol yang dirancang khusus untuk berfungsi pada tautan, yang merupakan elemen jaringan yang bertanggung jawab untuk menghubungkan node dan host. Protokol yang tercakup dalam strata terendah adalah Ethernet untuk jaringan area lokal dan Protokol Resolusi Alamat.

Paket protokol TCP/IP dapat digunakan untuk memfasilitasi login jaringan jarak jauh untuk transmisi file interaktif, pengiriman email dan halaman web berbasis jaringan, serta akses jarak jauh ke sistem file host server. Tujuan dari konsep ini adalah untuk menggambarkan transformasi informasi saat melintasi dari lapisan fisik nyata ke lapisan aplikasi konseptual dalam jaringan. Pernyataan ini menjelaskan protokol penting atau mekanisme komunikasi yang digunakan di setiap tingkatan saat informasi melintas melalui sistem.

2.8 Kelebihan dan kekurangan TCP/IP

Pemanfaatan model TCP/IP menghasilkan keuntungan tertentu, sebagaimana digariskan oleh Shacklett (2021).

1. Perangkat lunak ini memfasilitasi pembentukan korelasi antar model komputer yang beragam. Ini beroperasi secara independen dari sistem operasi yang mendasarinya dan menyediakan dukungan untuk berbagai protokol perutean.
2. Sistem ini menggunakan arsitektur client-server yang sangat terukur. Ini memiliki kemampuan untuk beroperasi secara mandiri dan kompatibel dengan banyak protokol routing.

3. Perangkat lunak ini dicirikan oleh sifatnya yang ringan, yang memastikan tidak membebani mesin atau jaringan secara berlebihan.

Salah satu kelemahan yang terkait dengan TCP/IP, seperti yang diidentifikasi oleh Shacklett (2021), adalah sebagai berikut:

1. Konfigurasi dan pengelolaan sistem memberikan tantangan, karena lapisan transport tidak memiliki jaminan untuk pengiriman paket.
2. Ada beberapa tantangan terkait penggantian protokol TCP/IP. Pertama, framework tidak memiliki diferensiasi eksplisit antara layanan, antarmuka, dan protokol, membuatnya tidak memadai untuk mendeskripsikan teknologi baru dalam jaringan yang muncul. Selain itu, TCP/IP sangat rentan terhadap serangan sinkronisasi, suatu bentuk serangan *denial-of-service* yang mengeksploitasi mekanisme sinkronisasi.

2.9 Bagaimana TCP/IP berbeda dari IP?

Ada beberapa perbedaan mencolok antara TCP/IP dan IP. Salah satu contoh protokol internet tingkat rendah adalah IP, yang memfasilitasi transmisi data melalui internet. Tujuan utama dari sistem ini adalah untuk memfasilitasi pengiriman paket data. Paket-paket ini terdiri dari header yang berisi detail navigasi terkait, seperti asal dan tujuan data, serta muatan data aktual.

Kapasitas transmisi IP terbatas dalam hal jumlah data yang dapat ditransmisikan. Panjang maksimum paket data IP tunggal, yang mencakup header dan data, berkisar antara 20 hingga 24 byte. Konsekuensinya, urutan data yang lebih panjang perlu dipartisi menjadi beberapa paket data, yang kemudian ditransmisikan secara mandiri dan selanjutnya disusun kembali dalam urutan yang sesuai.

Karena sifatnya yang melekat sebagai protokol kirim/terima, IP tidak memiliki mekanisme yang melekat untuk

memverifikasi keberhasilan penerimaan paket data yang dikirimkan. Protokol TCP/IP adalah sistem komunikasi yang canggih dan maju yang menawarkan kemampuan yang ditingkatkan dibandingkan dengan protokol IP. Rangkaian protokol TCP/IP menggunakan IP sebagai mekanisme dasarnya untuk mentransmisikan paket data, sekaligus memfasilitasi interkoneksi komputer, aplikasi, situs web, dan server web. Protokol Kontrol Transmisi (TCP) memiliki pemahaman komprehensif tentang keseluruhan aliran data yang diperlukan untuk memfungsikan aset ini. Ini menjamin keberhasilan transmisi volume data lengkap dalam satu upaya. Menurut Shacklett (2021), TCP menggabungkan mekanisme untuk memastikan pengiriman data yang andal.

Sambil memenuhi tanggung jawabnya, *Transmission Control Protocol* (TCP) mampu mengelola dan mengendalikan besarnya dan kecepatan transmisi data. Ini menjamin tidak adanya kemacetan jaringan yang dapat menghambat penerimaan data.

Salah satu contohnya adalah aplikasi yang bermaksud untuk mengirimkan sejumlah besar data melalui internet. Jika program hanya bergantung pada IP, maka perlu mempartisi data menjadi banyak paket IP. Mengingat bahwa permintaan IP dihasilkan berdasarkan per-paket, maka perlu membuat beberapa permintaan untuk mengirim dan menerima data.

Transmission Control Protocol (TCP) mampu mentransmisikan seluruh aliran data dengan satu permintaan, karena secara efisien mengelola data yang tersisa. Berbeda dengan IP, TCP memiliki kemampuan untuk mengidentifikasi masalah yang mungkin timbul dengan IP dan memulai proses transmisi ulang untuk setiap paket data yang telah hilang. *Transmission Control Protocol* (TCP) memiliki kemampuan untuk mengatur ulang paket secara efektif, sehingga memastikan pengirimannya dalam urutan yang tepat, sekaligus mengurangi kemacetan jaringan. Menurut Shacklett (2021), TCP/IP memainkan peran

penting dalam memungkinkan pengangkutan data melalui Internet.

2.10 Model OSI vs. TCP/IP

Departemen Pertahanan AS (DoD) mengembangkan *Transfer Control Protocol/Internet Protocol* (TCP/IP) sebelum model OSI. TCP/IP lebih sederhana, meruntuhkan beberapa lapisan OSI menjadi satu lapisan, yang merupakan perbedaan signifikan antara kedua model (Imperva.com, 2023).

1. TCP/IP menggabungkan lapisan OSI 5, 6, dan 7 ke dalam satu Lapisan Aplikasi.
2. TCP/IP menggabungkan OSI layer 1 dan 2 menjadi satu Network Access Layer; namun, TCP/IP tidak bertanggung jawab atas fungsi pengurutan dan pengakuan; ini ditangani oleh lapisan transport yang mendasarinya.

Variasi signifikan lainnya:

1. TCP/IP adalah model fungsional yang dirancang untuk mengatasi masalah komunikasi tertentu dan berdasarkan protokol standar. OSI adalah model generik yang tidak tergantung protokol yang dirancang untuk mengkarakterisasi semua jenis komunikasi jaringan.
2. Dalam TCP/IP, sebagian besar aplikasi menggunakan ketujuh lapisan, sedangkan aplikasi dasar OSI tidak. Hanya lapisan 1, 2, dan 3 yang diperlukan untuk komunikasi data.

Model TCP/IP dan OSI mungkin tampak hanya memiliki perbedaan kecil, tetapi komposisi, fitur, fungsi, dan tujuannya sangat berbeda. Perbedaan antara kedua istilah tersebut juga penting untuk Ujian IAS (Karthik JU'S, 2023).

Transmission Control Protocol/Internet Protocol (TCP/IP) adalah rangkaian protokol komunikasi yang memungkinkan perangkat jaringan terhubung ke Internet. Sebaliknya, Interkoneksi

Sistem Terbuka atau Model OSI adalah kerangka kerja konseptual yang digunakan untuk menggambarkan pengoperasian jaringan. Model jaringan TCP/IP dan OSI dibandingkan dalam tabel di bawah ini. Anda harus benar-benar meninjau perbedaan penting berikut antara keduanya:

Tabel 2.1. Analisis Komparatif TCP/IP vs Model OSI

Perbedaan antara TCP/IP dan Mode OSI	
TCP/IP	**Model OSI**
Bentuk lengkap dari TCP/IP adalah Transmission Control Protocol/Internet Protocol.	Bentuk lengkap dari OSI adalah Interkoneksi Sistem Terbuka.
Ini adalah protokol komunikasi berdasarkan protokol standar yang memungkinkan koneksi jaringan host.	Ini adalah model terstruktur yang membahas pengoperasian jaringan..
Model TCP/IP menjadi bahasa ARPANET kanonik pada tahun 1982.	Pada tahun 1984, International Organization for Standardization (ISO) memperkenalkan model OSI.
Ini terdiri dari empat lapisan: ● Network Interface ● Internet ● Transport ● Application	Ini terdiri dari tujuh lapisan: ● Physical ● Data link ● Network ● Transport ● Session ● Presentation ● Application
Ini mengikuti pendekatan horizontal.	Ini mengikuti pendekatan vertikal.
TCP/IP adalah implementasi Model OSI.	Berdasarkan Model Referensi OSI, sebuah jaringan dibangun.
Itu tergantung protokol.	Ini adalah protokol independen.

Sumber: (Karthik JU'S, 2023)

Perbandingan yang ditunjukkan pada Tabel 2.1 ini mengilustrasikan perbedaan antara model TCP/IP dan OSI dengan jelas.

Namun, ada beberapa kesamaan antara keduanya, seperti yang dijelaskan di bawah ini. Ada kesamaan antara model TCP/IP dan OSI (Karthik JU'S, 2023).

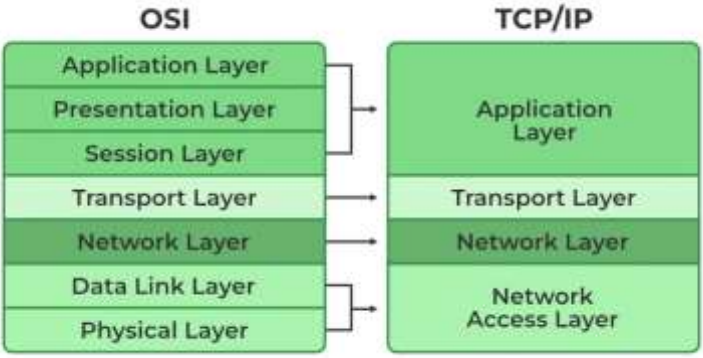
1. Kedua model didasarkan pada organisasi bertingkat.
2. Dalam kedua model, data terutama digunakan untuk mengubah data yang belum diproses menjadi paket dan mengirimkannya ke node tujuan.
3. Protokol didefinisikan lapis demi lapis di kedua arsitektur.
4. Lapisan model dibandingkan satu sama lain. Lapisan fisik model OSI dan lapisan tautan data sesuai dengan lapisan tautan model TCP/IP.
5. Lapisan aplikasi model TCP/IP terdiri dari lapisan sesi, lapisan presentasi, dan lapisan aplikasi model OSI.
6. Dalam kedua konfigurasi, lapisan jaringan dan transport adalah sama.

TCP/IP dan OSI adalah protokol komunikasi jaringan yang paling populer. Perbedaan utamanya adalah bahwa OSI adalah paradigma konseptual yang tidak digunakan untuk komunikasi dalam praktiknya. Sebaliknya, itu menentukan bagaimana aplikasi dapat berkomunikasi melalui jaringan. Di sisi lain, TCP/IP banyak digunakan untuk membangun koneksi dan interaksi jaringan.

Protokol TCP/IP menentukan standar di mana Internet dibangun, sedangkan model OSI menentukan bagaimana komunikasi harus dilakukan. Oleh karena itu, TCP/IP adalah model yang lebih praktis.

Model TCP/IP dan OSI berbagi dan memiliki perbedaan. TCP/IP hanya terdiri dari empat lapisan, sedangkan model OSI terdiri dari tujuh lapisan berikut: physics, Data Link, Network, Presentation, Transportation, dan Session. Lapisan aplikasi adalah

lapisan atas dari model TCP/IP dan model OSI. Terlepas dari kenyataan bahwa lapisan ini melakukan tugas yang sama di setiap model, tugas tersebut dapat bervariasi tergantung pada data yang diterima oleh masing-masing model.



Gambar 2.4. Perbandingan diagram model TCP/IP dan OSI (Sumber: Mary E. Shacklett, 2021)

Karena masing-masing model beroperasi pada lapisan jaringan dan lapisan transport, fungsi yang dilakukan oleh masing-masing model juga serupa. Model TCP/IP dan OSI keduanya terutama digunakan untuk transmisi paket data. Meskipun mereka akan tiba di tempat tujuan dengan berbagai cara dan rute, mereka tetap akan melakukannya.

Model TCP/IP dan model OSI berbagi karakteristik sebagai berikut:

1. Keduanya adalah model logis.
2. Mereka menetapkan standar jaringan.
3. Mekanisme komunikasi jaringan dipisahkan menjadi beberapa lapisan.
4. Mereka menawarkan kerangka kerja untuk pengembangan dan penerapan standar dan perangkat jaringan.
5. Mereka mengizinkan satu produsen untuk memproduksi perangkat dan komponen jaringan yang dapat hidup

berdampingan dan berfungsi dengan yang diproduksi oleh produsen lain.

Berikut ini adalah perbedaan antara model TCP/IP dan model OSI:

1. TCP/IP mendefinisikan fungsionalitas lapisan atas hanya menggunakan satu lapisan (aplikasi), sedangkan OSI menggunakan tiga lapisan (aplikasi, presentasi, dan sesi).
2. TCP/IP mendefinisikan fungsionalitas lapisan bawah menggunakan satu lapisan (fisik), sedangkan OSI menggunakan dua lapisan (fisik dan tautan data).
3. Header TCP/IP berukuran 20 byte, sedangkan header OSI berukuran 5 byte.
4. OSI adalah paradigma umum yang didasarkan pada fungsionalitas setiap lapisan, sedangkan TCP/IP adalah standar yang berpusat pada protokol.
5. TCP/IP mengambil pendekatan horizontal, sedangkan OSI mengambil pendekatan vertikal.
6. Dalam TCP/IP, protokol dirancang terlebih dahulu, diikuti oleh model. Di OSI, model dibuat terlebih dahulu, diikuti oleh protokol untuk setiap lapisan.
7. OSI membantu membakukan router, switch, motherboard, dan perangkat keras lainnya, sedangkan TCP/IP membantu membangun koneksi antara berbagai jenis komputer.

DAFTAR PUSTAKA

Imperva.com. 2023. *What Is the OSI Model*, *imperva.com*. Available at: https://www.imperva.com/learn/application-security/osi-model/ (Accessed: 16 Agustus 2023).

Jain, P. 2023. *TCP/IP Model*, *geeksforgeeks.org*. Available at: https://www.geeksforgeeks.org/tcp-ip-model/ (Accessed: 16 August 2023).

Karthik JU'S. 2023. *Difference Between TCP/IP and OSI Model*, *byjus.com*. Available at: https://byjus.com/free-ias-prep/difference-between-tcp-ip-and-osi-model/#:~:text=The TCP%2FIP or the,a network can be described. (Accessed: 16 Agustus 2023).

Mary E. Shacklett. 2021. *What is TCP/IP*, *techtarget.com*. Available at: https://www.techtarget.com/searchnetworking/definition/TCP-IP (Accessed: 16 Agustus 2023).

OSI model. 2023. *wikipedia.org*. Available at: https://en.wikipedia.org/wiki/OSI_model (Accessed: 16 August 2023).

Pintusaini. 2022. *History of TCP/IP*, *geeksforgeeks.org*. Available at: https://www.geeksforgeeks.org/history-of-tcp-ip/ (Accessed: 16 Agustus 2023).

BAB 3
TEKNOLOGI JARINGAN NIRKABEL

Oleh Arief Yanto Rukmana

3.1 Pendahuluan

Teknologi jaringan nirkabel merupakan landasan konektivitas modern, memungkinkan transmisi data tanpa memerlukan kabel fisik (Kizza et al., 2013). Teknologi ini bergantung pada perambatan gelombang elektromagnetik, khususnya gelombang radio, untuk memfasilitasi komunikasi antar perangkat pada jarak yang berbeda-beda. Mendalami komponen-komponen utama dan prinsip-prinsip teknologi jaringan nirkabel sangat penting dalam dunia kita yang saling terhubung (Jacob & Darney, 2021).

Inti dari teknologi nirkabel adalah gelombang radio, yang menjangkau berbagai frekuensi dalam spektrum elektromagnetik. Gelombang ini berfungsi sebagai pembawa untuk transmisi data antar perangkat nirkabel (Strinati & Barbarossa, 2021). Frekuensi dan panjang gelombang gelombang ini menentukan karakteristik perambatannya, mempengaruhi faktor-faktor seperti jangkauan sinyal dan penetrasi melalui rintangan(Olenik et al., 2021).

Modulasi adalah teknik dasar dalam komunikasi nirkabel, yang melibatkan variasi satu atau lebih sifat sinyal pembawa untuk menyandikan data digital (Mughal, 2022). Modulasi Amplitudo (AM), Modulasi Frekuensi (FM), dan Modulasi Fase (PM) adalah metode modulasi analog yang umum. Untuk data digital, skema modulasi seperti Binary Phase Shift Keying (BPSK), Quadrature Phase Shift Keying (QPSK), dan lainnya digunakan untuk menyandikan informasi ke sinyal pembawa (Eid et al., 2021).

Demodulasi adalah proses kebalikan dari modulasi, mengekstraksi data asli dari sinyal yang diterima (Kiesler, 1986). Ini adalah langkah penting dalam komunikasi nirkabel, karena memungkinkan perangkat menafsirkan dan menggunakan informasi yang dikirimkan secara akurat (Alani & Al-Sadi, 2023). Demodulasi membalikkan perubahan yang diterapkan selama modulasi, mengembalikan data ke bentuk aslinya untuk diproses (Long et al., 2021).

Keamanan jaringan nirkabel sangat penting untuk melindungi data dari akses dan pelanggaran yang tidak sah. Enkripsi memainkan peran sentral dalam keamanan nirkabel, mengacak data selama transmisi dan membuatnya tidak dapat dibaca oleh pengguna yang tidak berwenang. Protokol seperti WPA2 dan WPA3 menggunakan algoritma enkripsi yang kuat untuk melindungi komunikasi nirkabel (Tang et al., 2019).

Jaringan nirkabel menggunakan titik akses (AP) untuk menjembatani kesenjangan antara perangkat nirkabel dan infrastruktur kabel. AP mengirim dan menerima data antara klien nirkabel dan jaringan pusat, sehingga memperluas jangkauan jaringan (Pamarthi & Narmadha, 2022). Penempatan dan konfigurasinya yang strategis sangat penting untuk menentukan jangkauan dan kinerja jaringan (Marin, 2005).

Beberapa perangkat nirkabel dapat hidup berdampingan di area yang sama, sehingga menimbulkan potensi interferensi dan kemacetan (Sadiku & Akujuobi, 2022). Teknologi nirkabel menggunakan berbagai teknik untuk mengurangi tantangan ini. Pita frekuensi, saluran, dan teknik seperti keragaman spasial digunakan untuk mengoptimalkan kualitas sinyal dan meminimalkan interferensi (Lalit et al., 2022).

Teknologi jaringan nirkabel bergantung pada transmisi data melalui gelombang elektromagnetik, menggunakan teknik modulasi dan demodulasi untuk menyandikan dan mendekode informasi. Spektrum elektromagnetik, gelombang radio, titik akses,

dan langkah-langkah keamanan merupakan komponen integral dari teknologi nirkabel. Memahami prinsip-prinsip ini sangat penting untuk merancang, menerapkan, dan memelihara jaringan nirkabel yang efisien dan aman di dunia yang saling terhubung secara digital (Wakil et al., 2022).

3.2 Dasar-dasar Komunikasi Nirkabel

Komunikasi nirkabel adalah tulang punggung konektivitas modern, memungkinkan pertukaran informasi tanpa koneksi fisik (Hammond & O'Reilly, 1986). Hal ini bergantung pada perambatan gelombang elektromagnetik melalui udara, memanfaatkan pita frekuensi tertentu dalam spektrum radio (Elsayed & Erol-Kantarci, 2019). Gelombang elektromagnetik ini berfungsi sebagai pembawa transmisi data dalam jaringan nirkabel, dan memahami karakteristiknya merupakan hal mendasar untuk efektif dalam mendalami lebih lanjut terkait dasar dasar komunikasi nirkabel (Kang et al., 2021).

Spektrum elektromagnetik mencakup rentang frekuensi yang luas, dengan setiap pita frekuensi cocok untuk berbagai jenis komunikasi nirkabel. Gelombang radio, yang termasuk dalam spektrum, sangat penting untuk teknologi nirkabel. Melakukan perjalanan melalui ruang angkasa dalam bentuk medan listrik dan magnet yang berosilasi dan dapat merambat dalam jarak yang bervariasi, tergantung pada frekuensi dan energinya. Perilaku propagasi ini mempengaruhi jangkauan dan keandalan jaringan nirkabel (Kizza et al., 2013).

Modulasi dan demodulasi adalah teknik kunci dalam komunikasi nirkabel. Modulasi melibatkan memvariasikan satu atau lebih properti sinyal pembawa, seperti amplitudo, frekuensi, atau fase, untuk menyandikan data digital. Modulasi Amplitudo (AM), Modulasi Frekuensi (FM), dan Modulasi Fase (PM) adalah teknik modulasi analog yang umum, sedangkan skema modulasi digital seperti Penguncian Pergeseran Fasa Biner (BPSK),

Penguncian Pergeseran Fasa Kuadratur (QPSK), dan Penguncian Pergeseran Frekuensi (QPSK), dan Penguncian Pergeseran Frekuensi (FSK) digunakan untuk transmisi data digital (Eid et al., 2021).

Pilihan skema modulasi bergantung pada faktor-faktor seperti kecepatan data, rasio signal-to-noise, dan bandwidth yang tersedia. Misalnya, BPSK cocok untuk aplikasi dengan kecepatan data rendah, sedangkan QPSK dan skema modulasi tingkat tinggi digunakan untuk kecepatan data yang lebih tinggi. Selain itu, teknik modulasi ini sensitif terhadap noise dan interferensi, yang dapat menurunkan kualitas sinyal (Dai et al., 2019).

Dalam komunikasi nirkabel, data digital harus dimodulasi ke sinyal pembawa untuk transmisi, dan di ujung penerima, proses demodulasi digunakan untuk mengekstrak informasi asli (Yu et al., 2022). Demodulasi membalikkan proses modulasi, memulihkan data digital dari sinyal yang diterima. Proses ini sangat penting untuk mengirimkan dan menerima data secara akurat dalam jaringan nirkabel (Tang et al., 2019).

Komunikasi nirkabel mengandalkan transmisi data melalui gelombang elektromagnetik dalam spektrum radio (Forouzan & Mukhopadhyay, 2015). Memahami dasar-dasar spektrum elektromagnetik, teknik modulasi, dan demodulasi sangat penting untuk merancang dan mengoperasikan sistem komunikasi nirkabel yang efektif (Rukmana, 2023a). Konsep-konsep ini mendasari fondasi teknologi nirkabel dan penerapannya di dunia yang saling terhubung (Rukmana et al., 2023).

3.3 Topologi Jaringan Nirkabel

Topologi jaringan nirkabel menentukan bagaimana perangkat dalam jaringan nirkabel saling terhubung dan berkomunikasi satu sama lain (Peterson & Davie, 2007). Topologi ini menentukan struktur dan aliran data dalam jaringan. Ada

beberapa topologi jaringan nirkabel yang umum, masing-masing memiliki kelebihan dan kekurangannya sendiri (Kaeo, 2004).

Tautan nirkabel *Point-to-Point* adalah bentuk topologi jaringan nirkabel yang paling sederhana. Dalam pengaturan ini, dua perangkat berkomunikasi secara langsung satu sama lain. Ini adalah metode langsung untuk membuat koneksi antara dua titik, biasanya dalam jarak dekat. Tautan *Point-to-Point* dapat dikonfigurasi untuk komunikasi simpleks (komunikasi satu arah) atau komunikasi dupleks penuh (komunikasi dua arah), tergantung pada kebutuhan (Fernando et al., 2023).

LAN Nirkabel (WLAN) lazim di rumah dan bisnis. Jaringan ini menggunakan mode infrastruktur atau ad-hoc. Dalam mode infrastruktur, perangkat nirkabel terhubung ke hub pusat, yang dikenal sebagai titik akses (AP), yang mengontrol dan mengelola jaringan. Mode ad-hoc, di sisi lain, memungkinkan perangkat untuk terhubung langsung satu sama lain tanpa memerlukan titik akses pusat (Quarterman & Hoskins, 1986).

Wireless Metropolitan Area Networks (WMAN) dirancang untuk mencakup wilayah yang lebih luas, seperti kota besar atau kecil. Standar IEEE 802.16, umumnya dikenal sebagai WiMAX, sering digunakan untuk WMAN. WiMAX menyediakan akses broadband nirkabel berkecepatan tinggi melalui area yang lebih luas dibandingkan WLAN, sehingga cocok untuk menyediakan akses internet ke komunitas yang lebih luas (Dooley et al., 2018).

Wireless Wide Area Networks (WWAN) mencakup wilayah geografis yang lebih luas dan umumnya dikaitkan dengan jaringan seluler. Teknologi seluler seperti 3G, 4G, dan 5G memungkinkan komunikasi nirkabel dalam jarak yang luas (Rukmana & Sudarmanto, 2023). Jaringan ini digunakan untuk komunikasi seluler, memungkinkan pengguna melakukan panggilan suara, mengirim pesan teks, dan mengakses internet hampir dari mana saja (Sjioen et al., 2023).

Jaringan mesh adalah topologi nirkabel yang fleksibel dan kuat. Dalam jaringan mesh, setiap perangkat tidak hanya berkomunikasi dengan hub pusat tetapi juga dengan perangkat lain di dekatnya. Hal ini menciptakan redundansi dan meningkatkan keandalan jaringan karena data dapat menempuh banyak jalur untuk mencapai tujuannya (Peterson & Davie, 2007). Jaringan mesh sering digunakan dalam skenario dimana jangkauan jaringan perlu diperluas, seperti di rumah pintar atau lingkungan luar ruangan (Marin, 2005).

Arsitektur jaringan hybrid menggabungkan elemen topologi yang berbeda untuk memenuhi kebutuhan tertentu. Misalnya, suatu jaringan mungkin menggunakan kombinasi tautan point-to-point, WLAN, dan jaringan mesh untuk menyediakan cakupan komprehensif dan transfer data yang efisien dalam lingkungan yang kompleks (Almaiah et al., 2022).

Topologi jaringan nirkabel menentukan bagaimana perangkat terhubung dan berkomunikasi dalam jaringan nirkabel. Pilihan topologi bergantung pada faktor-faktor seperti ukuran jaringan, area jangkauan, dan persyaratan spesifik aplikasi (Davronbekov, 2020). Memahami topologi ini sangat penting untuk merancang dan menerapkan jaringan nirkabel yang memenuhi kebutuhan berbagai skenario, mulai dari jaringan rumah lokal hingga wilayah metropolitan yang luas (Kang et al., 2021).

3.4 Arsitektur Jaringan Nirkabel

Arsitektur jaringan nirkabel menentukan struktur dan organisasi jaringan nirkabel, memberikan cetak biru bagaimana perangkat berkomunikasi dan berkolaborasi dalam jaringan (Cilfone et al., 2019). Arsitektur ini dirancang untuk memenuhi persyaratan operasional dan fungsional tertentu (Davronbekov, 2020). Di sini, kita mempelajari beberapa arsitektur jaringan nirkabel utama:

Jaringan Infrastruktur berfungsi sebagai landasan bagi banyak pengaturan nirkabel. Dalam arsitektur ini, titik akses (AP) memainkan peran sentral. AP bertindak sebagai perantara yang menghubungkan perangkat nirkabel ke jaringan kabel. Mengontrol komunikasi dan mengatur lalu lintas jaringan (Long et al., 2021). Jaringan infrastruktur biasanya digunakan di rumah, bisnis, dan hotspot Wi-Fi publik, menyediakan cara yang terstruktur dan efisien untuk memperluas akses internet secara nirkabel (Dai et al., 2019).

Jaringan Peer-to-Peer, juga dikenal sebagai jaringan ad-hoc, berbeda dari jaringan infrastruktur. Dalam arsitektur ini, perangkat nirkabel berkomunikasi langsung satu sama lain, sehingga tidak memerlukan titik akses pusat. Jaringan peer-to-peer berguna dalam situasi di mana jaringan infrastruktur tidak praktis, seperti koneksi sementara antar perangkat atau dalam skenario pemulihan bencana. Sangat fleksibel namun kurang efisien untuk penerapan skala besar (Ebi et al., 2019).

Arsitektur Terpusat memperkenalkan pengontrol atau koordinator terpusat yang mengelola operasi jaringan. Arsitektur ini tipikal dalam pengaturan perusahaan, khususnya untuk LAN nirkabel (WLAN). Pengontrol bertanggung jawab atas tugas-tugas seperti kontrol akses, penegakan keamanan, dan penyeimbangan beban (Kaeo, 2004). Hal ini memastikan manajemen jaringan yang seragam dan kebijakan yang konsisten di semua perangkat yang terhubung (Jacob & Darney, 2021).

Arsitektur Terdistribusi, berbeda dengan arsitektur terpusat, mendistribusikan kecerdasan dan kontrol jaringan ke beberapa perangkat. Setiap perangkat, sering kali merupakan titik akses, mengelola segmen jaringannya secara independen (Ak & Canberk, 2021). Pendekatan terdesentralisasi ini bisa lebih tangguh dan terukur, sehingga cocok untuk lingkungan nirkabel yang lebih besar dan kompleks. Jaringan mesh adalah contoh utama arsitektur terdistribusi (Olenik et al., 2021).

Jaringan Mesh adalah arsitektur nirkabel serbaguna yang dicirikan oleh node-node yang saling berhubungan. Dalam jaringan mesh, setiap perangkat dapat berkomunikasi dengan beberapa perangkat tetangga, menciptakan banyak jalur untuk dilalui data (Tawalbeh et al., 2020). Redundansi ini meningkatkan keandalan jaringan dan memperluas jangkauan. Jaringan mesh unggul dalam skenario dimana cakupan yang kuat dan toleransi kesalahan sangat penting, seperti di kota pintar atau penerapan sensor skala besar (Elsayed & Erol-Kantarci, 2019).

Arsitektur Hibrid menggabungkan elemen berbagai arsitektur untuk memenuhi kebutuhan spesifik. Misalnya, jaringan hybrid mungkin menggabungkan elemen infrastruktur dan arsitektur mesh untuk menyediakan jangkauan Wi-Fi yang lancar di dalam dan di luar ruangan. Jaringan ini dapat disesuaikan untuk memenuhi tuntutan operasional tertentu dan mengoptimalkan kinerja dan keandalan (Wei et al., 2021).

Arsitektur jaringan nirkabel menyediakan kerangka struktural untuk komunikasi nirkabel. Pilihan arsitektur bergantung pada faktor-faktor seperti skala jaringan, cakupan yang diinginkan, dan kasus penggunaan tertentu (Duan et al., 2019).

3.5 Komponen Jaringan Nirkabel

Komponen jaringan nirkabel mencakup elemen perangkat keras penting yang diperlukan untuk membangun dan memelihara komunikasi nirkabel (Vlačić et al., 2021). Komponen-komponen ini sangat penting bagi berfungsinya jaringan nirkabel dan memainkan peran berbeda dalam memfasilitasi konektivitas nirkabel (Potlapally et al., 2003).

Access Point (AP) berfungsi sebagai komponen penting dalam jaringan nirkabel. Bertindak sebagai perangkat perantara yang menjembatani perangkat nirkabel ke infrastruktur jaringan kabel. AP mengirim dan menerima data antara klien nirkabel dan jaringan pusat, sehingga secara efektif memperluas jangkauan

jaringan (Fluckiger, 1995). Dilengkapi dengan transceiver radio yang memungkinkan komunikasi nirkabel, dan penempatan serta konfigurasinya sangat penting dalam menentukan jangkauan dan kinerja jaringan (Mughal, 2022).

Router Nirkabel menggabungkan fungsionalitas router dan titik akses. Di jaringan rumah dan kantor kecil, router nirkabel sering kali menjadi titik pusat untuk menghubungkan beberapa perangkat ke internet (Dai et al., 2019). Perangkat ini menangani tugas-tugas seperti terjemahan alamat jaringan (NAT) dan DHCP, memungkinkan beberapa perangkat untuk berbagi satu koneksi internet (Jacob & Darney, 2021). Selain itu, menawarkan titik akses nirkabel untuk menghubungkan perangkat nirkabel ke jaringan (Román-Castro et al., 2018).

Kartu Antarmuka Jaringan Nirkabel (NIC) adalah komponen penting dalam perangkat berkemampuan nirkabel seperti laptop, ponsel cerdas, dan tablet. NIC ini menyediakan kemampuan perangkat ini untuk terhubung ke jaringan nirkabel. Berisi transceiver radio dan driver yang diperlukan untuk mengirim dan menerima data secara nirkabel. NIC tersedia dalam berbagai faktor bentuk, termasuk kartu PCIe mini, adaptor USB, dan komponen internal (Seberry & Pieprzyk, 1989).

Antena dan Penguat Sinyal sangat penting untuk meningkatkan kekuatan dan jangkauan sinyal nirkabel. Antena adalah komponen pasif yang membentuk pola radiasi sinyal nirkabel, mengarahkannya ke area atau perangkat tertentu. Penguat sinyal, di sisi lain, secara aktif memperkuat dan memperluas jangkauan sinyal nirkabel. Komponen ini sering digunakan di lingkungan yang jangkauan sinyalnya perlu dioptimalkan, seperti gedung besar, area luar ruangan, atau lokasi terpencil (Ukil et al., 2011).

Pengkabelan Jaringan memainkan peran penting dalam jaringan nirkabel, khususnya dalam infrastruktur backhaul. Meskipun komunikasi nirkabel bersifat nirkabel pada titik akhir,

data sering kali berpindah melalui koneksi kabel di latar belakang. Kabel Ethernet, kabel serat optik, dan jenis kabel jaringan lainnya menghubungkan titik akses, router, dan komponen jaringan lainnya ke infrastruktur pusat. Memastikan pemasangan kabel berkualitas tinggi sangat penting untuk meminimalkan kesalahan transmisi data dan menjaga keandalan jaringan (Bishop, 2004).

Peralatan *Power over Ethernet* (PoE) menyederhanakan penerapan titik akses nirkabel, khususnya di area dengan sumber daya terbatas. Peralatan PoE memungkinkan data dan daya ditransmisikan melalui satu kabel Ethernet. Hal ini menghilangkan kebutuhan akan sumber listrik terpisah di dekat setiap titik akses, menyederhanakan instalasi dan mengurangi biaya infrastruktur (Tang et al., 2019).

Komponen jaringan nirkabel mencakup beragam elemen perangkat keras yang memungkinkan konektivitas nirkabel. Titik akses, router, NIC, antena, penguat sinyal, kabel jaringan, dan peralatan PoE secara kolektif membentuk fondasi jaringan nirkabel, mendukung transmisi data yang lancar antara perangkat nirkabel dan infrastruktur jaringan kabel. Memahami peran dan kemampuan komponen-komponen ini sangat penting untuk merancang dan memelihara jaringan nirkabel yang efisien dan andal (Gerodimos et al., 2023).

3.6 Keamanan Nirkabel

Keamanan nirkabel merupakan aspek penting dalam menjaga kerahasiaan, integritas, dan ketersediaan data dalam jaringan nirkabel. Ini mencakup serangkaian tindakan dan protokol yang dirancang untuk melindungi terhadap akses tidak sah, pelanggaran data, dan ancaman keamanan lainnya dalam komunikasi nirkabel (Novianto et al., 2023).

Salah satu aspek terpenting dari keamanan nirkabel adalah enkripsi. Teknik enkripsi digunakan untuk mengacak data yang dikirimkan melalui jaringan nirkabel, sehingga tidak dapat dibaca

oleh siapa pun tanpa kunci dekripsi yang tepat. Standar enkripsi populer untuk jaringan nirkabel mencakup WEP (*Wired Equivalent Privacy*), WPA (*Wi-Fi Protected Access*), WPA2, dan WPA3. Standar ini menggunakan algoritma seperti AES (*Advanced Encryption Standard*) untuk melindungi data selama transmisi.

Mekanisme otentikasi adalah elemen penting lainnya dari keamanan nirkabel (Choubey et al., 2022). Otentikasi memastikan bahwa hanya pengguna yang berwenang yang dapat mengakses jaringan nirkabel. WPA dan WPA2, misalnya, menggabungkan metode seperti *Pre-Shared Keys* (PSKs) atau *Extensible Authentication Protocol* (EAP) untuk memverifikasi identitas pengguna atau perangkat yang mencoba terhubung. Otentikasi yang kuat mencegah pengguna yang tidak sah mendapatkan akses (Wang et al., 2022).

Sistem deteksi dan pencegahan intrusi (IDS/IPS) digunakan untuk memantau dan melindungi jaringan nirkabel dari aktivitas mencurigakan atau berbahaya. Sistem ini terus menganalisis lalu lintas jaringan, mencari pola yang tidak biasa atau tanda serangan yang diketahui. Ketika terdeteksi, dapat memicu alarm, memblokir akses, atau mengambil tindakan perlindungan lainnya untuk mengurangi ancaman dan intrusi (Atlam et al., 2020).

Segmentasi jaringan adalah praktik keamanan yang melibatkan pembagian jaringan nirkabel menjadi segmen yang lebih kecil dan terisolasi atau VLAN (Virtual LAN). Hal ini mencegah pengguna atau perangkat yang tidak sah berpindah ke samping di seluruh jaringan setelah mendapatkan akses ke satu segmen. Dengan membatasi akses ke area sensitif jaringan, segmentasi jaringan dapat membantu mengatasi pelanggaran keamanan dan mengurangi permukaan serangan (Ebi et al., 2019).

Keamanan nirkabel juga melibatkan pengamanan infrastruktur fisik. Titik akses fisik, seperti titik akses dan router, harus dilindungi secara fisik untuk mencegah gangguan atau akses yang tidak sah. Selain itu, pembuangan peralatan nirkabel lama

atau yang sudah tidak digunakan dengan benar sangat penting untuk memastikan bahwa informasi sensitif tidak dapat diakses oleh orang yang tidak berwenang (Tawalbeh et al., 2020).

Pembaruan dan patch perangkat lunak secara berkala sangat penting untuk menjaga keamanan nirkabel. Produsen merilis pembaruan untuk mengatasi kerentanan dan kelemahan keamanan pada perangkat dan perangkat lunak. Dengan menerapkan pembaruan ini secara rutin, administrator jaringan dapat memperkuat keamanan jaringan nirkabel dan melindungi dari ancaman yang diketahui (Wei et al., 2021).

Praktik terbaik keamanan, termasuk penggunaan kata sandi yang kuat dan unik, penerapan pemantauan dan pencatatan jaringan, serta mendidik pengguna tentang kesadaran keamanan, merupakan hal mendasar dalam keamanan nirkabel. Pengguna harus menyadari risiko yang terkait dengan koneksi ke jaringan Wi-Fi publik dan harus berhati-hati saat berbagi informasi sensitif melalui jaringan tersebut (Cotrim & Kleinschmidt, 2020).

Keamanan nirkabel adalah disiplin multifaset yang bertujuan melindungi jaringan nirkabel dari akses tidak sah, pelanggaran data, dan ancaman keamanan. Ini mencakup enkripsi, otentikasi, deteksi dan pencegahan intrusi, segmentasi jaringan, keamanan fisik, pembaruan perangkat lunak, dan praktik terbaik untuk memastikan keamanan dan privasi data yang dikirimkan melalui jaringan nirkabel. Menerapkan strategi keamanan nirkabel yang kuat sangat penting dalam dunia yang saling terhubung saat ini dimana komunikasi nirkabel ada dimana-mana (Kizza, 2005).

3.7 Protokol Jaringan Nirkabel

Protokol jaringan nirkabel adalah seperangkat aturan dan konvensi yang menentukan bagaimana data dikirim, diterima, dan dikelola dalam komunikasi nirkabel (Jacob & Darney, 2021). Protokol ini menentukan standar dan prosedur yang

memungkinkan perangkat berkomunikasi secara efektif dalam jaringan nirkabel (Dai et al., 2019).

TCP/IP (Transmission Control Protocol/Internet Protocol) adalah rangkaian protokol dasar yang mendasari internet dan sebagian besar jaringan nirkabel. Ini menyediakan kerangka standar untuk transmisi data, pengalamatan, routing, dan penanganan kesalahan. TCP memastikan pengiriman paket data yang andal dan teratur, sementara IP menangani pengalamatan dan perutean data di seluruh jaringan (Cilfone et al., 2019).

IEEE 802.11 adalah keluarga standar jaringan nirkabel yang mengatur komunikasi LAN nirkabel (WLAN). Ini mencakup standar terkenal seperti 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, dan 802.11ax (Wi-Fi 6). Standar ini menentukan spesifikasi lapisan lapisan fisik (PHY) dan kontrol akses media (MAC) untuk komunikasi nirkabel. Menentukan pita frekuensi, kecepatan data, dan skema modulasi yang digunakan dalam WLAN (Cotrim & Kleinschmidt, 2020).

Protokol Aplikasi Nirkabel memungkinkan perangkat nirkabel untuk berinteraksi dengan layanan dan aplikasi jaringan. Protokol-protokol ini termasuk HTTP (*Hypertext Transfer Protocol*), yang digunakan untuk penelusuran web; FTP (*File Transfer Protocol*), untuk transfer file; dan SMTP/POP3/IMAP, yang menangani komunikasi email melalui jaringan nirkabel. Protokol ini memungkinkan perangkat nirkabel mengakses konten web, mengirim dan menerima email, dan terlibat dengan berbagai layanan online (Ak & Canberk, 2021).

Mobile IP (*Internet Protocol*) adalah protokol yang dirancang untuk memfasilitasi mobilitas perangkat dalam jaringan nirkabel tanpa batas. Hal ini memungkinkan perangkat untuk mempertahankan alamat IP dan konektivitasnya saat berpindah antar jaringan yang berbeda. IP Seluler sangat penting untuk perangkat seluler seperti ponsel cerdas dan tablet, memastikan

perangkat tersebut tetap terhubung saat pengguna bertransisi antara Wi-Fi dan jaringan seluler (Davronbekov, 2020).

Mekanisme Serah Terima sangat penting untuk memastikan konektivitas tidak terputus saat perangkat berpindah dalam jaringan nirkabel. Mekanisme ini, seperti Fast BSS Transition (FT), memungkinkan perangkat untuk beralih antar titik akses tanpa kehilangan koneksi jaringan. Protokol serah terima membantu menjaga pengalaman pengguna yang lancar dan lancar dalam jaringan nirkabel (Almaiah et al., 2022).

Bluetooth adalah protokol komunikasi nirkabel yang digunakan untuk koneksi jarak pendek antar perangkat. Ini biasanya digunakan untuk menghubungkan periferal seperti keyboard, mouse, headphone, dan perangkat IoT ke ponsel cerdas, tablet, dan komputer. Bluetooth beroperasi pada pita ISM 2,4 GHz dan menggunakan berbagai profil untuk berbagai jenis interaksi perangkat (Kang et al., 2021).

Near Field Communication (NFC) adalah protokol komunikasi nirkabel untuk pertukaran data jarak pendek. NFC memungkinkan perangkat berkomunikasi dengan mendekatkannya, biasanya dalam jarak beberapa sentimeter. Biasanya digunakan untuk pembayaran nirsentuh, kontrol akses, dan transfer data antara ponsel cerdas dan perangkat berkemampuan NFC lainnya (Almaiah et al., 2022).

Protokol jaringan nirkabel adalah dasar dari komunikasi nirkabel modern, yang menentukan bagaimana perangkat berkomunikasi dan berbagi data melalui jaringan nirkabel. Protokol-protokol ini mencakup berbagai standar dan spesifikasi, memastikan kompatibilitas dan interoperabilitas di antara beragam perangkat dan teknologi nirkabel. Memahami dan menerapkan protokol-protokol ini sangat penting untuk membangun dan memelihara jaringan nirkabel yang efisien dan andal di dunia yang saling terhubung saat ini (Cilfone et al., 2019).

3.8 *Quality of Service* (QoS)

Quality of Service (QoS) dalam jaringan nirkabel adalah seperangkat protokol dan mekanisme yang mengatur bagaimana lalu lintas data dikelola dan diprioritaskan untuk memastikan pengalaman pengguna yang andal dan konsisten. QoS sangat penting dalam lingkungan nirkabel, dimana kondisi jaringan dapat bervariasi dan dapat mengalami interferensi dan kemacetan (Olenik et al., 2021).

Salah satu aspek mendasar dari QoS adalah klasifikasi lalu lintas. Berbagai jenis lalu lintas data memiliki persyaratan berbeda dalam hal latensi, bandwidth, dan keandalan. Mekanisme QoS mengklasifikasikan data ke dalam kategori berdasarkan persyaratan ini. Misalnya, data suara dan video diklasifikasikan sebagai lalu lintas berprioritas tinggi, sedangkan unduhan file atau email mungkin dianggap berprioritas lebih rendah. Klasifikasi ini memungkinkan jaringan untuk memperlakukan berbagai jenis lalu lintas yang berbeda (Jacob & Darney, 2021).

Manajemen bandwidth adalah komponen penting dari QoS. Jaringan nirkabel seringkali memiliki bandwidth terbatas, sehingga harus dialokasikan secara efisien untuk memenuhi kebutuhan berbagai aplikasi. Mekanisme QoS memprioritaskan lalu lintas berprioritas tinggi dan mengalokasikan sebagian dari bandwidth yang tersedia untuk memastikan bahwa aplikasi penting, seperti konferensi video real-time atau panggilan suara, menerima sumber daya yang diperlukan untuk kelancaran pengoperasian (Cilfone et al., 2019).

Prioritas paket adalah elemen kunci lain dari QoS. Dalam jaringan nirkabel, data dikirimkan dalam bentuk paket. Mekanisme QoS menetapkan tag prioritas ke paket-paket ini berdasarkan klasifikasi lalu lintasnya. Paket berprioritas tinggi dikirimkan sebelum paket berprioritas lebih rendah, sehingga mengurangi latensi untuk aplikasi yang sensitif terhadap waktu. Hal ini memastikan bahwa, misalnya, panggilan suara tidak akan

mengalami penundaan yang signifikan bahkan dalam jaringan yang padat (Dai et al., 2019).

Mekanisme QoS juga mencakup pembentukan dan pengawasan lalu lintas. Pembentukan lalu lintas mengatur aliran data untuk memastikan bahwa aliran tersebut mematuhi kebijakan QoS yang ditentukan. Hal ini mencegah kemacetan jaringan dan memastikan lalu lintas berprioritas tinggi tidak kewalahan oleh lalu lintas berprioritas lebih rendah. Polisi lalu lintas, di sisi lain, memantau lalu lintas untuk mengidentifikasi dan memitigasi pelanggaran kebijakan QoS (Elsayed & Erol-Kantarci, 2019).

Dalam LAN nirkabel, standar IEEE 802.11e memainkan peran penting dalam implementasi QoS. Ini memperkenalkan fitur seperti *Enhanced Distributed Channel Access* (EDCA), yang menyediakan prioritas kategori lalu lintas yang berbeda. Melalui EDCA, titik akses nirkabel dapat membedakan lalu lintas suara, video, dan data, sehingga memungkinkan mengelola dan memprioritaskan paket yang sesuai (Long et al., 2021).

QoS sangat penting untuk aplikasi *real-time* seperti Voice over IP (VoIP) dan streaming video. Dalam VoIP, misalnya, menjaga latensi rendah dan memastikan bahwa paket suara tiba tepat waktu dan dapat diprediksi sangat penting untuk percakapan yang jelas dan tidak terputus. Mekanisme QoS dalam jaringan nirkabel membantu mencapai tujuan ini dengan memprioritaskan lalu lintas suara (Wei et al., 2021).

Quality of Service (QoS) dalam jaringan nirkabel adalah seperangkat protokol dan mekanisme yang dirancang untuk mengelola dan memprioritaskan lalu lintas data untuk memenuhi beragam kebutuhan aplikasi yang berbeda. Hal ini memastikan bahwa data penting, seperti suara dan video, menerima sumber daya yang diperlukan untuk transmisi yang andal dan berlatensi rendah, bahkan di lingkungan nirkabel yang menantang dengan bandwidth terbatas dan potensi interferensi. QoS memainkan peran penting dalam memberikan pengalaman pengguna yang

konsisten dan berkualitas tinggi dalam komunikasi nirkabel (Cilfone et al., 2019).

3.9 Manajemen Jaringan Nirkabel

Manajemen jaringan nirkabel adalah proses perencanaan, konfigurasi, pemantauan, dan pemeliharaan jaringan nirkabel untuk memastikan kinerja, keamanan, dan keandalan optimal. Manajemen jaringan yang efektif sangat penting dalam lingkungan nirkabel saat ini, dimana konektivitas sangat penting baik untuk operasional pribadi maupun bisnis (Akhmad Al Aidhi, 2023).

Pemantauan Jaringan adalah aspek mendasar dari manajemen jaringan nirkabel. Ini melibatkan pengawasan berkelanjutan terhadap kinerja jaringan, pola lalu lintas, dan status perangkat. Alat dan perangkat lunak pemantauan membantu administrator mengidentifikasi masalah seperti kemacetan, gangguan, atau akses tidak sah. Alat-alat ini memberikan wawasan real-time mengenai kesehatan jaringan, memungkinkan respons tepat waktu terhadap masalah (Dai et al., 2019).

Konfigurasi dan Pengaturan mencakup penerapan awal komponen jaringan nirkabel, termasuk titik akses, router, dan pengaturan keamanan. Konfigurasi yang tepat memastikan perangkat berkomunikasi secara efisien dan aman. Administrator jaringan menetapkan SSID (Service Set Identifiers), protokol keamanan (misalnya WPA2 atau WPA3), dan kunci enkripsi untuk melindungi transmisi data (Ak & Canberk, 2021).

Pembaruan Firmware sangat penting untuk menjaga perangkat jaringan tetap mutakhir dan aman (Kizza et al., 2013). Produsen secara rutin merilis pembaruan firmware untuk mengatasi kerentanan, meningkatkan kinerja, dan menambahkan fitur baru. Administrator jaringan harus secara teratur memeriksa pembaruan dan menerapkannya untuk menjaga integritas dan keamanan jaringan (Anizira et al., 2023).

Pengoptimalan Kinerja melibatkan penyempurnaan pengaturan jaringan untuk memastikan throughput data yang optimal dan meminimalkan latensi. Hal ini dapat mencakup penyesuaian penetapan saluran, mengoptimalkan penempatan antena, dan mengonfigurasi pengaturan Kualitas Layanan (QoS) untuk memprioritaskan lalu lintas untuk aplikasi atau pengguna tertentu (Jacob & Darney, 2021).

Load Balancing sangat penting dalam jaringan nirkabel yang lebih besar dengan banyak titik akses. Ini mendistribusikan lalu lintas jaringan secara merata di seluruh titik akses untuk mencegah kelebihan beban pada satu perangkat. Penyeimbangan beban meningkatkan efisiensi jaringan dan memastikan pengalaman pengguna yang konsisten, bahkan selama periode penggunaan puncak (Alsharif et al., 2020).

Manajemen Keamanan adalah aspek penting dari manajemen jaringan nirkabel. Ini mencakup penerapan protokol keamanan, kontrol akses, dan sistem deteksi intrusi (Davronbekov, 2020). Administrator jaringan harus meninjau dan memperbarui pengaturan keamanan secara berkala untuk melindungi dari ancaman yang terus berkembang (Kizza et al., 2013).

Pemecahan Masalah Jaringan melibatkan diagnosis dan penyelesaian masalah yang mungkin timbul dalam jaringan nirkabel. Alat dan teknik pemecahan masalah membantu administrator mengidentifikasi akar penyebab masalah, seperti masalah konektivitas, gangguan sinyal, atau kesalahan konfigurasi perangkat. Pemecahan masalah yang efektif memastikan waktu henti dan gangguan yang minimal (Davronbekov, 2020).

Perencanaan Kapasitas mengantisipasi permintaan jaringan di masa depan dan persyaratan skalabilitas (Rukmana & Sudarmanto, 2023). Administrator menganalisis pola penggunaan saat ini dan membuat ketentuan untuk mengakomodasi peningkatan lalu lintas data atau perangkat tambahan (Bakri et al.,

2023). Pendekatan proaktif ini membantu menghindari kemacetan jaringan dan penurunan kinerja (Harto et al., 2023).

Dokumentasi dan Manajemen Dokumentasi sangat penting untuk menjaga infrastruktur jaringan yang terorganisir dan terdokumentasi dengan baik (Almahdali et al., 2023). Administrator jaringan menyimpan catatan konfigurasi, inventaris perangkat, dan prosedur pemecahan masalah. Dokumentasi menyederhanakan tugas manajemen di masa depan dan membantu pemulihan bencana (Rizal et al., 2023).

Pelatihan dan Dukungan Pengguna merupakan komponen penting dari manajemen jaringan nirkabel. Administrator harus memberikan pelatihan dan dukungan kepada pengguna akhir, membantu memahami praktik terbaik, langkah-langkah keamanan, dan cara melaporkan masalah jaringan. Pengguna yang berpengetahuan luas berkontribusi pada lingkungan jaringan yang lebih aman dan efisien (Khuan et al., 2023).

Manajemen jaringan nirkabel adalah proses komprehensif yang mencakup perencanaan, konfigurasi, pemantauan, pemeliharaan, dan langkah-langkah keamanan untuk memastikan pengoperasian jaringan nirkabel yang efisien dan aman (Kizza et al., 2013). Hal ini memerlukan pendekatan proaktif dan terdokumentasi dengan baik untuk mengatasi masalah, mengoptimalkan kinerja, dan memenuhi tuntutan komunikasi nirkabel modern yang terus berkembang (Kang et al., 2021).

3.10 Tren yang Muncul dalam Jaringan Nirkabel

Gambar 3.1. Teknologi Nirkabel
(Sumber : www.edsurge.com)

Tren yang muncul dalam jaringan nirkabel mengubah cara kita terhubung dan berkomunikasi di dunia yang semakin digital (Rukmana, 2023b). Tren-tren ini mewakili kemajuan mutakhir dalam teknologi nirkabel, didorong oleh permintaan yang terus meningkat akan jaringan nirkabel yang lebih cepat, lebih andal, dan serbaguna (Kizza et al., 2013).

Salah satu tren yang paling menonjol adalah evolusi teknologi 5G. Ketika jaringan 5G terus diluncurkan di seluruh dunia, jaringan tersebut menjanjikan peningkatan kecepatan data, pengurangan latensi, dan peningkatan konektivitas (Parmaxi, 2023). Hal ini memungkinkan berbagai aplikasi, termasuk *augmented reality* (AR), *virtual reality* (VR), kendaraan otonom, dan kota pintar. Kemampuan 5G diharapkan dapat mendukung pengembangan layanan dan industri yang inovatif (Rukmana & Sudarmanto, 2023).

Internet of Things (IoT) mengalami pertumbuhan pesat, menyebabkan lonjakan jumlah perangkat yang terhubung. Untuk mengakomodasi ekspansi ini, tren yang muncul berfokus pada *Low*

Power Wide Area Networks (LPWANs) seperti LoRaWAN dan NB-IoT. Teknologi-teknologi ini menawarkan konektivitas jangka panjang dan berdaya rendah, menjadikannya ideal untuk berbagai aplikasi IoT, mulai dari pertanian cerdas hingga pelacakan aset (Kang et al., 2021).

Komputasi tepi mendapatkan daya tarik sebagai tren penting dalam jaringan nirkabel (Almaiah et al., 2022). Dengan memproses data lebih dekat ke tempat data dihasilkan (di tepi jaringan), komputasi tepi mengurangi latensi dan meningkatkan kinerja waktu nyata (Aydos et al., 1999). Hal ini sangat penting untuk aplikasi seperti kendaraan otonom, otomasi industri, dan game yang imersif (Bakri et al., 2023).

Virtualisasi jaringan nirkabel adalah tren penting lainnya. Hal ini memungkinkan beberapa jaringan virtual untuk berbagi infrastruktur fisik yang sama, sehingga meningkatkan alokasi sumber daya dan efisiensi jaringan (Setiawan et al., 2023). Konsep pemotongan jaringan, yang merupakan bagian integral dari 5G, memungkinkan penyedia untuk membuat jaringan virtual terisolasi yang disesuaikan dengan kasus penggunaan tertentu, seperti layanan kesehatan, pabrik pintar, atau keselamatan publik (Baali et al., 2023).

Konvergensi adalah tren yang berupaya menyatukan berbagai teknologi dan frekuensi nirkabel (Halsall, 1995). Konvergensi ini memungkinkan perangkat untuk beralih secara mulus antara jaringan nirkabel dan titik akses yang berbeda, sehingga menyederhanakan konektivitas (Wahdiniawati et al., 2023). Ini sangat berharga di lingkungan dengan beragam teknologi nirkabel yang beroperasi, seperti rumah dengan perangkat Wi-Fi, Zigbee, dan Bluetooth (Naim et al., 2023).

Keamanan dan privasi semakin penting dalam jaringan nirkabel. Dengan meningkatnya kekhawatiran mengenai pelanggaran data dan pelanggaran privasi, tren yang muncul menekankan penerapan langkah-langkah keamanan yang kuat

(Taylor et al., 2011). Teknologi seperti keamanan tanpa kepercayaan dan *Secure Access Service Edge* (SASE) bertujuan untuk memastikan perlindungan data dan mengamankan akses jaringan, bahkan dalam skenario jarak jauh atau berbasis cloud (Jeyaraj et al., 2023).

Integrasi kecerdasan buatan (AI) adalah tren lain yang sedang berkembang. Pembelajaran mesin dan algoritma AI diterapkan untuk mengoptimalkan kinerja jaringan, memprediksi dan mencegah kegagalan jaringan, dan beradaptasi dengan perubahan kondisi secara real-time. Manajemen jaringan berbasis AI meningkatkan efisiensi dan keandalan (Permana et al., 2023).

Tren yang muncul dalam jaringan nirkabel mendorong evolusi teknologi nirkabel. Mulai dari potensi transformatif 5G dan proliferasi perangkat IoT hingga munculnya edge computing, virtualisasi, konvergensi, peningkatan keamanan, dan integrasi AI, tren-tren ini membentuk masa depan komunikasi nirkabel, menjanjikan lanskap digital yang lebih terhubung, efisien, dan aman (Rukmana & Sudarmanto, 2023).

DAFTAR PUSTAKA

Ak, E., & Canberk, B. 2021. Forecasting quality of service for next-generation data-driven WiFi6 campus networks. *IEEE Transactions on Network and Service Management*, *18*(4), 4744–4755.

Akhmad Al Aidhi, M. A. K. H. A. Y. R. 2023. Peningkatan Daya Saing Ekonomi melalui peranan Inovasi. *Jurnal Multidisiplin West Science*. https://wnj.westscience-press.com/index.php/jmws/article/view/229/160

Alani, T. O., & Al-Sadi, A. M. 2023. Survey of optimizing dynamic virtual local area network algorithm for software-defined wide area network. *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, *21*(1), 77–87.

Almahdali, H., Pane, E. P., Rukmana, A. Y., Nasution, A. K. P., Jannah, L. U., & Razilu, Z. 2023. *NEW TECHNOLOGIES IN TEACHING AND LEARNING*. Get Press Indonesia.

Almaiah, M. A., Al-Rahmi, A., Alturise, F., Hassan, L., Lutfi, A., Alrawad, M., Alkhalaf, S., Al-Rahmi, W. M., Al-sharaieh, S., & Aldhyani, T. H. H. 2022. Investigating the Effect of Perceived Security, Perceived Trust, and Information Quality on Mobile Payment Usage through Near-Field Communication (NFC) in Saudi Arabia. *Electronics*, *11*(23), 3926.

Alsharif, M. H., Kelechi, A. H., Albreem, M. A., Chaudhry, S. A., Zia, M. S., & Kim, S. 2020. Sixth generation (6G) wireless networks: Vision, research activities, challenges and potential solutions. *Symmetry*, *12*(4), 676.

Anizira, A., Nasution, R. A., Zarkasi, Z., & Rukmana, A. Y. 2023. Industrial Revolution Ideas 4.0 for Professional Development. *Jurnal Manajemen Riset Inovasi*, *1*(4), 26–36.

Atlam, H. F., Alenezi, A., Alassafi, M. O., Alshdadi, A. A., & Wills, G. B. 2020. Security, cybercrime and digital forensics for IoT. *Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm*, 551–577.

Aydos, M., Savas, E., & Koc, C. K. 1999. Implementing network security protocols based on elliptic curve cryptography. *Proceedings of the Fourth Symposium on Computer Networks*, 130–139.

Baali, Y., Sasewa, D. R., Sjioen, A. E., Rejeki, S., Wahyuarini, T., Saputra, Y. M. D., Harlina, S., Wijaya, I. M. S., Rukmana, A. Y., & Hariyanti, N. K. D. 2023. *SISTEM INFORMASI MANAJEMEN: KONSEP DAN APLIKASI BISNIS*. Get Press Indonesia.

Bakri, A. A., Sudarmanto, E., Fitriansyah, N. D. P. S., Rukmana, A. Y., & Utami, E. Y. 2023. Blockchain Technology and its Disruptive Potential in the Digital Economy. *West Science Journal Economic and Entrepreneurship*, *1*(03), 116–123.

Bishop, M. 2004. *Introduction to computer security*. Addison-Wesley Professional.

Choubey, D. K., Shukla, V., Soni, V., Kumar, J., & Dheer, D. K. 2022. A review on IoT architectures, protocols, security, and applications. *Industrial Internet of Things*, 225–242.

Cilfone, A., Davoli, L., Belli, L., & Ferrari, G. 2019. Wireless mesh networking: An IoT-oriented perspective survey on relevant technologies. *Future Internet*, *11*(4), 99.

Cotrim, J. R., & Kleinschmidt, J. H. 2020. LoRaWAN mesh networks: A review and classification of multihop communication. *Sensors*, *20*(15), 4273.

Dai, J. Y., Tang, W. K., Zhao, J., Li, X., Cheng, Q., Ke, J. C., Chen, M. Z., Jin, S., & Cui, T. J. 2019. Wireless communications through a simplified architecture based on time-domain digital coding metasurface. *Advanced Materials Technologies*, *4*(7), 1900044.

Davronbekov, D. A. 2020. The role of wireless networking technology today. *ИННОВАЦИОННЫЕ НАУЧНЫЕ ИССЛЕДОВАНИЯ: ТЕОРИЯ, МЕТОДОЛОГИЯ, ПРАКТИКА*, 77–79.

Dooley, D. M., Griffiths, E. J., Gosal, G. S., Buttigieg, P. L., Hoehndorf, R., Lange, M. C., Schriml, L. M., Brinkman, F. S. L., & Hsiao, W. W. L. 2018. FoodOn: a harmonized food ontology to increase global food traceability, quality control and data integration. *Npj Science of Food*, *2*(1), 23.

Duan, Y., Edwards, J. S., & Dwivedi, Y. K. 2019. Artificial intelligence for decision making in the era of Big Data–evolution, challenges and research agenda. *International Journal of Information Management*, *48*, 63–71.

Ebi, C., Schaltegger, F., Rüst, A., & Blumensaat, F. 2019. Synchronous LoRa mesh network to monitor processes in underground infrastructure. *IEEE Access*, *7*, 57663–57677.

Eid, M. M. A., Sorathiya, V., Lavadiya, S., Habib, M. A., Helmy, A., & Rashed, A. N. Z. 2021. Dispersion compensation FBG with optical quadrature phase shift keying (OQPSK) modulation scheme for high system capacity. *Journal of Optical Communications*, *0*, 000010151520210022.

Elsayed, M., & Erol-Kantarci, M. 2019. AI-enabled future wireless networks: Challenges, opportunities, and open issues. *IEEE Vehicular Technology Magazine*, *14*(3), 70–77.

Fernando, Y., Tseng, M.-L., Wahyuni-Td, I. S., de Sousa Jabbour, A. B. L., Chiappetta Jabbour, C. J., & Foropon, C. 2023. Cyber supply chain risk management and performance in industry 4.0 era: information system security practices in Malaysia. *Journal of Industrial and Production Engineering*, *40*(2), 102–116.

Fluckiger, F. 1995. *Understanding networked multimedia: applications and technology*. Prentice Hall International (UK) Ltd.

Forouzan, B. A., & Mukhopadhyay, D. 2015. *Cryptography and network security* (Vol. 12). Mc Graw Hill Education (India) Private Limited New York, NY, USA:

Gerodimos, A., Maglaras, L., Ferrag, M. A., Ayres, N., & Kantzavelou, I. 2023. IoT: Communication protocols and security threats. *Internet of Things and Cyber-Physical Systems*.

Halsall, F. 1995. *Data communications, computer networks and open systems*. Addison Wesley Longman Publishing Co., Inc.

Hammond, J. L., & O'Reilly, P. P. 1986. *Performance analysis of local computer networks*. Addison-Wesley Longman Publishing Co., Inc.

Harto, B., Rukmana, A. Y., Subekti, R., Tahir, R., Waty, E., Situru, A. C., & Sepriano, S. 2023. *TRANSFORMASI BISNIS DI ERA DIGITAL: Teknologi Informasi dalam Mendukung Transformasi Bisnis di Era Digital*. PT. Sonpedia Publishing Indonesia.

Jacob, D. I. J., & Darney, D. P. E. 2021. Artificial bee colony optimization algorithm for enhancing routing in wireless networks. *Journal of Artificial Intelligence and Capsule Networks*, *3*(1), 62–71.

Jeyaraj, R., Balasubramaniam, A., MA, A. K., Guizani, N., & Paul, A. 2023. Resource Management in Cloud and Cloud-influenced Technologies for Internet of Things Applications. *ACM Computing Surveys*, *55*(12), 1–37.

Kaeo, M. (2004). *Designing network security*. Cisco Press.

Kang, Y., Lee, S., Gwak, S., Kim, T., & An, D. 2021. Time-sensitive networking technologies for industrial automation in wireless communication systems. *Energies*, *14*(15), 4497.

Khuan, H., Andriani, E., & Rukmana, A. Y. 2023. The Role of Technology in Fostering Innovation and Growth in Start-up Businesses. *West Science Journal Economic and Entrepreneurship*, *1*(03), 124–133.

Kiesler, S. 1986. *The hidden messages in computer networks*. Harvard Business Review Case Services.

Kizza, J. M. 2005. *Computer network security*. Springer.

Kizza, J. M., Kizza, W., & Wheeler. 2013. *Guide to computer network security* (Vol. 8). Springer.

Lalit, M., Chawla, S. K., Rana, A. K., Nisar, K., Soomro, T. R., & Khan, M. A. 2022. IoT networks: Security vulnerabilities of application layer protocols. *2022 14th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS)*, 1–5.

Long, W., Chen, R., Moretti, M., Zhang, W., & Li, J. 2021. A promising technology for 6G wireless networks: Intelligent reflecting surface. *Journal of Communications and Information Networks*, *6*(1), 1–16.

Marin, G. A. 2005. Network security basics. *IEEE Security & Privacy*, *3*(6), 68–72.

Mughal, A. A. 2022. Well-Architected Wireless Network Security. *Journal of Humanities and Applied Science Research*, *5*(1), 32–42.

Naim, S., A'ffar, M., Sulistyowati, N. W., Destiana, R., Supriatna, E., Rukmana, A. Y., & Chusumastuti, D. 2023. TRANSFORMASI TOKO TRADISIONAL MENJADI TOKO BERBASIS DIGITAL: PELATIHAN DAN PENDAMPINGAN UNTUK MENGHADAPI ERA DIGITALISASI. *Eastasouth Journal of Impactive Community Services*, *1*(03), 215–222.

Novianto, E., Ujianto, E. H. H., & Rianto, R. 2023. KEAMANAN INFORMASI (INFORMATION SECURITY) PADA APLIKASI SISTEM INFORMASI MANAJEMEN SUMBER DAYA MANUSIA. *Rabit: Jurnal Teknologi Dan Sistem Informasi Univrab*, *8*(1), 10–15.

Olenik, S., Lee, H. S., & Güder, F. 2021. The future of near-field communication-based wireless sensing. *Nature Reviews Materials*, *6*(4), 286–288.

Pamarthi, S., & Narmadha, R. 2022. Literature review on network security in Wireless Mobile Ad-hoc Network for IoT applications: Network attacks and detection mechanisms. *International Journal of Intelligent Unmanned Systems*, *10*(4), 482–506.

Parmaxi, A. 2023. Virtual reality in language learning: A systematic review and implications for research and practice. *Interactive Learning Environments*, *31*(1), 172–184.

Permana, A. A., Darmawan, R., Saputri, F. R., Harto, B., Al-Hakim, R. R., Wijayanti, R. R., Safii, M., Pasaribu, J. S., & Rukmana, A. Y. 2023. *ARTIFICIAL INTELLIGENCE MARKETING*. Get Press Indonesia.

Peterson, L. L., & Davie, B. S. 2007. *Computer networks: a systems approach*. Elsevier.

Potlapally, N. R., Ravi, S., Raghunathan, A., & Jha, N. K. 2003. Analyzing the energy consumption of security protocols. *Proceedings of the 2003 International Symposium on Low Power Electronics and Design*, 30–35.

Quarterman, J. S., & Hoskins, J. C. 1986. Notable computer networks. *Communications of the ACM*, *29*(10), 932–971.

Rizal, M., Rukmana, A. Y., Permana, A. A., Fianty, M. I., Saputra, H., Saputri, F. R., Pomalingo, S., Sutomo, R., Darmawan, R., & Akbar, N. 2023. *TRANSFORMASI DIGITAL: MEMAHAMI INTERNET OF THINGS*. Get Press Indonesia.

Román-Castro, R., López, J., & Gritzalis, S. 2018. Evolution and trends in IoT security. *Computer*, *51*(7), 16–25.

Rukmana, A. Y. 2023a. BAB 3 TEKNOLOGI DIGITAL. *Digital Marketing Dan E-Commerce*, 27.

Rukmana, A. Y. 2023b. Revolusi Bisnis di Era Digital: Strategi dan Dampak Transformasi Proses Teknologi terhadap Keunggulan Kompetitif dan Pertumbuhan Organisasi. *Jurnal Bisnis Dan Manajemen West Science*, *2*(03), 297–305.

Rukmana, A. Y., Rahman, R., Afriyadi, H., Moeis, D., Setiawan, Z., Subchan, N., Magdalena, L., Singadji, M., El Rayeb, A., & Kusuma, A. T. A. P. 2023. *PENGANTAR SISTEM INFORMASI: Panduan Praktis Pengenalan Sistem Informasi & Penerapannya*. PT. Sonpedia Publishing Indonesia.

Rukmana, A. Y., & Sudarmanto, E. 2023. Transformasi Bisnis dan Manajemen: Dampak Implementasi Teknologi 5G di Era Konektivitas Cepat. *Jurnal Bisnis Dan Manajemen West Science*, *2*(03), 226–238.

Sadiku, M. N. O., & Akujuobi, C. M. 2022. *Fundamentals of Computer Networks*. Springer.

Seberry, J., & Pieprzyk, J. 1989. *Cryptography: an introduction to computer security*. Prentice-Hall, Inc.

Setiawan, Z., Jauhar, N., Putera, D. A., Santosa, A. D., Fenanlampir, K., Sembel, H. F., Harto, B., Roza, T. A., Dermawan, A. A., & Rukmana, A. Y. 2023. *Kewirausahaan Digital*. Global Eksekutif Teknologi.

Sjioen, A. E., Rukmana, A. Y., & Wahyudi, I. 2023. Bisnis Berkelanjutan dan Tanggung Jawab Sosial Perusahaan: Studi tentang Dampak dan Strategi Implementasi. *Jurnal Bisnis Dan Manajemen West Science*, *2*(03), 239–248.

Strinati, E. C., & Barbarossa, S. 2021. 6G networks: Beyond Shannon towards semantic and goal-oriented communications. *Computer Networks*, *190*, 107930.

Tang, W., Dai, J. Y., Chen, M., Li, X., Cheng, Q., Jin, S., Wong, K., & Cui, T. J. 2019. Programmable metasurface-based RF chain-free 8PSK wireless transmitter. *Electronics Letters*, *55*(7), 417–420.

Tawalbeh, L., Muheidat, F., Tawalbeh, M., & Quwaider, M. 2020. IoT Privacy and security: Challenges and solutions. *Applied Sciences*, *10*(12), 4102.

Taylor, M., Haggerty, J., Gresty, D., & Lamb, D. 2011. Forensic investigation of cloud computing systems. *Network Security*, *2011*(3), 4–10.

Ukil, A., Sen, J., & Koilakonda, S. 2011. Embedded security for Internet of Things. *2011 2nd National Conference on Emerging Trends and Applications in Computer Science*, 1–6.

Vlačić, B., Corbo, L., e Silva, S. C., & Dabić, M. 2021. The evolving role of artificial intelligence in marketing: A review and research agenda. *Journal of Business Research*, *128*, 187–203.

Wahdiniawati, S. A., Rukmana, A. Y., Ma'sum, H., Pasaribu, J. S., Fauzan, R., Soetikno, Y. J. W., Aditya, A., & Harto, B. 2023. *ENTERPRISE INFORMATION SYSTEM*. Get Press Indonesia.

Wakil, A., Cahyani, R. R., Harto, B., Latif, A. S., Hidayatullah, D., Simanjuntak, P., Rukmana, A. Y., & Sihombing, F. A. H. 2022. *Transformasi Digital Dalam Dunia Bisnis*. Global Eksekutif Teknologi.

Wang, Y., Su, Z., Zhang, N., Xing, R., Liu, D., Luan, T. H., & Shen, X. 2022. A survey on metaverse: Fundamentals, security, and privacy. *IEEE Communications Surveys & Tutorials*.

Wei, Z., Yuan, W., Li, S., Yuan, J., Bharatula, G., Hadani, R., & Hanzo, L. 2021. Orthogonal time-frequency space modulation: A promising next-generation waveform. *IEEE Wireless Communications*, *28*(4), 136–144.

Yu, J., Ye, X., & Li, H. 2022. A high precision intrusion detection system for network security communication based on multi-scale convolutional neural network. *Future Generation Computer Systems*, *129*, 399–406.

BAB 4
INFRASTRUKTUR JARINGAN

Oleh James Philip

4.1 Pendahuluan

Jaringan komputer adalah adanya komputer- komputer yang terdiri dari dua atau lebih terhubung satu sama lain melalui media transmisi yang sesuai yang memungkinkan mereka untuk berbagi data dengan menggunakan protokol komunikasi dalam menyediakan layanan dan sumber daya kepada pengguna berupa: file, folder, printer, email, database (Kustanto & Saputro, 2008)

Pengertian lain dari jaringan komputer adalah setiap kelompok komputer yang terhubung bersama dapat disebut jaringan komunikasi data dan dapat berbagi layanan dan sumber daya kepada pengguna berupa aplikasi web, jejaring sosial, VoIP, konferensi multimedia (Oetomo, 2003).

Setiap kelompok komputer yang terhubung bersama dan proses berbagi sumber daya antar komputer melalui komunikasi data jaringan dengan tujuan:

1. Berbagi file antara dua komputer
2. Obrolan video (video chatting) antar berbagai tempat di dunia
3. Berselancar di web
4. Pesan instan (IM, instant messaging) antara komputer dengan perangkat lunak IM yang terinstal
5. Surat elektronik (E-mail)
6. Suara melalui IP (VoIP)

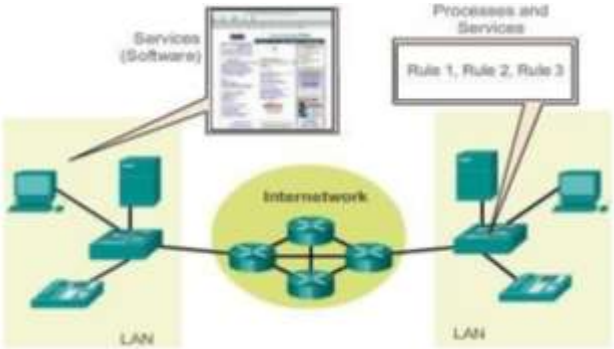
Jaringan konvergensi adalah jaringan yang menyediakan banyak layanan (video, suara, dan data) melalui satu infrastruktur.

Koneksi internet kabel adalah contoh jaringan konvergen. Jenis jaringan ini menggunakan infrastruktur yang sama untuk menyediakan layanan internet dan televisi kabel. Jaringan konvergensi menawarkan banyak manfaat, termasuk peningkatan efisiensi dan biaya yang lebih rendah (Jessica, 2022).

4.2 Komponen-komponen Jaringan

Komponen-komponen jaringan adalah:

1. Elemen fisik atau perangkat keras seperti router, WAP (*wireless access point*), laptop, switch, kabel yang digunakan untuk menghubungkan perangkat, … dll.
2. Layanan, disebut perangkat lunak, yang memberikan informasi sebagai respons terhadap permintaan seperti layanan hosting email dan layanan hosting web.



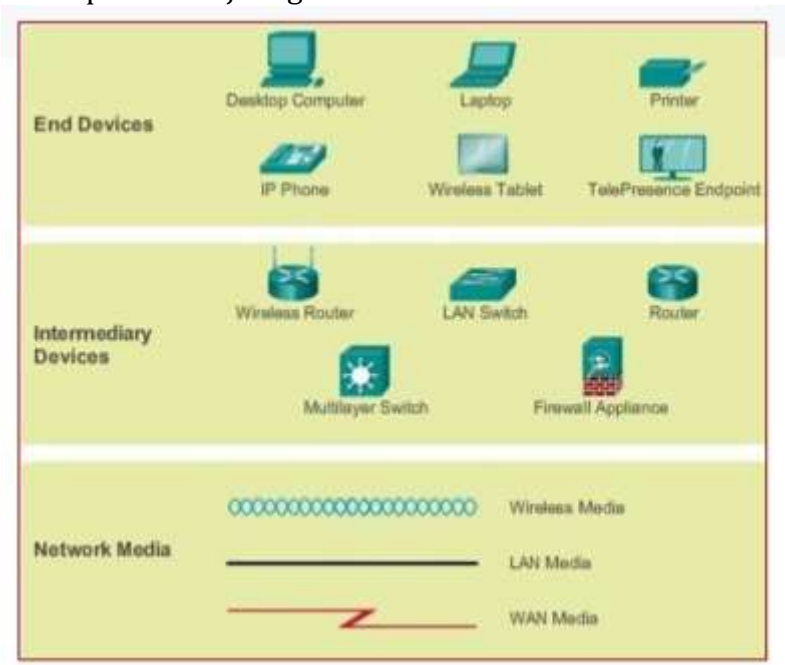
Gambar 4.1. Komponen-komponen jaringan

Komponen-komponen fisik jaringan berupa:

1. Host: perangkat ini membentuk antarmuka antara pengguna dan jaringan komunikasi. Contoh host adalah komputer (*work station, laptop, file server, web server*), printer jaringan, telepon VoIP, perangkat genggam seluler, dan lain-lain. Perangkat host adalah sumber atau tujuan pesan yang dikirimkan melalui jaringan.

2. Perangkat jaringan perantara: menghubungkan host ke jaringan dan dapat menghubungkan beberapa jaringan individual untuk membentuk suatu internetwork, internet (gabungan dari berbagai jaringan komputer). Contoh perangkat perantara adalah switch, wireless access point, router, firewall, dan lain-lain. Perangkat ini menggunakan alamat host tujuan untuk menentukan jalur pesan yang harus diambil melalui jaringan.
3. Media Jaringan: Media menyediakan saluran dari mana pesan dikirimkan oleh sumber ke tujuan. Ketiga jenis media tersebut adalah Copper (Coaxial, STP, UTP), Fiber Optic, dan Wireless.

Contoh representasi jaringan:



Gambar 4.2. Representasi jaringan.

NIC (*Network Interface Card*): adalah perangkat yang dipasang di komputer, printer, atau komponen jaringan lainnya sehingga dapat terhubung ke suatu jaringan.

Gambar 4.3. NIC (*Network Interface Card*)

Klien: Istilah klien mendefinisikan perangkat yang digunakan pengguna akhir untuk mengakses jaringan. Contoh: workstation, laptop, tablet, smartphone, televisi, server, atau perangkat terminal lainnya. Bisa juga berupa perangkat apa saja yang terhubung ke jaringan.

Gambar 4.4. Klien

Server: Server menyediakan sumber daya ke jaringan (Email, Web pages, atau file). Server yang berbeda menyediakan fungsi yang berbeda, seperti E-mail server, Web server, File server, Chat server dan Print server. Dapat berupa server khusus perangkat keras/perangkat lunak ataupun dapat berupa perangkat yang bertindak seperti server untuk fungsi tertentu.

Gambar 4.5. Server

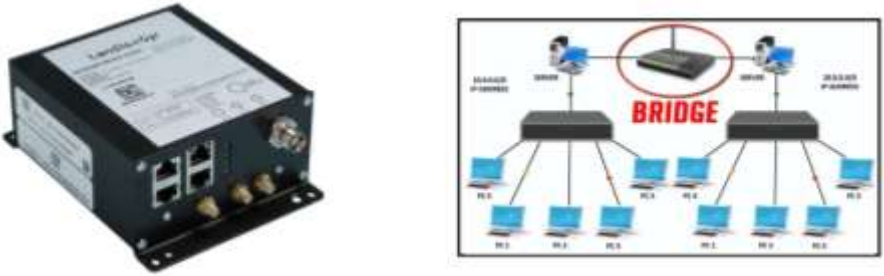
Hub adalah perangkat yang berisi banyak port untuk menghubungkan beberapa komputer atau perangkat jaringan satu sama lain. Ketika sebuah komputer mengirimkan data melalui hub, maka hub tersebut akan broadcast data tersebut ke seluruh komputer lain yang terhubung dengannya. Broadcast: data dikirim ke setiap perangkat di jaringan.

Gambar 4.6. Hub

Switch: adalah perangkat yang berisi banyak port untuk menghubungkan beberapa komputer atau perangkat jaringan satu sama lain. Berbeda dengan hub, switch hanya dapat mengirimkan data ke komputer yang dituju.

Gambar 4.7. Swich

Bridge: dapat dikatakan bahwa bridge adalah versi lama dari switch, dimana bridge bekerja hampir seperti swich.



Gambar 4.8. Bridge

Router: adalah perangkat yang tujuan utamanya adalah menghubungkan dua atau lebih jaringan dan menentukan titik jaringan berikutnya dimana data harus diteruskan untuk mencapai tujuannya.

Gambar 4.9. Router

Wireless Access Point (WAP):

1. WAP memungkinkan perangkat wireless terhubung ke jaringan kabel
2. Biasa digunakan di rumah, usaha kecil bahkan beberapa perusahaan besar
3. Bertindak sebagai hub wireless

Gambar 4.10. Wireless Access Point (WAP)

Media jaringan: Hubungkan dua perangkat atau satu perangkat ke port. Terbuat dari kabel tembaga, kabel serat optik atau gelombang frekuensi radio (WiFi). Masing-masing jenis memiliki kekuatan dan keterbatasan, seperti bandwidth yang

tersedia, kapasitas, jarak yang dapat ditempuh, serta biaya pemasangan dan pemeliharaan.

Gambar 4.11. Media jaringan

4.3 Tipe Jaringan

Jaringan komputer dapat dibagi berdasarkan skala dan fungsinya.

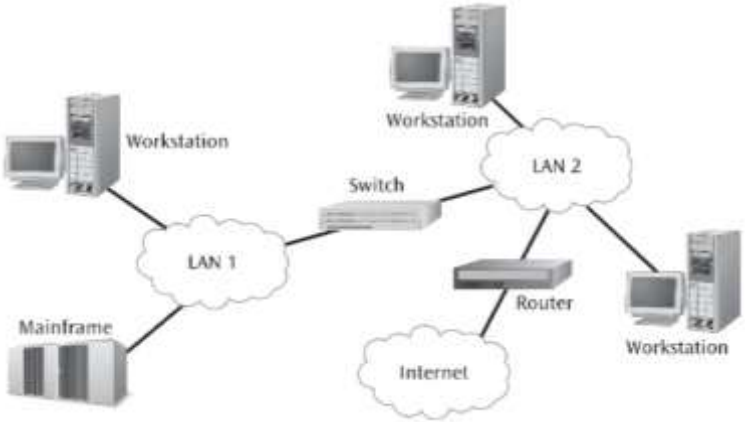
4.3.1 Tipe jaringan berdasarkan skalanya

Klasifikasi *computer network* atau jenis-jenis jaringan komputer dapat berdasarkan jangkauan geografis (Sofana, 2013). Berdasarkan skalanya ini, jaringan komputer terbagi menjadi 6 jenis yaitu Jaringan Area Pribadi (*Personal Area Network*, PAN), Jaringan Area Lokal (*Local Area Network*, LAN), Jaringan Area Kampus (*Campus Area Network*, CAN), Jaringan Area Metropolitan (*Metropolitan Area Network*, MAN), Jaringan Area Luas (*Wide Area Network*, WAN) dan Jaringan Area Global (*Global Area Network*, GAN).

Personal Area Network (PAN) merupakan jenis jaringan kabel atau wireless. Mencakup area paling sedikit (beberapa meter) yaitu sekitar 9-10 meter. Contoh: Ponsel Bluetooth ke mobil, harddisk USB ke laptop, video kamera Firewire ke komputer. PAN dapat menggunakan teknologi kabel (*wire*) dengan USB dan Firewire, PAN dengan teknologi nirkabel (*wireless*) melalui Bluetooth, WiFi, dan Infrared.

LAN (*Local Area Network*) adalah jaringan yang menghubungkan komputer dan perangkat di wilayah geografis yang terbatas seperti rumah, sekolah, laboratorium komputer, kantor bangunan, atau kelompok bangunan yang letaknya

berdekatan. LAN menghubungkan komponen dalam jarak terbatas. LAN tidak termasuk Internet, meskipun mungkin terhubung ke Internet. Setiap segmen dibatasi untuk jarak pendek, misalnya 100 meter dengan kabel CAT 5. Terdiri dari jaringan Ethernet (IEEE 802.3) atau WiFi (802.11). Contoh: Jaringan kabel atau wireless internal.

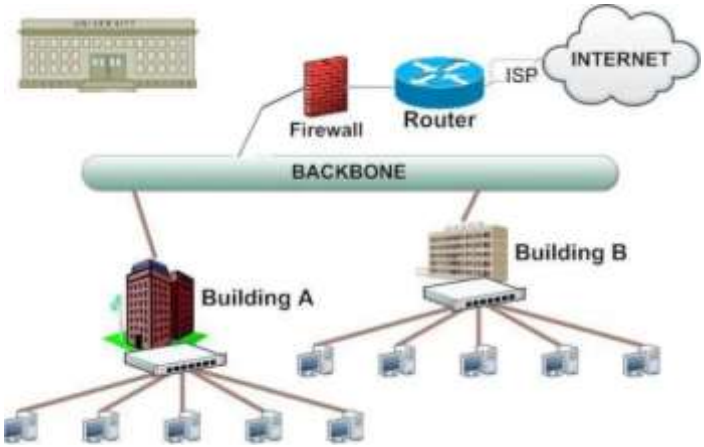


Gambar 4.12. Jaringan LAN terhubung dengan jaringan LAN, Internet, dan komputer mainframe

Keuntungan LAN:

1. Berbagi sumber daya secara efisien
2. Stasiun kerja (*workstation*) individu mungkin bertahan dari kegagalan jaringan, jika tidak bergantung pada stasiun kerja lain
3. Evolusi komponen tidak bergantung pada evolusi sistem
4. Mendukung perangkat keras/perangkat lunak yang heterogen
5. Akses ke LAN dan WAN lain
6. Kecepatan transfer tinggi dengan tingkat kesalahan rendah

Campus Area Network (CAN): menghubungkan LAN yang berpusat pada gedung di universitas, kawasan industri, atau kawasan bisnis. CAN mencakup banyak mil persegi dan bangunan. Contoh: kampus perguruan tinggi, taman bisnis, pangkalan militer.

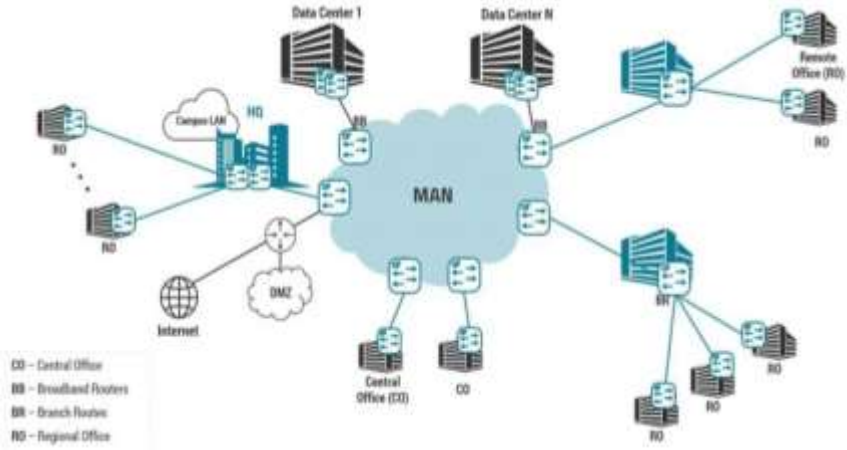


Gambar 4.13. Layout CAN

Setiap gedung di kampus biasanya memiliki satu atau lebih LAN, dengan setiap LAN memiliki sekumpulan komputer yang dihubungkan bersama melalui switch L2. Perangkat jaringan backbone dalam bentuk switch L2 yang lebih kuat menghubungkan LAN dari gedung yang berbeda. Untuk komunikasi eksternal ke internet, switch backbone L2 terhubung ke Router L3 (biasanya disebut gateway eksternal). Jaringan Perusahaan/Perusahaan kecil mirip dengan CAN.

Metropolitan Area Network (MAN): menghubungkan lokasi yang tersebar di seluruh kota. Lebih besar dari CAN, namun lebih kecil dari WAN. MAN mungkin merupakan sebuah jaringan tunggal seperti televisi kabel jaringan atau biasanya menghubungkan sejumlah jaringan area lokal (LAN) dengan menggunakan kapasitas

tinggi teknologi backbone, seperti sambungan serat optik, dan menyediakan layanan up-link WAN dan Internet. MAN biasanya beroperasi pada kecepatan 1,5 Mbps hingga 10 Mbps dan panjangnya berkisar dari lima mil hingga beberapa ratus mil. Contoh: departemen kota seperti departemen kepolisian, community college dengan kampus-kampus yang tersebar di suatu daerah.



Gambar 4.14. Layout MAN

Wide Area Network (WAN): jenis jaringan komunikasi data tertua yang menyediakan kecepatan relatif lambat, transmisi jarak jauh data, suara, dan video pada wilayah geografis yang relatif luas dan tersebar luas, seperti negara atau benua. WAN menghubungkan router di lokasi berbeda. WAN berbeda dari LAN dalam beberapa cara penting. Kebanyakan WAN (seperti Internet) tidak dimiliki oleh satu organisasi apapun melainkan berada di bawah kepemilikan kolektif atau terdistribusi dan pengelolaan. Terdiri dari jalur sewaan atau Virtual Private Networks yang disalurkan melalui Internet. Mencakup jarak di seluruh negeri atau

di seluruh dunia. Contoh: Internet (WAN terbesar), menghubungkan dua jaringan perusahaan swasta dari New York ke Seattle.

Gambar 4.15. Geografi Jaringan

GAN menyediakan koneksi antar negara di seluruh dunia. Internet adalah contoh yang baik dan pada dasarnya adalah jaringan yang terdiri dari jaringan lain yang menghubungkan hampir setiap negara di dunia. GAN beroperasi dari 1,5 Mbps hingga 100 Gbps dan menempuh jarak ribuan mil.

4.3.2 Berdasarkan pola operasinya

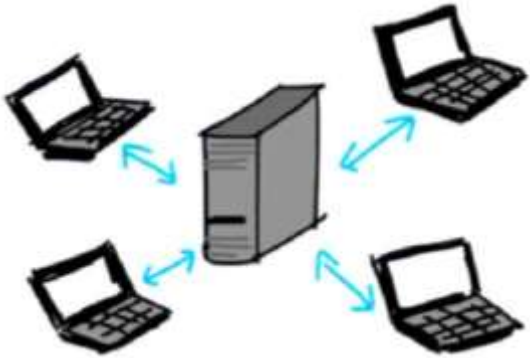
Berdasarkan pola operasi, jaringan komputer dapat dibagi menjadi:

Model Peer to peer: jenis jaringan komputer di mana setiap komputer bisa menjadi server sekaligus client. Setiap komputer dapat menerima dan memberikan acces dari atau ke komputer lain. Peer (PC) berbagi sumber daya (file/printer) satu sama lain secara langsung. Administrasi dan backup lebih sulit karena sumber daya terletak di banyak PC sehingga menambah beban administratif.

Gambar 4.16. Model Peer to peer

Manfaat *Peer to Peer*: biaya rendah, tidak diperlukan sumber daya khusus, tidak diperlukan sistem operasi khusus. Kekurangan *Peer to Peer*: manajemen terdesentralisasi, tidak efisien untuk jaringan besar, skalabilitas yang buruk.

a. Model Klien/Server: Di sini, satu komputer ditunjuk sebagai server dan komputer lainnya adalah client. Arsitektur Dedicated Server dapat meningkatkan efisiensi sistem client-server dengan menggunakan satu server untuk setiap aplikasi yang ada dalam sebuah organisasi. Server yang ditunjuk menyimpan semua file dan aplikasi jaringan untuk program dan berfungsi hanya sebagai server dan tidak digunakan sebagai klien atau workstation. Klien komputer dapat mengakses server dan berbagi file yang ditransfer ke server tersebut melalui media transmisi. Di beberapa jaringan klien/server, komputer klien mengirimkan pekerjaan ke satu server dan setelah mereka memproses pekerjaan, hasilnya dikirim kembali ke klien komputer. Administrasi dan backup lebih mudah karena sumber daya terletak di beberapa server utama.



Gambar 4.17. Model Klien/Server

Manfaat Klien/Server: administrasi terpusat, manajemen lebih mudah, skalabilitas yang lebih baik.

Kekurangan Klien/Server: biaya lebih tinggi, membutuhkan sumber daya khusus, membutuhkan sistem operasi jaringan.

4.4 Topologi Jaringan

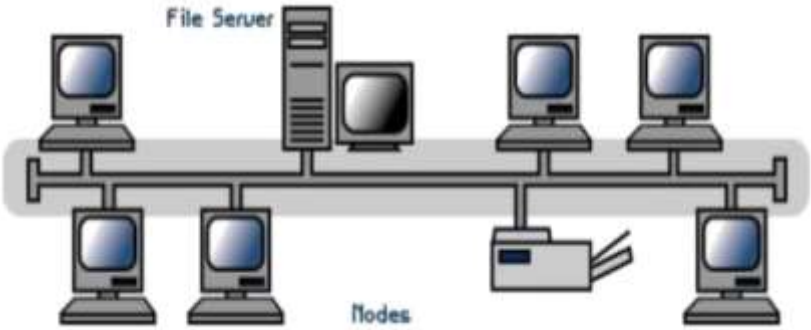
Dalam jaringan komputer, topologi mengacu pada tata letak perangkat yang terhubung, yaitu bagaimana komputer, kabel, dan komponen lain dalam jaringan komunikasi data saling berhubungan, baik secara fisik maupun logis. Terdapat dua macam topologi yaitu:

1. Topologi Fisik: Bagaimana perangkat terhubung secara fisik melalui media
2. Topologi Logis : Bagaimana arus lalu lintas sebenarnya dalam jaringan.

4.4.1 Topologi fisik

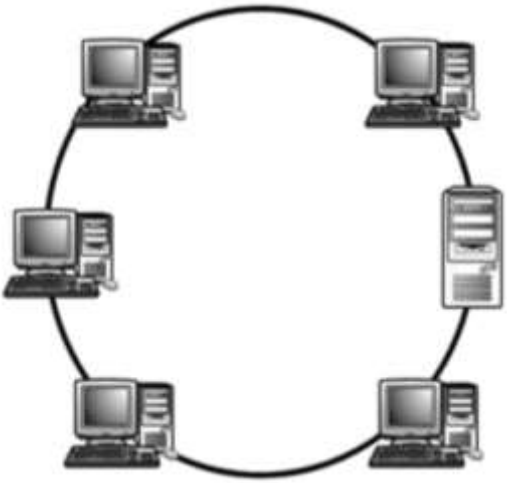
Topologi Fisik secara umum terdapat 6 model besar, yakni *Bus, Ring, Star, Extended Star, Mesh* dan *Hybrid* (Herlambang, Moch. Linto & Catur L., 2008).

Topologi Bus: menggunakan kabel yang melintasi area yang memerlukan konektivitas jaringan. Topologi bus adalah metode paling sederhana dan paling umum untuk menghubungkan komputer. Teknologi lama, sudah tidak umum digunakan lagi. Perangkat pada kabel membentuk domain tabrakan tunggal.



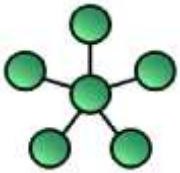
Gambar 4.18. Topologi bus

Topologi Cincin (ring): menggunakan kabel yang berjalan melingkar. Setiap perangkat terhubung ke ring, tetapi data bergerak dalam satu arah. FDDI (jaringan Fiber) menggunakan dua cincin counter-rotating untuk redundansi. Pada jaringan token ring, perangkat menunggu giliran untuk berkomunikasi di ring dengan meneruskan token. Dalam jaringan ring (terkadang disebut loop), setiap perangkat memiliki persis dua tetangga untuk tujuan komunikasi. Semua pesan berjalan melalui sebuah cincin di arah yang sama (baik searah jarum jam atau berlawanan arah jarum jam). Semua stasiun ada saling berhubungan secara tandem (seri) sehingga membentuk suatu putaran atau lingkaran tertutup. Transmisi adalah searah dan harus merambat melalui semua stasiun dalam loop.



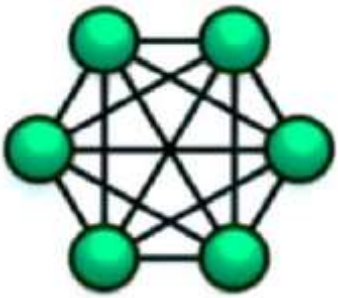
Gambar 4.19. Topologi bus

Topologi Bintang (Star): topologi fisik LAN paling populer. Perangkat terhubung ke satu titik. Paling umum digunakan dengan kabel Ethernet, tetapi wireless atau fiber juga digunakan. Jika perangkat pusat gagal, seluruh jaringan gagal.



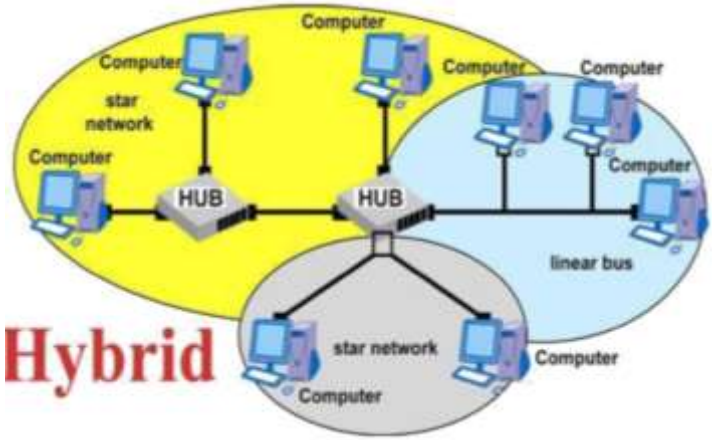
Gambar 4.20. Topologi ring

Topologi Mesh Penuh: topologi paling redundan. Setiap node terhubung ke setiap node lainnya. Perutean optimal selalu tersedia. Sangat mahal untuk pemeliharaan dan pengoperasiannya. Jumlah koneksi: x = $n \frac{(n-1)}{2}$.



Gambar 4.21. Topologi mesh penuh

Topologi Mesh Parsial: topologi ini (terkadang disebut topologi hybrid) gabungan dua atau lebih topologi tradisional untuk membentuk topologi yang lebih besar dan kompleks. Tujuan utamanya adalah untuk dapat berbagi keuntungan dari topologi yang berbeda. Menyediakan rute optimal antar beberapa situs, sekaligus menghindari biaya menghubungkan setiap situs. Harus mempertimbangkan pola lalu lintas jaringan untuk merancangnya secara efektif.



Gambar 4.22. Topologi mesh parsial (hybrid)

4.4.2 Topologi logika

Topologi logika menjelaskan bagaimana data sebenarnya mengalir melalui jaringan. Topologi ini pada umumnya ada 5 macam, yaitu: Ethernet, Token Ring, Local Talk, FDDI (*Fiber Distributed Data Interface*), dan ATM (*Asynchronous Transfer Mode*). Atau dapat dikatakan secara umum terdapat dua jenis topologi logika, yaitu:

1. *Broadcast.* Topologi Broadcast adalah tipe pertama dari topologi logic komputer dimana dapat digambarkan yaitu suatu host yang mengirimkan data kepada seluruh host lain pada media jaringan. Topologi Logis adalah susunan perangkat jaringan dan node untuk membentuk struktur logis atau fisik. Ada berbagai jenis topologi jaringan yang dapat digunakan untuk menyusun node jaringan hingga membentuk struktur jaringan. Arti harfiah dari topologi adalah struktur jaringan dan node-node yang saling berhubungan. Jadi pada topologi ini semua komputer yang berperan sebagai client atau user menerima secara penuh semua data yang dimiliki oleh komputer server atau host, tanpa adanya suatu batasan atau limitasi pada masing – masing user atau client. Prinsip pada topologi ini adalah First Come First Serve, First In First Out (FCFS/FIFO). Topologi logis berarti bagaimana tata letak perangkat jaringan akan ditampilkan dan bagaimana data akan ditransfer. Misalnya - Ring, Bus, Star, dan Mesh.
2. *Token Passing*. Jaringan token-ring adalah topologi jaringan area lokal (LAN) yang mengirimkan data dalam satu arah ke sejumlah lokasi tertentu dengan menggunakan token. Token adalah simbol otoritas untuk mengendalikan saluran transmisi. Pada jaringan area local (LAN), token passing adalah metode akses saluran di mana paket yang disebut token diteruskan antar node untuk memberi otorisasi pada node tersebut untuk berkomunikasi.

Berbeda dengan metode akses polling, tidak ada node "master" yang telah ditentukan sebelumnya. Jadi hanya komputer client atau user yang memilki token saja yang berhak dan dapat melakukan akses data ke dalam server ataupun host dalam suatu jaringan komputer. Ketika host menerima token. Maka host tersebut dapat mengirim data. Jika tidak ada data yang dikirim maka token tersebut dilewatkan ke host berikutnya dan proses ini berulang terus-menerus. Jadi mengatur pengiriman data pada host melalui media dengan menggunakan token yang secara teratur berputar pada seluruh host. Penggunaan token passing dapat ditemukan pada *Token Ring* dan *Fiber Distributed Data Interface (FDDI).*

DAFTAR PUSTAKA

Herlambang, Moch. Linto & Catur L., A. . *Panduan lengkap Menguasai Router Masa Depan Menggunakan Mikrotik RouterOS*. Yogyakarta: Andi.

Jessica. 2022. *A Converged Network: What It Is And Why It Matters*, *OpenWorldLearning*. Available at: https://www.openworldlearning.org/a-converged-network-what-it-is-and-why-it-matters/#google_vignette.

Kustanto & Saputro, D. T. 2008. *Membangun server internet dengan mikrotik OS*. Gava Media.

Oetomo, B. S. D. 2003. *Konsep dan Perancangan Jaringan Komputer*. Yogyakarta: Andi.

Sofana, I. 2013. *Membangun Jaringan Komputer*. Bandung: Informatika.

BAB 5
PROTOKOL JARINGAN

Oleh Angga Aditya Permana

5.1 Pendahuluan

Gambar 5.1. Protokol jaringan
Sumber : https://jagad.id/

Protokol jaringan adalah seperangkat aturan, prosedur, dan standar yang digunakan dalam komunikasi dan pertukaran data antara perangkat yang terhubung ke jaringan komputer. Tujuan utama dari protokol ini adalah untuk memastikan bahwa perangkat di dalam jaringan dapat berkomunikasi dengan benar dan efisien. Protokol jaringan menentukan bagaimana data dikirim,

diterima, dan diproses, serta bagaimana kesalahan dan konflik dapat diatasi. Dengan adanya protokol, perangkat dari berbagai vendor dan platform yang berbeda dapat berinteraksi secara interoperabel, yang merupakan kunci keberhasilan jaringan komputer modern. (Logistics 2008; Davie 2012)

Salah satu komponen penting dari protokol jaringan adalah format data yang digunakan untuk mengemas informasi yang akan dikirim. Ini mencakup struktur data, pengkodean, dan pembungkus data, yang memungkinkan perangkat untuk memahami dan menguraikan pesan yang diterima. Selain itu, protokol jaringan juga mengatur proses autentikasi, otorisasi, dan enkripsi untuk menjaga keamanan dan privasi data yang ditransmisikan.

Protokol jaringan dapat berlaku pada berbagai tingkatan dalam jaringan, mulai dari tingkat fisik (seperti protokol Ethernet untuk transmisi data di kabel) hingga tingkat aplikasi (seperti HTTP untuk komunikasi web). Selain itu, protokol ini juga dapat digunakan dalam jaringan lokal (LAN) maupun jaringan luas (WAN) untuk menghubungkan perangkat di berbagai lokasi geografis.

Ketika perangkat dalam jaringan ingin berkomunikasi, mereka harus sepakat untuk menggunakan protokol yang sama. Ini disebut sebagai "negosiasi protokol" dan terjadi sebelum pertukaran data dimulai. Setiap protokol memiliki peran dan fungsi tertentu dalam jaringan, yang dapat berupa pengiriman pesan, pertukaran file, pengaksesan situs web, atau layanan lainnya sesuai dengan jenis protokol yang digunakan.

Dalam dunia yang semakin terhubung dan kompleks, protokol jaringan menjadi pondasi yang krusial dalam menjaga keterhubungan dan komunikasi yang andal antara berbagai perangkat dan aplikasi. Protokol ini terus berkembang seiring perkembangan teknologi jaringan untuk memenuhi tuntutan yang semakin meningkat akan kinerja, keamanan, dan kehandalan jaringan komputer.

Jaringan perlu protokol karena protokol adalah seperangkat aturan dan standar yang mengatur komunikasi dan pertukaran data antara perangkat yang terhubung ke jaringan komputer. Ada beberapa alasan mengapa protokol sangat penting dalam jaringan:

1. Interoperabilitas: Protokol memastikan bahwa perangkat dari berbagai vendor, platform, dan sistem operasi dapat berkomunikasi secara efektif dan saling memahami. Tanpa protokol yang seragam, perangkat mungkin tidak dapat berkomunikasi satu sama lain, yang akan menghambat pertukaran data dan kolaborasi di dalam jaringan.
2. Ketepatan: Protokol memastikan bahwa data dikirim, diterima, dan diproses dengan benar. Mereka mendefinisikan format data, pengkodean, dan cara pengiriman data. Ini membantu mencegah kesalahan dalam komunikasi, yang dapat menyebabkan kerusakan data atau ketidaksesuaian.
3. Keamanan: Banyak protokol jaringan mencakup fitur-fitur keamanan seperti autentikasi, otorisasi, dan enkripsi. Ini membantu melindungi data yang dikirimkan melalui jaringan dari akses yang tidak sah dan pemantauan oleh pihak ketiga yang tidak diinginkan.
4. Pengelolaan Jaringan: Protokol jaringan memungkinkan administrator jaringan untuk mengelola dan mengawasi kinerja jaringan dengan lebih baik. Mereka dapat memantau lalu lintas jaringan, mendeteksi masalah, dan menerapkan kebijakan keamanan dan manajemen dengan lebih efisien berkat penggunaan protokol yang konsisten.
5. Kontrol Kesalahan: Protokol sering menyertakan metode untuk mendeteksi dan mengatasi kesalahan dalam komunikasi. Contohnya, dalam protokol TCP/IP, ada mekanisme pengiriman ulang (*retransmission*) untuk

memastikan bahwa data yang hilang atau rusak diterima dengan benar.

6. Optimasi Kinerja: Protokol dapat dirancang untuk mengoptimalkan kinerja jaringan dengan cara seperti kompresi data, caching, dan pengaturan prioritas untuk jenis lalu lintas tertentu. Ini membantu meningkatkan efisiensi penggunaan bandwidth dan mengurangi waktu yang diperlukan untuk mentransfer data.
7. Dengan kata lain, protokol jaringan adalah dasar dari semua komunikasi dan pertukaran data dalam jaringan komputer. Mereka memastikan bahwa jaringan beroperasi dengan baik, efisien, aman, dan dapat dielola dengan baik. Tanpa protokol, jaringan modern tidak akan berfungsi dengan baik dan tidak akan mampu memenuhi tuntutan kompleks dari berbagai aplikasi dan layanan yang dijalankan di atasnya.

5.2 Hal Penting Dalam Protokol

Gambar 5.2. Penting dalam Protokol
Sumber : https://lamantekno.com/

Dalam merancang, menerapkan, dan mengelola protokol jaringan, ada beberapa hal penting yang perlu diperhatikan: (Logistics 2008; Davie 2012)

1. Kepatuhan Standar: Pastikan protokol yang digunakan sesuai dengan standar industri yang berlaku. Kepatuhan standar membantu memastikan interoperabilitas dengan perangkat dan sistem lain, serta memungkinkan pengembangan jaringan yang dapat diandalkan dan dapat dikelola.
2. Keamanan: Pertimbangkan aspek keamanan saat merancang atau memilih protokol. Pastikan protokol ini memiliki mekanisme keamanan yang memadai, seperti autentikasi, otorisasi, enkripsi, dan perlindungan terhadap serangan jaringan seperti serangan Denial of Service (DoS) atau serangan Man-in-the-Middle (MitM).
3. Kinerja: Protokol harus memiliki kinerja yang baik agar tidak menghambat lalu lintas jaringan atau membuat jaringan bekerja lambat. Pertimbangkan latensi, throughput, dan penggunaan sumber daya saat memilih atau merancang protokol.
4. Skalabilitas: Protokol harus mampu beroperasi dengan baik dalam lingkungan jaringan yang berkembang. Protokol yang baik harus dapat menangani peningkatan jumlah perangkat, lalu lintas, dan beban jaringan tanpa mengurangi kinerja atau kehandalan.
5. Manajemen dan Monitoring: Protokol harus mendukung kemampuan manajemen jaringan dan pemantauan kinerja. Ini penting untuk mengelola jaringan dengan efisien, mendeteksi masalah dengan cepat, dan mengambil tindakan yang diperlukan.
6. Toleransi Kesalahan: Protokol sebaiknya memiliki mekanisme untuk mendeteksi dan mengatasi kesalahan dalam komunikasi, termasuk pengiriman ulang data yang

hilang atau rusak. Ini penting untuk memastikan keandalan komunikasi dalam jaringan.

7. Efisiensi Penggunaan Bandwidth: Protokol harus dirancang untuk mengoptimalkan penggunaan bandwidth jaringan. Ini dapat mencakup kompresi data, penghapusan redundansi, dan manajemen aliran lalu lintas.
8. Kebijakan Keamanan dan Privasi: Pastikan protokol memungkinkan penerapan kebijakan keamanan dan privasi yang sesuai dengan kebutuhan organisasi. Ini bisa mencakup kontrol akses, pengaturan hak akses, dan audit.
9. Kompatibilitas Mundur: Jika memungkinkan, pastikan protokol mendukung kompatibilitas mundur dengan versi sebelumnya. Ini membantu organisasi dalam mengadopsi perubahan teknologi secara bertahap.
10. Dokumentasi dan Pelatihan: Penting untuk memiliki dokumentasi yang baik dan pelatihan bagi personel yang akan menggunakan atau mengelola protokol tersebut. Ini membantu menghindari kesalahan penggunaan dan pemahaman yang salah.
11. Pemeliharaan dan Pembaruan: Protokol jaringan perlu dipelihara dan diperbarui sesuai dengan perkembangan teknologi dan kebutuhan organisasi. Pastikan ada proses pemeliharaan yang terencana dan mekanisme untuk mengatasi kerentanan atau masalah yang mungkin muncul.
12. Pengujian: Sebelum mengimplementasikan protokol dalam lingkungan produksi, lakukan pengujian menyeluruh untuk memastikan kinerjanya sesuai dengan ekspektasi dan memenuhi persyaratan organisasi.

Memperhatikan aspek-aspek di atas membantu memastikan bahwa protokol jaringan yang digunakan atau dirancang memenuhi kebutuhan organisasi dan berfungsi dengan baik dalam lingkungan yang selalu berubah. Selain itu, protokol

harus dikelola secara efisien selama seluruh siklus hidupnya, termasuk pemeliharaan dan pembaruan secara berkala.

5.3 Macam-macam Protokol

Gambar 5.3. Macam-macam Protokol
Sumber : https://www.nesabamedia.com/

Ada banyak protokol yang digunakan dalam berbagai lapisan dan aspek jaringan komputer. Berikut adalah beberapa contoh protokol yang umum digunakan dalam jaringan: (Logistics 2008; Davie 2012)

1. **Protokol Transport Layer:**
   a. TCP (*Transmission Control Protocol*): Protokol ini menyediakan pengiriman data yang andal dan terurut di antara perangkat dalam jaringan.
   b. UDP (*User Datagram Protocol*): Protokol ini menyediakan pengiriman data yang lebih cepat tetapi tidak andal, sering digunakan untuk aplikasi yang

memerlukan respons cepat seperti streaming video dan game online.

2. **Protokol Internet Layer:**
   a. IP (*Internet Protocol*): Protokol ini digunakan untuk mengatur alamat dan routing data di seluruh internet.
   b. ICMP (*Internet Control Message Protocol*): Protokol ini digunakan untuk mengirim pesan kesalahan dan kontrol di jaringan IP, seperti pesan ping.

3. **Protokol Application Layer:**
   a. HTTP (*Hypertext Transfer Protocol*): Digunakan untuk mengirimkan dokumen web dan data terkait.
   b. HTTPS (*Hypertext Transfer Protocol Secure*): Versi aman dari HTTP yang menggunakan enkripsi SSL/TLS untuk melindungi data.
   c. FTP (*File Transfer Protocol*): Protokol untuk mentransfer file antara perangkat.
   d. SMTP (*Simple Mail Transfer Protocol*): Digunakan untuk mengirim email.
   e. POP3 (*Post Office Protocol version* 3) dan IMAP (*Internet Message Access Protocol*): Protokol untuk mengakses email dari server.
   f. DNS (*Domain Name System*): Protokol untuk menerjemahkan nama domain menjadi alamat IP.
   g. SNMP (*Simple Network Management Protocol*): Protokol untuk mengelola dan memantau perangkat jaringan.
   h. SSH (*Secure Shell*): Protokol untuk akses aman ke perangkat jaringan melalui koneksi terenkripsi.
   i. Telnet: Protokol untuk akses jarak jauh ke perangkat, tetapi kurang aman dibandingkan dengan SSH.

j. DHCP (*Dynamic Host Configuration Protocol*): Protokol untuk konfigurasi otomatis alamat IP pada perangkat dalam jaringan.

4. Protokol Data Link Layer:

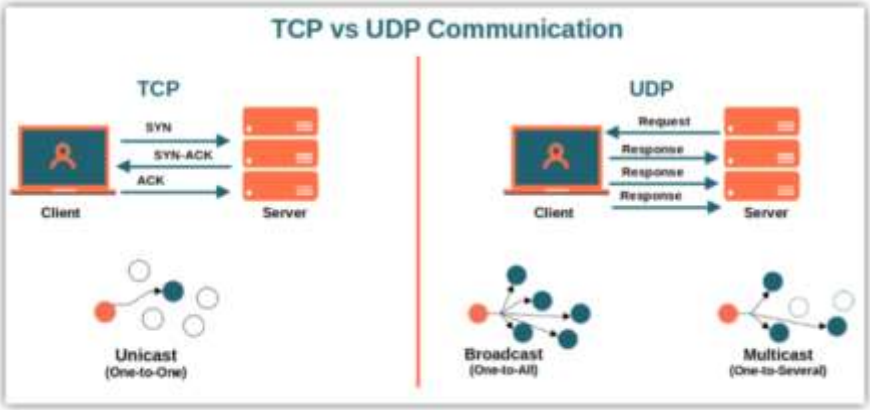
a. Ethernet: Protokol yang digunakan untuk mengirimkan data dalam segmen jaringan lokal (LAN).
b. Wi-Fi: Protokol yang digunakan untuk menghubungkan perangkat nirkabel ke jaringan.
c. PPP (*Point-to-Point Protocol*): Protokol yang digunakan untuk menghubungkan perangkat melalui jalur telepon atau serat optik.

5. Protokol lainnya:

a. BGP (*Border Gateway Protocol*): Protokol yang digunakan dalam routing di internet.
b. OSPF (*Open Shortest Path First*): Protokol routing interior yang digunakan di jaringan besar.
c. SNMP (*Simple Network Management Protocol*): Digunakan untuk memantau dan mengelola perangkat jaringan.
d. ICMP (*Internet Control Message Protocol*): Digunakan untuk mengirim pesan kesalahan dan kontrol di jaringan IP.

Ini hanyalah beberapa contoh protokol yang ada di berbagai lapisan jaringan komputer. Ada banyak lagi protokol lain yang digunakan dalam aplikasi dan lingkungan jaringan yang berbeda, dan penggunaan protokol tertentu akan tergantung pada kebutuhan spesifik dari jaringan Anda.

5.4 TCP VS UDP



Gambar 5.4. TCP vs UDP
Sumber : https://cheapsslsecurity.com/

***Transmission Control Protocol* (TCP)**

TCP adalah protokol yang bekerja pada lapisan transport dalam model referensi OSI. TCP dirancang untuk menyediakan komunikasi yang andal dan terurut antara perangkat dalam jaringan. Di bawah ini adalah cara kerja TCP dengan jelas: (Logistics 2008; Davie 2012)

1. Inisiasi Koneksi (*Three-Way Handshake*):
    a. Ketika perangkat ingin menginisiasi koneksi TCP ke perangkat lain, pertama-tama perangkat tersebut mengirimkan paket khusus yang disebut "SYN" (*synchronize*) ke perangkat tujuan.
    b. Perangkat tujuan menerima paket SYN dan meresponsnya dengan mengirimkan paket SYN-ACK (*synchronize-acknowledgment*) kembali ke perangkat pengirim.
    c. Perangkat pengirim menerima SYN-ACK, dan untuk menyelesaikan inisiasi koneksi, mengirimkan paket ACK (*acknowledgment*) ke perangkat tujuan.

d. Sekarang koneksi TCP telah berhasil dibuat, dan perangkat-perangkat ini dapat mulai berkomunikasi.

2. Pertukaran Data:
   a. Setelah koneksi didirikan, data dapat dikirim antara perangkat pengirim dan perangkat tujuan.
   b. Data yang akan dikirim dibagi menjadi segmen-segmen yang lebih kecil, yang kemudian dimasukkan ke dalam paket-paket TCP.
   c. Setiap paket TCP memiliki nomor urutan (*sequence number*) yang digunakan untuk mengidentifikasi posisi data dalam aliran dan memastikan data diterima dalam urutan yang benar.
   d. Perangkat pengirim mengirimkan paket-paket tersebut ke perangkat tujuan.

3. Konfirmasi Pengiriman:
   a. Ketika perangkat tujuan menerima paket TCP, ia mengirimkan konfirmasi (ACK) kembali ke perangkat pengirim untuk memberi tahu bahwa paket tersebut telah diterima.
   b. Jika perangkat pengirim tidak menerima ACK dalam batas waktu tertentu, itu akan menganggap paket tersebut hilang atau rusak dan akan mengirimkannya kembali.

4. Pengaturan Aliran (Flow Control):
   a. TCP memiliki mekanisme pengaturan aliran yang memungkinkan perangkat pengirim mengendalikan seberapa cepat data dikirim agar tidak membanjiri perangkat tujuan.
   b. Perangkat tujuan dapat mengirimkan sinyal "window size" ke perangkat pengirim, yang mengindikasikan berapa banyak data yang dapat diterima saat ini.

c. Dengan informasi ini, perangkat pengirim dapat mengatur laju pengiriman data untuk menghindari kelebihan beban perangkat tujuan.

5. Penutupan Koneksi:
   a. Ketika komunikasi selesai, salah satu perangkat (biasanya perangkat pengirim) mengirimkan paket FIN (finish) ke perangkat tujuan untuk mengindikasikan bahwa tidak akan ada lagi data yang akan dikirim.
   b. Perangkat tujuan merespons dengan mengirimkan paket ACK sebagai konfirmasi.
   c. Kemudian, perangkat tujuan mengirimkan paket FIN-ACK ke perangkat pengirim, dan perangkat pengirim mengirimkan ACK balik.
   d. Setelah semua paket FIN dan ACK ini ditukar, koneksi TCP dianggap ditutup.

TCP memastikan bahwa data dikirimkan dengan andal, terurut, dan dapat diandalkan di seluruh jaringan, dan jika terjadi kesalahan atau kehilangan paket, TCP akan mengambil tindakan yang diperlukan untuk memastikan pengiriman data yang benar. Ini adalah salah satu alasan mengapa TCP sering digunakan untuk aplikasi yang memerlukan keandalan, seperti transfer file, browsing web, dan email.

***User Datagram Protocol* (UDP)**

UDP adalah protokol yang bekerja pada lapisan transport dalam model referensi OSI. UDP dirancang untuk menyediakan komunikasi yang lebih cepat dan sederhana dibandingkan dengan TCP, tetapi tanpa jaminan pengiriman data yang andal dan terurut. Berikut adalah cara kerja UDP dengan jelas: (Logistics 2008; Davie 2012)

1. Pengemasan Data:
    a. Ketika perangkat ingin mengirim data menggunakan UDP, data yang akan dikirim dikemas ke dalam datagram UDP.
    b. Datagram ini tidak memerlukan inisiasi koneksi seperti yang dilakukan oleh TCP. Perangkat dapat langsung mengirim datagram UDP ke perangkat tujuan tanpa perlu pembentukan koneksi terlebih dahulu.

2. Penyimpanan Alamat Tujuan:
    a. Perangkat pengirim harus mengetahui alamat IP dan nomor port perangkat tujuan agar dapat mengirim datagram UDP ke tempat yang benar.
    b. Datagram UDP ini mungkin akan dikirim ke alamat IP tujuan tertentu dan port tertentu pada perangkat tujuan.

3. Pengiriman Datagram:
    a. Setelah data dikemas ke dalam datagram dan alamat tujuan diketahui, perangkat pengirim mengirim datagram UDP ke jaringan.
    b. Datagram UDP ini akan berisi data yang dikirim dan informasi alamat tujuan.

4. Penerimaan Datagram:
    a. Perangkat tujuan menerima datagram UDP yang dikirimkan oleh perangkat pengirim.
    b. Datagram ini kemudian diuraikan untuk mendapatkan data yang dikirim.

5. Tidak Ada Konfirmasi Pengiriman:
    a. Salah satu perbedaan utama antara UDP dan TCP adalah bahwa UDP tidak memiliki mekanisme

konfirmasi pengiriman. Ini berarti tidak ada ACK (*acknowledgment*) yang dikirim kembali ke perangkat pengirim untuk mengonfirmasi penerimaan datagram.

b. Jika datagram yang dikirimkan menggunakan UDP hilang atau rusak dalam perjalanan, tidak ada upaya otomatis untuk mengirim ulang datagram tersebut. Oleh karena itu, UDP lebih cepat tetapi kurang andal dibandingkan dengan TCP.

6. Tidak Ada Pengaturan Aliran:
   a. UDP tidak memiliki mekanisme pengaturan aliran seperti yang ada pada TCP. Ini berarti perangkat pengirim tidak dapat mengontrol kecepatan pengiriman data berdasarkan kondisi jaringan atau kemampuan perangkat tujuan.
   b. Jika perangkat pengirim mengirim data terlalu cepat dan perangkat tujuan tidak dapat mengikuti, data dapat hilang atau diabaikan.

7. Pemutusan Koneksi Tidak Diperlukan:
   a. Koneksi UDP tidak perlu ditutup seperti yang dilakukan oleh TCP. Datagram UDP dikirim sebagai entitas terpisah dan tidak ada perlu penutupan koneksi formal.

UDP sering digunakan dalam aplikasi yang memerlukan komunikasi yang cepat dan di mana kehilangan beberapa data tidak menjadi masalah besar, seperti dalam streaming video atau permainan online. Namun, karena ketidakandalan dan kurangnya jaminan pengiriman yang dimilikinya, UDP kurang cocok untuk aplikasi yang memerlukan keandalan mutlak dalam pengiriman data, seperti transfer file besar atau email.

TCP VS UDP

Mari kita gunakan analogi sederhana untuk memberikan gambaran perbedaan antara *Transmission Control Protocol* (TCP) dan *User Datagram Protocol* (UDP). (Logistics 2008; Davie 2012)

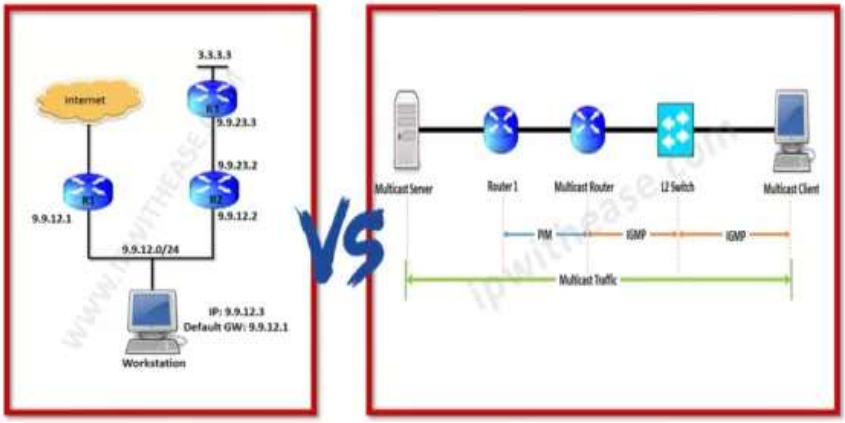
1. TCP (*Transmission Control Protocol*):
   Bayangkan Anda sedang mengirimkan surat yang sangat penting melalui pos. Anda ingin memastikan bahwa surat tersebut sampai ke tujuan dengan benar dan dalam keadaan baik. Dalam hal ini, Anda memilih untuk mengirim surat melalui layanan pos ekspres yang menyediakan pengiriman andal. Anda menulis nomor pelacakan di surat tersebut, sehingga Anda dapat melacaknya setiap kali surat tersebut melewati setiap pos pengiriman. Anda juga meminta penerima untuk mengirimkan konfirmasi setelah mereka menerima surat tersebut. Dengan cara ini, jika surat hilang atau rusak selama perjalanan, Anda akan tahu tentang masalah ini dan dapat mengambil tindakan yang sesuai untuk memastikan surat tersebut tetap aman dan terkirim.
   Dalam analogi ini, TCP adalah seperti layanan pos ekspres yang menjamin pengiriman surat dengan andal, melacaknya di sepanjang jalan, dan memastikan bahwa surat tersebut diterima dengan benar. Ini cocok untuk situasi di mana keandalan dan integritas data sangat penting, seperti mengunduh file besar, browsing web, atau mengirim email penting.

2. UDP (*User Datagram Protocol*):
   Sekarang, bayangkan Anda ingin mengirim undangan ke pesta ulang tahun teman Anda. Undangan ini bukan hal yang sangat penting, dan Anda ingin membuatnya sesederhana mungkin. Anda menulis undangan, meletakkannya di dalam amplop, dan hanya mencantumkan alamat teman Anda di luar amplop. Anda tidak peduli jika amplop tersebut hilang atau rusak

selama perjalanan, dan Anda tidak meminta konfirmasi penerimaan. Anda hanya mengirimkannya sekali dan berharap bahwa teman Anda akan membacanya dan datang ke pesta.
Dalam analogi ini, UDP adalah seperti pengiriman undangan sederhana yang tidak memiliki mekanisme pelacakan, konfirmasi, atau jaminan pengiriman. Ini cocok untuk situasi di mana kecepatan dan efisiensi lebih penting daripada keandalan mutlak, seperti dalam streaming video atau permainan online, di mana data yang tidak sampai dengan sempurna mungkin lebih baik diabaikan daripada menunggu pemulihan.

Dengan kata lain, TCP menekankan keandalan dan pengiriman data yang terurut, sementara UDP menekankan kecepatan dan efisiensi dalam pertukaran data. Pilihan antara keduanya tergantung pada jenis aplikasi dan kebutuhan spesifik dalam komunikasi.

5.5 IP VS ICMP



Gambar 5.5. IP vs ICMP
Sumber : https://networkinterview.com/

***Internet Protocol* (IP)**

IP adalah protokol yang berada di lapisan jaringan dalam model referensi OSI. IP adalah protokol yang mendasari internet dan merupakan inti dari komunikasi data di seluruh dunia. Berikut adalah cara kerja Internet Protocol (IP) dengan jelas: (Logistics 2008; Davie 2012)

1. Penugasan Alamat IP:
    a. Setiap perangkat yang terhubung ke internet diberikan alamat IP yang unik. Alamat IP ini berfungsi seperti alamat rumah dalam jaringan internet dan digunakan untuk mengidentifikasi perangkat di jaringan.
    b. Ada dua versi utama dari IP yang digunakan saat ini: IPv4 (*Internet Protocol version* 4) dan IPv6 (*Internet Protocol version* 6). IPv4 menggunakan alamat IP berbasis angka desimal (contoh: 192.168.1.1), sementara IPv6 menggunakan alamat IP berbasis heksadesimal yang lebih panjang (contoh: 2001:0db8:85a3:0000:0000:8a2e:0370:7334).

2. Pengemasan Data:
    a. Data yang akan dikirim dalam jaringan dibungkus dalam paket atau datagram IP. Setiap paket IP berisi informasi penting, termasuk alamat IP pengirim dan tujuan, serta data yang akan dikirim.

3. Pengiriman Data:
    a. Paket-paket IP dikirimkan ke jaringan. Rute yang akan diambil oleh paket tersebut dalam perjalanan menuju tujuannya ditentukan oleh router di seluruh jaringan.
    b. Router adalah perangkat jaringan yang memutuskan cara terbaik untuk mengirim paket ke tujuan berdasarkan alamat IP tujuan. Mereka menggunakan tabel routing untuk mengambil keputusan ini.

4. Routing:
    a. Router di seluruh jaringan bekerja sama untuk mengirimkan paket dari satu jaringan ke jaringan lainnya. Mereka menentukan jalur terbaik untuk mencapai tujuan berdasarkan informasi dalam header paket IP.
    b. Router juga dapat mengambil keputusan untuk mengalihkan paket ke jaringan lain atau mengirimkannya langsung ke tujuan, tergantung pada topologi jaringan dan tabel routing mereka.

5. Penanganan Kesalahan:
    a. Meskipun IP adalah protokol yang bersifat best-effort, artinya tidak menjamin pengiriman yang andal seperti TCP, namun IP memiliki beberapa mekanisme untuk mengatasi kesalahan.
    b. Ketika paket mengalami masalah, seperti hilang atau rusak dalam perjalanan, kadang-kadang router atau perangkat lain akan mengirimkan pesan ICMP (*Internet Control Message Protocol*) yang memberi tahu perangkat pengirim tentang masalah tersebut.

6. Penerimaan Data:
    a. Setelah mencapai tujuan, paket IP diuraikan, dan data yang ada di dalamnya dapat diakses oleh perangkat penerima.
    b. Data ini dapat digunakan oleh aplikasi atau protokol tingkat lebih tinggi untuk memproses informasi atau tindakan yang sesuai.

7. Penutupan Koneksi (Opsional):
    a. IP adalah protokol tanpa koneksi, yang berarti tidak ada perlu untuk inisiasi atau penutupan koneksi seperti yang dilakukan oleh protokol TCP.
    b. Beberapa protokol tingkat lebih tinggi, seperti TCP, mungkin memerlukan inisiasi dan penutupan koneksi terpisah sesuai kebutuhan aplikasi.

Dengan cara kerja ini, Internet Protocol (IP) memungkinkan perangkat di seluruh dunia untuk berkomunikasi satu sama lain melalui jaringan global yang kompleks. Router, tabel routing, dan alamat IP berperan penting dalam menjaga lalu lintas data bergerak secara efisien melalui internet, sehingga memungkinkan komunikasi global yang andal.

Internet Control Message Protocol (ICMP)

Internet Control Message Protocol (ICMP) adalah protokol yang berada di lapisan jaringan dalam model referensi OSI. ICMP digunakan untuk mengirim pesan kontrol dan pesan kesalahan dalam jaringan IP. Ini tidak digunakan untuk mengirim data pengguna, tetapi untuk mengelola jaringan dan memberikan informasi tentang kondisi jaringan. Berikut adalah cara kerja ICMP dengan jelas: (Logistics 2008; Davie 2012)

1. Generasi Pesan ICMP:
    a. Ketika ada situasi yang memerlukan pesan kesalahan atau pesan kontrol dalam jaringan IP, perangkat atau router yang terlibat akan menghasilkan pesan ICMP.
    b. Pesan ICMP ini biasanya mengandung informasi tentang jenis kesalahan atau peristiwa yang terjadi, seperti timeout dalam pengiriman paket atau host yang tidak dapat dijangkau.

2. Pengemasan Pesan ICMP:
    a. Pesan ICMP dikemas dalam paket IP khusus. Paket IP ini berisi header IP standar, dan pesan ICMP ditempatkan dalam payload (data) paket tersebut.
    b. Pesan ICMP memiliki jenis dan kode yang berbeda untuk mengidentifikasi jenis pesan dan detailnya.

3. Pengiriman Pesan ICMP:
    a. Setelah pesan ICMP dikemas, perangkat atau router yang menghasilkannya mengirimkannya ke alamat IP yang relevan.
    b. Ini dapat menjadi host atau router yang perlu diberi tahu tentang masalah atau situasi yang terjadi dalam jaringan.

4. Penerimaan Pesan ICMP:
    a. Perangkat atau router yang menerima pesan ICMP akan menguraikan pesan tersebut dan mengambil tindakan yang sesuai berdasarkan isi pesan.
    b. Pesan ICMP umumnya digunakan untuk tujuan berikut:
        1) *Ping*: Pesan ICMP *Echo Request* dan *Echo Reply* digunakan untuk menguji apakah perangkat atau host dapat dijangkau dalam jaringan. Ini adalah dasar dari perintah ping.
        2) *Time Exceeded*: Pesan ICMP ini dikirim ketika batas waktu (timeout) tercapai saat mencoba mengirimkan paket ke tujuan. Ini digunakan untuk mengukur latensi dalam jaringan.
        3) *Destination Unreachable*: Pesan ICMP ini dikirim ketika tujuan tidak dapat dijangkau atau tidak dapat mencapai tujuan. Ini bisa karena berbagai alasan, seperti alamat IP tujuan tidak valid atau host yang tidak aktif.

5. Tindakan Berdasarkan Pesan ICMP:
    a. Ketika pesan ICMP diterima, tindakan yang diambil oleh perangkat atau router bergantung pada jenis pesan dan konteksnya.
    b. Misalnya, jika pesan ICMP Time Exceeded diterima, router mungkin akan mengirim pesan ICMP kembali kepada pengirim untuk memberi tahu bahwa batas waktu telah tercapai.
    c. Jika pesan ICMP Destination Unreachable diterima, perangkat pengirim dapat mengambil tindakan untuk mencoba rute yang berbeda atau memberi tahu administrator jaringan tentang masalah tersebut.

ICMP adalah bagian integral dari operasi jaringan IP dan memainkan peran penting dalam memungkinkan perangkat dan router untuk berkomunikasi dan mengelola jaringan dengan efisien. Hal ini juga penting dalam pengujian jaringan dan pemecahan masalah, karena pesan ICMP dapat memberikan wawasan tentang kondisi jaringan dan masalah yang mungkin terjadi.

IP VS ICMP

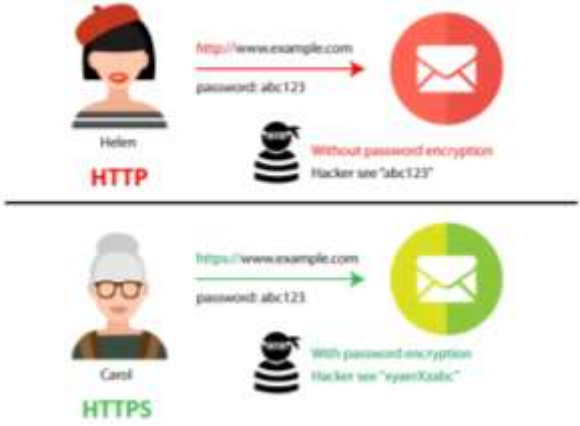
Mari kita gunakan analogi sederhana untuk memberikan gambaran perbedaan antara *Internet Protocol* (IP) dan *Internet Control Message Protocol* (ICMP). (Logistics 2008; Davie 2012)

1. IP (Internet Protocol):
   Bayangkan IP sebagai alamat fisik rumah Anda dalam sebuah kota. Setiap rumah memiliki alamat unik yang memungkinkan surat atau paket dikirimkan ke tujuan yang tepat. Ketika seseorang ingin mengirimkan surat atau paket ke rumah Anda, mereka menuliskan alamat fisik Anda pada surat atau paket tersebut. Alamat fisik ini adalah apa yang memungkinkan paket atau surat mencapai rumah Anda dengan benar.

2. ICMP (Internet Control Message Protocol):
   Sekarang, bayangkan ICMP sebagai jenis pesan yang bisa Anda kirim kepada tetangga Anda jika terjadi masalah dengan surat atau paket yang dikirim kepada Anda. Misalnya, jika ada surat yang hilang atau paket yang tidak sampai ke rumah Anda, Anda dapat mengirimkan pesan kepada tetangga Anda untuk memberi tahu mereka tentang masalah ini. Pesan ICMP ini adalah cara Anda berkomunikasi tentang masalah dalam pengiriman.

Dalam analogi ini, IP adalah alamat yang digunakan untuk mengarahkan surat atau paket ke tujuan yang benar, sedangkan ICMP adalah cara untuk memberi tahu tentang masalah atau kesalahan yang mungkin terjadi dalam pengiriman surat atau paket tersebut. IP berfokus pada pengiriman data, sementara ICMP berfokus pada pesan kontrol dan kesalahan dalam jaringan.

5.6 HTTP VS HTTPS



Gambar 5.6. HTTP vs HTTPS
Sumber : https://www.edhotels.com/

Hypertext Transfer Protocol (HTTP)

Hypertext Transfer Protocol (HTTP) adalah protokol aplikasi yang digunakan untuk mengirimkan dan menerima data di web. Ini adalah protokol yang digunakan oleh browser web Anda untuk mengunduh halaman web dari server. Berikut adalah cara kerja protokol HTTP dengan jelas: (Logistics 2008; Davie 2012)

1. Permintaan HTTP (HTTP Request):
    a. Proses dimulai ketika Anda memasukkan URL (*Uniform Resource Locator*) ke browser web Anda atau mengklik tautan di halaman web. URL ini merujuk ke alamat server web yang ingin Anda kunjungi.
    b. Browser Anda kemudian membuat permintaan HTTP ke server web dengan mengirimkan HTTP request. Request ini berisi berbagai informasi, termasuk metode (GET, POST, PUT, dll.) dan header yang berisi informasi tambahan seperti jenis browser yang digunakan.

2. Penerimaan Permintaan (*Request Handling*):
    a. Server web yang menerima permintaan HTTP kemudian memproses permintaan tersebut. Server ini mungkin menjalankan kode server, mengambil data dari basis data, atau melakukan tindakan lain yang sesuai dengan permintaan tersebut.
    b. Setelah pemrosesan selesai, server web menghasilkan sebuah respons HTTP.

3. Respon HTTP (HTTP Response):
    a. Respon HTTP adalah balasan dari server ke permintaan yang dibuat oleh browser. Respon ini berisi status kode HTTP yang mengindikasikan apakah permintaan berhasil, berhasil dengan masalah, atau gagal.

b. Respon HTTP juga berisi header yang berisi informasi tentang respon, seperti jenis konten (misalnya, teks, gambar, atau HTML), tanggal pembuatan, dan lain-lain.
c. Yang paling penting, respon HTTP juga berisi konten aktual yang diminta oleh browser, seperti halaman web atau data lain yang diperlukan.

4. Pengolahan Respon (*Response Processing*):
   a. Setelah menerima respon HTTP, browser web Anda menguraikan kontennya sesuai dengan jenis konten yang dinyatakan dalam header respons.
   b. Misalnya, jika kontennya adalah halaman web HTML, browser akan memahami dan menampilkan halaman tersebut dalam tampilan yang dapat Anda lihat.
   c. Jika kontennya adalah gambar, browser akan menampilkan gambar tersebut.

5. Interaksi Lanjutan (Optional):
   a. Setelah menampilkan halaman web, Anda dapat berinteraksi lebih lanjut dengan halaman tersebut, seperti mengklik tautan, mengirim formulir, atau menjalankan skrip JavaScript. Setiap interaksi ini menghasilkan permintaan HTTP tambahan ke server web.

6. Penutup Koneksi (Optional):
   a. Setelah semua permintaan dan respon HTTP selesai, koneksi HTTP antara browser dan server dapat ditutup.
   b. Di beberapa kasus, koneksi dapat dipertahankan agar permintaan berikutnya dapat dijalankan dengan lebih cepat tanpa memulai koneksi yang baru.

HTTP adalah dasar dari seluruh web dan digunakan dalam hampir setiap interaksi Anda dengan situs web. Ini adalah cara browser mengakses, mengunduh, dan menampilkan halaman web serta berbagai jenis konten lainnya. Semua ini terjadi dalam latar belakang secara cepat dan transparan, memungkinkan pengguna menjelajahi web dengan mudah.

Hypertext Transfer Protocol Secure (HTTPS)

Hypertext Transfer Protocol Secure (HTTPS) adalah versi aman dari protokol HTTP yang digunakan untuk mengamankan komunikasi antara perangkat pengguna (seperti browser web) dan server web. HTTPS menggunakan enkripsi data untuk melindungi informasi yang dikirim antara perangkat dan server dari akses yang tidak sah atau penyadapan. Berikut adalah cara kerja protokol HTTPS secara jelas: (Logistics 2008; Davie 2012)

1. Permintaan HTTPS (HTTPS Request):
    a. Proses dimulai ketika pengguna memasukkan URL (*Uniform Resource Locator*) yang diawali dengan "https://" ke browser web atau mengklik tautan yang menggunakan HTTPS.
    b. Browser kemudian membuat permintaan HTTPS ke server web dengan mengirimkan HTTPS request. Permintaan ini serupa dengan permintaan HTTP, tetapi menggunakan protokol HTTPS yang aman.

2. Tentukan Identitas Server (*Server Authentication*):
    a. Ketika browser menerima respons dari server, salah satu langkah pertama adalah memverifikasi identitas server. Ini adalah tahap penting untuk memastikan bahwa pengguna berkomunikasi dengan server yang sah dan bukan dengan server palsu.
    b. Server web yang valid harus memiliki sertifikat digital yang dikeluarkan oleh otoritas sertifikat tepercaya

(*Certificate Authority*, CA). Sertifikat ini berisi informasi tentang identitas server dan kunci enkripsi publik yang akan digunakan untuk melindungi data selama transmisi.

3. Tukar Kunci Enkripsi (*Key Exchange*):
   a. Setelah verifikasi identitas server, browser dan server web akan melakukan pertukaran kunci enkripsi.
   b. Kunci enkripsi ini digunakan untuk mengamankan data yang akan dikirim selama sesi HTTPS. Biasanya, metode enkripsi yang digunakan adalah Transport Layer Security (TLS) atau SSL (*Secure Sockets Layer*).
   c. Selama pertukaran kunci enkripsi, kunci enkripsi publik yang disertakan dalam sertifikat server digunakan untuk mengenkripsi kunci enkripsi simetris yang akan digunakan untuk mengamankan data selama komunikasi.

4. Enkripsi Data (*Data Encryption*):
   a. Setelah kunci enkripsi disepakati, semua data yang dikirimkan antara browser dan server akan dienkripsi menggunakan kunci enkripsi simetris.
   b. Enkripsi ini membuat data tidak dapat dibaca oleh pihak yang tidak memiliki kunci enkripsi yang sesuai, sehingga melindungi informasi pribadi dan sensitif pengguna dari penyadapan selama transmisi.

5. Pengiriman Data Terenkripsi (*Encrypted Data Transmission*):
   a. Selama sesi HTTPS, semua data yang dikirim antara browser dan server, termasuk halaman web, gambar, atau informasi formulir yang dimasukkan oleh pengguna, dikirim dalam bentuk terenkripsi.

b. Data ini hanya dapat didekripsi oleh server yang memiliki kunci enkripsi yang sesuai, sehingga menjaga kerahasiaan dan integritas data selama pengiriman.

6. Penutup Koneksi (Optional):
   a. Setelah semua permintaan dan respons HTTPS selesai, koneksi HTTPS dapat ditutup. Beberapa koneksi HTTPS mungkin juga dipertahankan untuk permintaan berikutnya, tergantung pada konfigurasi server dan browser.

HTTPS memastikan bahwa komunikasi antara perangkat pengguna dan server web dilindungi dan aman dari ancaman keamanan, seperti penyadapan data atau serangan man-in-the-middle. Ini adalah protokol yang sangat penting dalam menjaga privasi dan keamanan dalam beraktivitas di web, terutama ketika mengakses situs web yang mengharuskan Anda memasukkan informasi pribadi atau sensitif seperti informasi kartu kredit atau kata sandi.

HTTP VS HTTPS

Mari kita gunakan analogi pintu masuk ke sebuah bank untuk memberikan gambaran perbedaan antara HTTP dan HTTPS: (Logistics 2008; Davie 2012)

1. HTTP (*Hypertext Transfer Protocol*):
   Bayangkan Anda pergi ke sebuah bank yang memiliki pintu masuk terbuka tanpa pengaman. Ketika Anda masuk ke dalam bank, siapa pun di luar bank dapat dengan mudah melihat dan mendengar semua transaksi yang sedang berlangsung di dalam. Informasi pribadi seperti nomor rekening bank dan saldo Anda tersedia untuk siapa saja yang tertarik. Ini adalah situasi yang sangat tidak aman, dan siapa pun bisa mencuri atau memanipulasi data Anda dengan mudah.

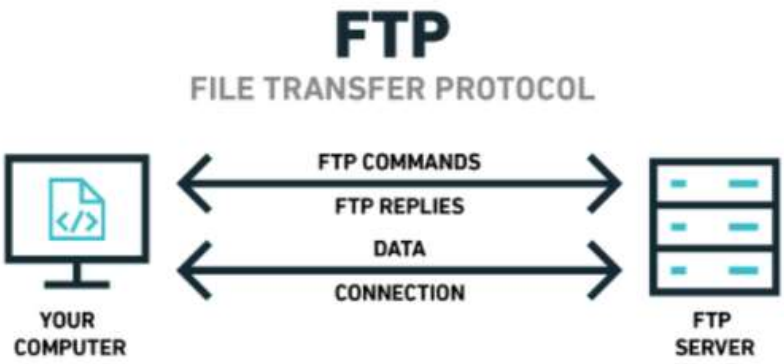
Dalam konteks web, HTTP mirip dengan pintu masuk terbuka ini. Data yang Anda kirimkan antara browser dan server tidak dienkripsi, sehingga mudah bagi pihak yang tidak sah untuk mengakses dan memanipulasi informasi tersebut. Ini sangat tidak aman, terutama jika Anda berinteraksi dengan situs web yang mengharuskan Anda memasukkan informasi pribadi.

2. HTTPS (*Hypertext Transfer Protocol Secure*):
   Sekarang, bayangkan Anda pergi ke bank yang memiliki pintu masuk yang sangat aman. Pintu masuk ini dilengkapi dengan sensor sidik jari, kamera pengawas, dan sistem pengamanan tingkat tinggi. Ketika Anda masuk ke dalam bank, Anda tahu bahwa transaksi Anda akan aman dan informasi pribadi Anda akan terlindungi dengan baik. Bahkan jika ada orang yang mencoba mendekati pintu masuk bank, mereka tidak dapat mengakses area dalam bank tanpa izin.
   Dalam konteks web, HTTPS mirip dengan pintu masuk yang sangat aman ini. Saat Anda mengakses situs web dengan protokol HTTPS, data yang Anda kirimkan antara browser dan server dienkripsi dengan kuat. Ini berarti bahwa bahkan jika ada pihak yang mencoba memata-matai komunikasi Anda, mereka hanya akan melihat data terenkripsi yang tidak dapat dibaca tanpa kunci enkripsi yang benar. Ini memberikan tingkat keamanan yang tinggi dan melindungi informasi sensitif Anda saat Anda berinteraksi dengan situs web yang aman, seperti situs perbankan online atau toko online.

Dalam kesimpulan, HTTPS adalah seperti pintu masuk bank yang aman, sementara HTTP adalah seperti pintu masuk terbuka. HTTPS menggunakan enkripsi untuk melindungi data Anda dan menjaga privasi serta keamanan informasi Anda saat Anda berkomunikasi dengan situs web. Itulah mengapa penting untuk selalu mencari tanda "https://" dan ikon gembok hijau dalam

browser Anda saat berinteraksi dengan situs web yang memerlukan keamanan.

5.7 File Transfer Protocol (FTP)



Gambar 5.7. File Transfer Protocol
Sumber : https://cyberhoot.com/

File Transfer Protocol (FTP) adalah protokol yang digunakan untuk mentransfer file antara komputer atau server melalui jaringan, seperti internet. FTP memungkinkan pengguna untuk mengunggah (*upload*) dan mengunduh (*download*) file dari server ke komputer atau sebaliknya. Berikut adalah cara kerja protokol FTP secara jelas: (Logistics 2008; Davie 2012)

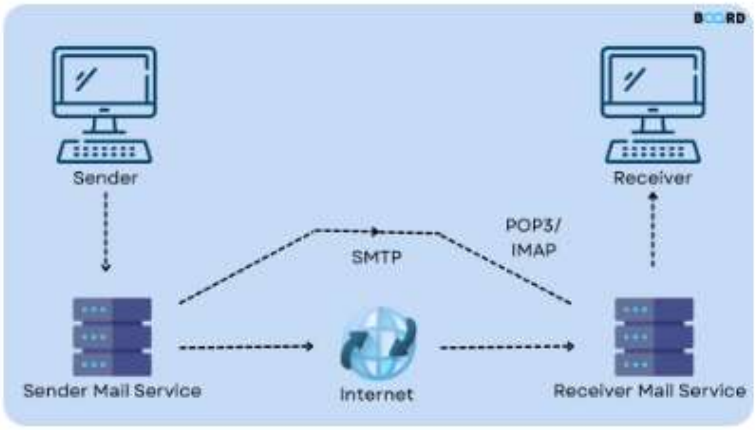
1. Koneksi ke Server FTP:
    a. Proses dimulai dengan pengguna yang menggunakan perangkat lunak FTP (biasanya disebut klien FTP) untuk membuat koneksi ke server FTP yang diinginkan. Pengguna harus memasukkan alamat IP atau nama domain server FTP, serta nama pengguna dan kata sandi yang valid untuk mengautentikasi diri pada server.

2. Autentikasi Pengguna:
    a. Setelah koneksi berhasil dibuat, server FTP memeriksa kredensial yang diberikan oleh pengguna untuk memastikan bahwa pengguna memiliki izin untuk mengakses server.
    b. Jika autentikasi berhasil, pengguna diizinkan untuk menjelajah dan mentransfer file di server sesuai dengan izin yang diberikan.
3. Navigasi Direktori:
    a. Setelah terautentikasi, pengguna dapat menjelajahi struktur direktori pada server FTP. Ini dilakukan dengan perintah-perintah seperti "CD" (*change directory*) untuk berpindah direktori atau "LS" (list) untuk melihat daftar file dan direktori yang tersedia.
4. Operasi Transfer File:
    a. Untuk mengunggah file dari komputer pengguna ke server, pengguna dapat menggunakan perintah "PUT" atau "UPLOAD". Mereka harus menentukan nama file sumber dan tujuan serta direktori yang sesuai di server.
    b. Untuk mengunduh file dari server ke komputer pengguna, perintah "GET" atau "DOWNLOAD" digunakan dengan menyertakan nama file sumber dan tujuan di komputer pengguna.
5. Penggunaan Mode Aktif atau Pasif (Optional):
    a. FTP mendukung dua mode koneksi: mode aktif dan mode pasif. Mode aktif adalah konfigurasi standar, di mana server membuka koneksi kembali ke pengguna untuk mentransfer data. Mode pasif memungkinkan pengguna untuk membuka koneksi ke server untuk menghindari masalah firewall yang mungkin ada di antara koneksi.

6. Penutupan Koneksi:
    a. Setelah operasi transfer file selesai, pengguna dapat memutuskan koneksi ke server FTP atau tetap terhubung untuk menjalankan operasi transfer tambahan.
    b. Ada juga perintah "QUIT" yang dapat digunakan untuk mengakhiri sesi FTP dan menutup koneksi dengan server.

FTP adalah protokol yang sering digunakan untuk mengelola dan mentransfer file di berbagai jenis server, termasuk server web dan server file. Ini adalah alat yang berguna untuk mengirim dan menerima file besar atau untuk mengelola situs web dan server jarak jauh. Meskipun ada beberapa masalah keamanan terkait dengan FTP, protokol ini tetap digunakan secara luas karena kemudahannya dalam mengelola file. Sebagai alternatif, FTPS (FTP Secure) dan SFTP (SSH *File Transfer Protocol*) adalah versi aman dari FTP yang menambahkan lapisan keamanan tambahan.

5.8 Simple Mail Transfer Protokol (SMTP)



Gambar 5.8. Simple Mail Transfer Protokol
Sumber : https://www.boardinfinity.com/

Simple Mail Transfer Protocol (SMTP) adalah protokol yang digunakan untuk mengirim email melalui jaringan komputer. SMTP adalah bagian integral dari proses pengiriman email, dan berikut adalah cara kerjanya secara jelas: (Logistics 2008; Davie 2012)

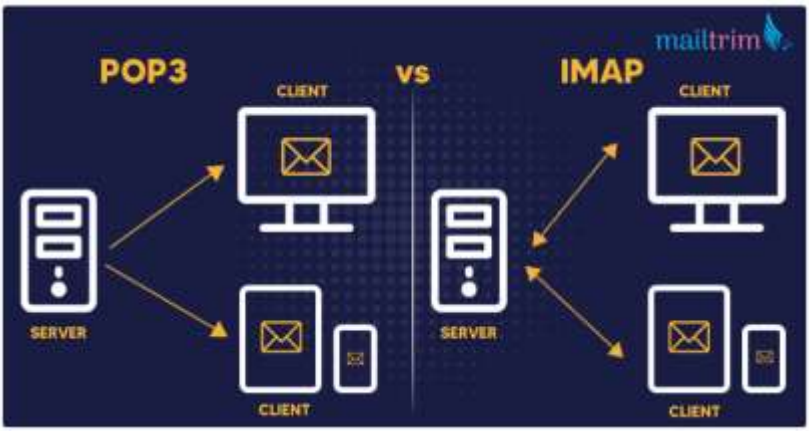
1. **Inisiasi Koneksi**:
    a. Proses dimulai ketika pengirim email (klien SMTP) ingin mengirim pesan email. Klien SMTP membuat koneksi ke server SMTP yang sesuai dengan alamat domain tujuan email (misalnya, smtp.example.com).
    b. Klien SMTP mengidentifikasi dirinya kepada server SMTP menggunakan nama pengguna dan kata sandi, jika diperlukan oleh server.
2. **Pengaturan Alamat Tujuan**:
    a. Setelah koneksi didirikan, klien SMTP menentukan alamat email tujuan (alamat penerima) dan alamat email pengirim (alamat pengirim) untuk pesan yang akan dikirim. Alamat-alamat ini termasuk dalam header pesan email.
3. **Penyusunan Pesan Email**:
    a. Klien SMTP membuat pesan email yang akan dikirim. Pesan email terdiri dari beberapa komponen, termasuk subjek, isi pesan, lampiran (jika ada), dan daftar penerima lainnya. Pesan ini dibentuk dalam format yang sesuai, seperti format teks biasa atau HTML.
4. **Transmisi Pesan ke Server SMTP**:
    a. Klien SMTP mengirim pesan email ke server SMTP menggunakan perintah-perintah yang didefinisikan dalam protokol SMTP.
    b. Server SMTP menerima pesan dan memprosesnya sesuai dengan aturan yang berlaku.

5. **Pengiriman Pesan antara Server SMTP**:
    a. Jika pesan dikirim ke alamat email dalam domain yang sama dengan server SMTP pengirim, server SMTP akan mengirimkan pesan langsung ke server SMTP tujuan. Ini disebut pengiriman lokal.
    b. Jika pesan harus dikirim ke alamat email di domain yang berbeda, server SMTP pengirim akan mengirimkan pesan ke server SMTP tujuan menggunakan protokol SMTP. Pesan ini akan melalui beberapa server SMTP antara jika diperlukan hingga mencapai server SMTP tujuan.
6. **Penyimpanan Pesan di Server Tujuan**:
    a. Setelah pesan mencapai server SMTP tujuan, pesan akan disimpan dalam kotak surat (mailbox) yang sesuai dengan alamat penerima.
    b. Penerima dapat mengakses pesan ini dengan menggunakan protokol seperti *Internet Message Access Protocol* (IMAP) atau *Post Office Protocol* (POP).
7. **Notifikasi Pengiriman (Optional)**:
    a. Server SMTP pengirim dapat mengirim notifikasi pengiriman (Delivery Status Notification atau DSN) kepada pengirim jika konfigurasi server mendukung fitur ini. DSN memberi tahu pengirim apakah pesan telah berhasil atau gagal dikirim.
8. **Penutupan Koneksi**:
    a. Setelah semua pesan dikirim, klien SMTP dapat menutup koneksi dengan server SMTP, mengakhiri sesi SMTP.

SMTP adalah protokol yang bekerja di latar belakang untuk mengirim email dengan cepat dan efisien di seluruh dunia. Ini merupakan dasar dari sistem email modern dan memungkinkan pengguna untuk berkomunikasi melalui email dengan mudah. Dalam proses pengiriman email yang lebih kompleks, seperti

mengatasi antispam dan otentikasi pengirim, SMTP juga berperan penting.

5.9 POP3 VS IMAP



Gambar 5.9. POP3 vs IMAP
Sumber : https://www.mailtrim.com/

***Post Office Protocol* 3 (POP3)**

Post Office Protocol 3 (POP3) adalah protokol yang digunakan untuk mengambil email dari server email. POP3 memungkinkan pengguna untuk mengunduh pesan email dari server ke perangkat mereka. Berikut adalah cara kerja protokol POP3 dengan jelas: (Logistics 2008; Davie 2012)

1. **Inisiasi Koneksi**:
    a. Proses dimulai ketika pengguna membuka aplikasi email mereka (klien POP3) dan ingin mengambil pesan email dari server email mereka.
    b. Klien POP3 membuat koneksi ke server email yang sesuai menggunakan alamat server yang telah dikonfigurasi sebelumnya.

2. **Autentikasi Pengguna**:
    a. Setelah koneksi berhasil dibuat, klien POP3 mengidentifikasi dirinya kepada server email dengan menggunakan nama pengguna dan kata sandi yang valid.
    b. Autentikasi ini memungkinkan server untuk memverifikasi identitas pengguna dan memberikan izin untuk mengakses email yang tersimpan di server.
3. **Pemeriksaan Status Email**:
    a. Setelah berhasil diotentikasi, klien POP3 dapat mengirim perintah kepada server POP3 untuk memeriksa status email.
    b. Server akan memberikan informasi tentang jumlah pesan yang ada di kotak surat pengguna, serta ukuran total dari semua pesan tersebut.
4. **Unduh Pesan Email**:
    a. Klien POP3 dapat mengunduh pesan email yang telah diterima dari server ke perangkat mereka. Ini dilakukan dengan perintah "RETR" (*Retrieve*).
    b. Pengguna dapat memilih untuk mengunduh seluruh pesan atau pesan tertentu dengan menentukan nomor pesan yang ingin diambil.
5. **Penyimpanan Pesan di Perangkat**:
    a. Setelah diunduh, pesan email akan disimpan di perangkat pengguna, dan biasanya akan diatur dalam aplikasi email atau klien.
    b. Pengguna dapat membaca, menyimpan, atau menghapus pesan email sesuai kebutuhan mereka.
6. **Penandai Pesan Sebagai Sudah Diambil (Optional)**:
    a. Setelah pesan email diunduh, klien POP3 dapat mengirim perintah kepada server POP3 untuk menandai pesan-pesan tersebut sebagai "sudah diambil."

b. Ini akan menginformasikan server bahwa pengguna telah mengambil pesan tersebut dan dapat menghapusnya dari server, jika pengaturan klien POP3 mengizinkannya.

7. **Penutupan Koneksi**:
   a. Setelah pengguna selesai mengambil pesan email, klien POP3 dapat menutup koneksi dengan server POP3 untuk mengakhiri sesi.
8. **Opsi untuk Menghapus dari Server (Optional)**:
   a. Pengguna dapat mengkonfigurasi klien POP3 untuk menghapus pesan dari server setelah diunduh. Ini berarti pesan akan dihapus dari server email, dan hanya tersimpan di perangkat pengguna.
   b. Namun, ada juga opsi untuk menyimpan pesan di server jika pengguna ingin mengakses email mereka dari beberapa perangkat.

POP3 adalah protokol yang umum digunakan untuk mengambil pesan email dari server. Ini cocok untuk penggunaan di mana email diunduh ke satu perangkat, seperti komputer desktop. Namun, POP3 memiliki batasan dalam hal sinkronisasi email di beberapa perangkat, dan pesan email biasanya dihapus dari server setelah diunduh, kecuali jika konfigurasi pengguna mengizinkannya.

Internet Message Access Protocol (IMAP)

Internet Message Access Protocol (IMAP) adalah protokol yang digunakan untuk mengakses dan mengelola email yang disimpan di server email dari berbagai perangkat. IMAP memungkinkan pengguna untuk menjaga email mereka, folder, dan status email yang konsisten di berbagai perangkat. Berikut adalah cara kerja protokol IMAP dengan jelas: (Logistics 2008; Davie 2012)

1. **Inisiasi Koneksi**:
    a. Proses dimulai ketika pengguna membuka aplikasi email mereka (klien IMAP) dan ingin mengakses email dari server email mereka.
    b. Klien IMAP membuat koneksi ke server email yang sesuai menggunakan alamat server dan port yang telah dikonfigurasi sebelumnya.
2. **Autentikasi Pengguna**:
    a. Setelah koneksi berhasil dibuat, klien IMAP mengidentifikasi dirinya kepada server email dengan menggunakan nama pengguna dan kata sandi yang valid.
    b. Autentikasi ini memungkinkan server untuk memverifikasi identitas pengguna dan memberikan izin untuk mengakses email yang tersimpan di server.
3. **Synchronization (Sinkronisasi)**:
    a. Salah satu fitur utama IMAP adalah kemampuannya untuk menjaga email dan folder yang konsisten di semua perangkat. Ini berarti bahwa email yang dibaca, dihapus, atau dipindahkan di satu perangkat akan tercermin secara otomatis di semua perangkat lainnya yang terhubung ke akun IMAP yang sama.
    b. Klien IMAP akan mengambil daftar folder dan status email dari server, termasuk baca/belum dibaca, bintang, dan lainnya, dan menyesuaikannya dengan tampilan klien.
4. **Akses Email**:
    a. Setelah sinkronisasi awal, pengguna dapat mengakses email dan folder mereka dengan cara yang sama seperti mereka melakukannya di aplikasi email. Mereka dapat membaca pesan, mengirim balasan, menyusun pesan baru, menghapus pesan, dan lainnya.
    b. Semua tindakan ini diteruskan ke server email melalui koneksi IMAP.

5. **Penyimpanan di Server**:
    a. Email tetap disimpan di server email bahkan setelah diakses oleh pengguna. Ini memungkinkan pengguna untuk mengakses email mereka dari banyak perangkat dengan konsistensi data.
    b. Pengguna dapat membuat folder baru di server untuk mengatur email mereka dan bahkan dapat memindahkan email antara folder sesuai kebutuhan.
6. **Penutupan Koneksi**:
    a. Setelah pengguna selesai mengakses email mereka, klien IMAP dapat menutup koneksi dengan server IMAP untuk mengakhiri sesi.
7. **Opsi Sinkronisasi Otomatis (Optional)**:
    a. Banyak klien IMAP mendukung sinkronisasi otomatis, yang berarti mereka akan secara berkala memeriksa server email untuk email baru dan memperbarui tampilan email secara otomatis tanpa perlu tindakan pengguna.

IMAP adalah protokol yang sangat berguna bagi mereka yang ingin mengakses email mereka dari beberapa perangkat atau ingin menjaga konsistensi email dan folder di berbagai tempat. Ini memungkinkan akses email yang fleksibel dan memudahkan manajemen email di berbagai perangkat dengan aman.

POP3 VS IMAP

Mari kita gunakan analogi kotak surat untuk memberikan gambaran perbedaan antara POP3 (*Post Office Protocol* 3) dan IMAP (*Internet Message Access Protocol*): (Logistics 2008; Davie 2012)

POP3 (*Post Office Protocol* 3): Bayangkan Anda memiliki kotak surat di kantor pos lokal. Setiap kali ada surat baru yang masuk ke alamat Anda, kantor pos mengirimkan surat tersebut ke

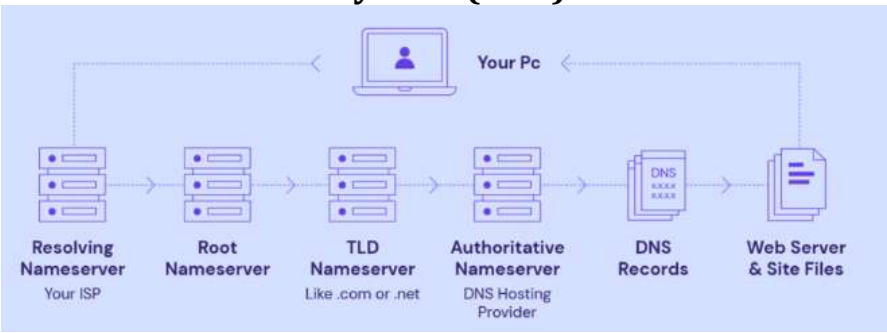
kotak surat Anda. Ketika Anda pergi ke kantor pos, Anda mengambil semua surat dari kotak surat Anda dan membawanya pulang. Setelah Anda mengambil surat-surat tersebut, mereka tidak lagi ada di kotak surat di kantor pos. Anda memiliki salinan fisik dari surat-surat tersebut di rumah Anda, dan jika Anda ingin mengakses surat-surat tersebut dari tempat lain, Anda harus membawanya.

Dalam konteks email, POP3 bekerja mirip. Email dikirim ke server email Anda, dan ketika Anda memeriksa email, email tersebut diunduh ke perangkat Anda. Email ini kemudian tidak lagi ada di server email. Jadi, email berada di satu perangkat saja (biasanya komputer Anda), dan jika Anda ingin mengaksesnya dari perangkat lain, Anda tidak akan menemukannya di sana.

IMAP (*Internet Message Access Protocol*): Sekarang, bayangkan Anda memiliki akses ke kotak surat di kantor pos yang bersifat bersama. Setiap kali ada surat baru yang masuk ke alamat Anda, itu tetap ada di kotak surat di kantor pos. Anda dapat membawa satu salinan dari setiap surat yang ingin Anda baca, tetapi surat itu tetap ada di kotak surat di kantor pos. Jadi, jika Anda pergi ke kantor pos dari komputer atau perangkat lain, Anda masih dapat melihat dan mengelola surat-surat tersebut.

Dalam konteks email, IMAP bekerja mirip. Email tetap di server email bahkan setelah Anda membaca atau mengunduhnya ke perangkat Anda. Anda memiliki akses ke email dari berbagai perangkat, dan perubahan yang Anda lakukan (membaca, menghapus, memindahkan ke folder) tercermin di semua perangkat yang terhubung ke akun IMAP yang sama. Ini memungkinkan Anda untuk menjaga konsistensi email Anda di berbagai perangkat dan mengakses email Anda dari mana saja.

5.10 Domain Name System (DNS)



Gambar 5.10. Domain Name System
Sumber : https://www.hostinger.com/

Domain Name System (DNS) adalah sistem yang digunakan di internet untuk menghubungkan alamat IP (*Internet Protocol*) numerik dengan nama domain yang lebih mudah diingat. DNS berfungsi sebagai buku telepon internet yang menerjemahkan nama domain seperti www.example.com menjadi alamat IP seperti 192.0.2.1. Berikut adalah cara kerja protokol DNS dengan jelas: (Logistics 2008; Davie 2012)

1. **Permintaan DNS (DNS Query)**:
   a. Proses dimulai ketika seseorang memasukkan nama domain (seperti www.example.com) ke browser web mereka atau melakukan tindakan seperti mengklik tautan.
   b. Browser web atau perangkat yang memerlukan resolusi DNS membuat permintaan DNS ke server DNS. Permintaan ini berisi nama domain yang perlu diterjemahkan menjadi alamat IP.
2. **Pemeriksaan Cache Lokal (*Local Cache Check*)**:
   a. Sebelum melakukan permintaan ke server DNS eksternal, perangkat mungkin pertama-tama memeriksa cache DNS lokalnya. Cache DNS adalah daftar sementara yang berisi hasil resolusi DNS sebelumnya. Jika nama domain sudah

ada dalam cache dengan alamat IP yang sesuai, permintaan selesai dan tidak perlu menghubungi server DNS eksternal.

3. **Server DNS Rekursif (Recursive DNS Server)**:
   a. Jika data DNS tidak ada di cache lokal atau sudah kadaluwarsa, perangkat akan menghubungi server DNS rekursif. Server DNS rekursif adalah server DNS khusus yang bertanggung jawab untuk menemukan resolusi DNS yang akurat.
   b. Permintaan DNS dikirim ke server DNS rekursif, yang kemudian mulai mencari informasi DNS yang sesuai.
4. **Hierarki DNS (DNS Hierarchy)**:
   a. Server DNS rekursif pertama kali memeriksa zona tertentu dalam hierarki DNS, yang disebut zona akar (*root zone*). Zona akar ini berisi informasi tentang server DNS di seluruh dunia dan mengarahkan permintaan ke zona berikutnya dalam hierarki.
   b. Zona berikutnya adalah zona *top-level domain* (TLD), seperti .com, .org, .net, dll. Server DNS rekursif akan menghubungi server DNS TLD yang sesuai untuk nama domain yang dicari.
   c. Server DNS TLD kemudian mengarahkan permintaan ke server DNS yang mengelola domain spesifik, seperti example.com dalam contoh www.example.com.
5. **Resolusi DNS (DNS Resolution)**:
   a. Server DNS yang mengelola domain spesifik (misalnya, example.com) memiliki catatan DNS yang memetakan nama domain ke alamat IP yang sesuai. Server ini mengirimkan informasi ini kembali ke server DNS rekursif, yang kemudian mengirimkannya kembali ke perangkat pengguna.
   b. Perangkat pengguna sekarang memiliki alamat IP yang sesuai dengan nama domain yang dicari.

6. **Pengguna Akhir (End User)**:
    a. Perangkat pengguna menerima resolusi DNS dari server DNS rekursif dan menggunakan alamat IP yang ditemukan untuk menghubungi server web yang sesuai.
    b. Browser web perangkat mengirimkan permintaan ke alamat IP yang ditemukan, dan server web yang sesuai mengirimkan halaman web atau sumber daya yang diminta kembali ke perangkat pengguna.
7. **Penyimpanan Cache DNS Lokal (Local DNS Cache Storage)**:
    a. Hasil resolusi DNS yang berhasil akan disimpan dalam cache DNS lokal perangkat untuk digunakan di masa depan. Ini mengurangi waktu yang diperlukan untuk resolusi DNS jika permintaan serupa dibuat di kemudian hari.

DNS adalah komponen penting dalam operasi internet karena memungkinkan kita untuk menggunakan nama domain yang mudah diingat daripada harus mengingat alamat IP numerik yang panjang. Ini memfasilitasi penemuan sumber daya di internet dan memungkinkan pengguna untuk mengakses situs web dan layanan dengan mudah.

5.11 Simple Network Management Protocol (SNMP)

Gambar 5.11. *Simple Network Management Protocol* (SNMP)
Sumber : https://networkwalks.com/

Simple Network Management Protocol (SNMP) adalah protokol jaringan yang digunakan untuk mengelola dan mengawasi perangkat jaringan, seperti router, switch, server, dan printer, di dalam suatu jaringan. SNMP memungkinkan administrator jaringan untuk memantau kinerja perangkat, mendeteksi masalah, dan mengelola perangkat jaringan secara efisien. Berikut adalah cara kerja protokol SNMP secara jelas: (Logistics 2008; Davie 2012)

1. **Agent SNMP**:
   a. Proses dimulai dengan menginstal perangkat lunak atau perangkat keras yang disebut "SNMP agent" pada setiap perangkat jaringan yang ingin dimonitor atau dikelola. SNMP agent berfungsi sebagai antarmuka antara perangkat dan protokol SNMP.
2. **Manajer SNMP**:
   a. Di sisi lain, ada perangkat atau aplikasi yang disebut "SNMP manager" atau "NMS (*Network Management*

System)." SNMP manager ini digunakan oleh administrator jaringan untuk mengelola perangkat-perangkat yang terhubung dalam jaringan.

b. SNMP manager memiliki antarmuka pengguna yang memungkinkan administrator untuk memantau dan mengelola perangkat dengan menggunakan SNMP.

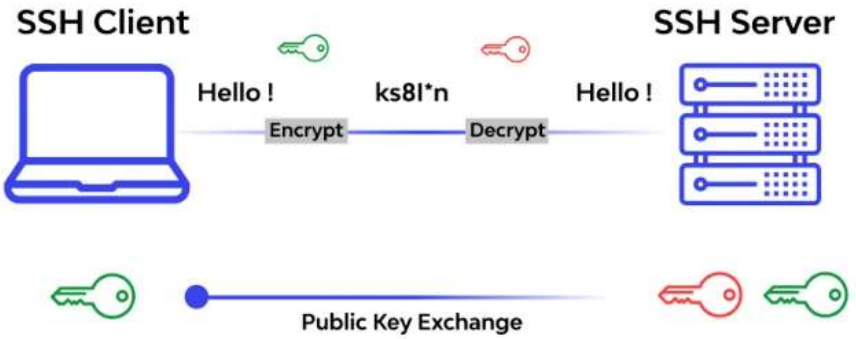
3. **Permintaan dan Respon SNMP**:
   a. SNMP manager mengirim permintaan (query) ke SNMP agent di perangkat jaringan yang ingin dimonitor atau dikelola. Permintaan ini dapat berupa permintaan informasi, seperti statistik kinerja atau penggunaan bandwidth, atau permintaan untuk mengubah konfigurasi perangkat.
   b. SNMP agent di perangkat jaringan menerima permintaan dan memprosesnya. Jika permintaan valid, SNMP agent akan merespons dengan data yang diminta atau mengambil tindakan yang sesuai, seperti mengubah konfigurasi.
4. **Struktur Obyek SNMP (SNMP *Object Structure*)**:
   a. SNMP menggunakan struktur data yang disebut "Management Information Base" (MIB) untuk mengorganisasi informasi yang dapat diakses melalui protokol ini. MIB adalah koleksi dari obyek-obyek yang mewakili informasi dan operasi pada perangkat jaringan.
   b. Setiap obyek dalam MIB memiliki alamat yang unik yang disebut "OID (*Object Identifier*)." Administrator mengidentifikasi obyek yang ingin diakses menggunakan OID.
5. **Protokol Transportasi**:
   a. SNMP dapat beroperasi di atas protokol transportasi seperti *User Datagram Protocol* (UDP) atau *Transmission Control Protocol* (TCP) sesuai dengan versi SNMP yang

digunakan. UDP umumnya digunakan dalam implementasi SNMP karena sifatnya yang ringan.

6. **Versi SNMP**:
   a. SNMP memiliki beberapa versi, termasuk SNMPv1, SNMPv2, dan SNMPv3. Setiap versi memiliki tingkat keamanan yang berbeda, dengan SNMPv3 yang paling aman karena mendukung enkripsi data dan autentikasi pengguna.
7. **Akses Hak (*Community String*)**:
   a. SNMP agent biasanya dilindungi dengan "*community string*," yang berfungsi sebagai kata sandi atau kunci akses. SNMP manager harus memberikan community string yang benar untuk mengakses informasi atau mengontrol perangkat.
8. **Pemantauan dan Pengelolaan Berkelanjutan**:
   a. SNMP manager dapat secara berkala mengirim permintaan ke SNMP agent untuk memantau kinerja dan status perangkat. Ini memungkinkan administrator untuk mendeteksi masalah atau anomali, dan jika diperlukan, untuk mengambil tindakan perbaikan.
9. **Notifikasi SNMP (SNMP Traps)**:
   a. Selain permintaan dari SNMP manager, SNMP agent juga dapat mengirimkan notifikasi yang disebut "SNMP traps" ke SNMP manager saat terjadi peristiwa penting atau masalah di perangkat jaringan. SNMP manager dapat mengambil tindakan berdasarkan notifikasi ini.

Dengan bantuan SNMP, administrator jaringan dapat mengawasi, mendiagnosa, dan mengelola perangkat jaringan dengan lebih efisien dan efektif. Hal ini sangat penting dalam menjaga kinerja jaringan yang optimal dan meminimalkan waktu henti yang tidak diinginkan.

5.12 Secure Shell (SSH)



Gambar 5.12. Secure Shell (SSH)
Sumber : https://course-net.com/

Secure Shell (SSH) adalah protokol dan aplikasi yang digunakan untuk mengamankan koneksi dan komunikasi antara dua perangkat jarak jauh melalui jaringan, seperti antara komputer klien dan server. SSH mengenkripsi data yang dikirimkan antara perangkat, sehingga melindungi informasi sensitif dari potensi pihak yang tidak sah. Berikut adalah cara kerja protokol SSH dengan jelas: (Logistics 2008; Davie 2012)

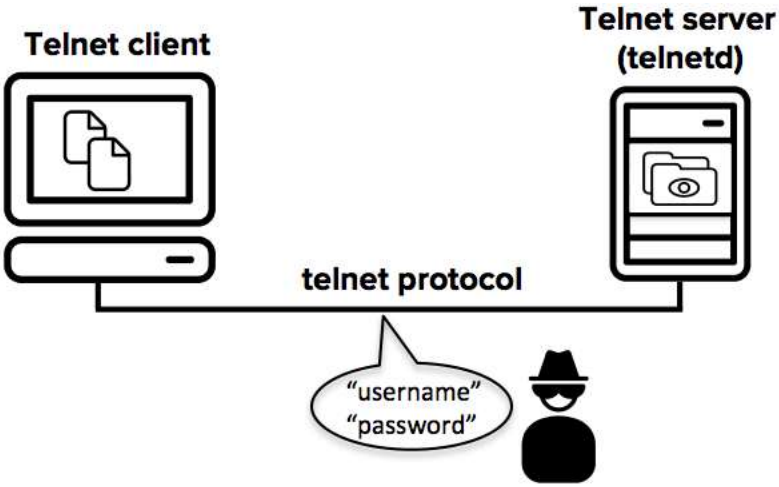
1. **Inisiasi Koneksi**:
    a. Proses dimulai ketika pengguna ingin terhubung ke perangkat jarak jauh melalui SSH. Pengguna biasanya menggunakan perangkat lunak SSH klien, seperti OpenSSH atau PuTTY, untuk menginisiasi koneksi.
    b. Pengguna harus menentukan alamat IP atau nama domain server yang akan diakses dan mengidentifikasi diri dengan nama pengguna dan kata sandi, atau metode otentikasi lainnya, seperti kunci SSH.

2. **Persetujuan Kunci Enkripsi**:
    a. Setelah koneksi didirikan, klien dan server SSH saling berkomunikasi untuk menegosiasikan metode enkripsi yang akan digunakan untuk mengamankan komunikasi. Ini melibatkan pertukaran informasi tentang kunci enkripsi yang akan digunakan selama sesi SSH.
    b. Salah satu metode enkripsi yang umum digunakan dalam SSH adalah algoritma RSA atau Ed25519.
3. **Otentikasi Pengguna**:
    a. Setelah kunci enkripsi disepakati, pengguna harus mengautentikasi diri kepada server SSH. Ini dapat dilakukan dengan memasukkan kata sandi pengguna atau menggunakan metode otentikasi lainnya seperti kunci SSH atau sertifikat X.509.
    b. Otentikasi ini memungkinkan server untuk memverifikasi identitas pengguna yang mencoba terhubung.
4. **Sesi SSH Dibuat**:
    a. Setelah pengguna berhasil diautentikasi, sesi SSH yang aman dibuat antara klien dan server. Selama sesi ini, semua data yang dikirimkan antara klien dan server dienkripsi menggunakan kunci yang telah disepakati.
    b. Sesi SSH ini memungkinkan pengguna untuk menjalankan perintah dan operasi di perangkat jarak jauh seolah-olah mereka berada di sana secara fisik.
5. **Perintah dan Komunikasi**:
    a. Selama sesi SSH, pengguna dapat menjalankan perintah di server jarak jauh. Perintah-perintah ini dikirim dari klien ke server dalam bentuk teks yang dienkripsi.
    b. Output dari perintah-perintah tersebut, jika ada, juga dikirimkan kembali ke klien dan didekripsi sehingga dapat ditampilkan kepada pengguna.

6. **Pemutusan Koneksi**:
    a. Sesuai kebutuhan, pengguna dapat mengakhiri sesi SSH dengan menutup koneksi atau menghentikan perangkat lunak klien SSH. Server juga dapat mengakhiri sesi jika diperlukan.
7. **Logging dan Auditing**:
    a. Aktivitas yang terjadi selama sesi SSH dapat dicatat (*logged*) untuk keperluan audit dan keamanan. Ini termasuk perintah yang dijalankan, data yang dikirim, dan detail otentikasi.

SSH adalah protokol yang sangat penting untuk keamanan jaringan dan pengelolaan sistem jarak jauh. Dengan mengenkripsi komunikasi antara perangkat, SSH melindungi data sensitif dan mencegah pihak yang tidak sah dari mengakses informasi atau meretas perangkat jarak jauh.

5.13 Telnet



Gambar 5.13. Telnet
Sumber : https://www.ssh.com/

Telnet adalah protokol yang digunakan untuk mengakses dan mengendalikan perangkat jarak jauh melalui jaringan, terutama melalui internet. Meskipun Telnet masih digunakan dalam beberapa konteks, seperti konfigurasi perangkat jaringan, perlu diingat bahwa Telnet tidak mengenkripsi data yang dikirimkan, sehingga data dapat terekspose pada pihak yang tidak sah. Berikut adalah cara kerja protokol Telnet: (Logistics 2008; Davie 2012)

1. **Inisiasi Koneksi**:
    a. Proses dimulai ketika pengguna ingin terhubung ke perangkat jarak jauh melalui Telnet. Pengguna biasanya menggunakan perangkat lunak Telnet klien, seperti PuTTY atau terminal yang mendukung Telnet, untuk menginisiasi koneksi.
    b. Pengguna harus menentukan alamat IP atau nama domain server yang akan diakses.
2. **Koneksi ke Port Telnet**:
    a. Telnet menggunakan port standar 23 (TCP) untuk berkomunikasi. Ketika pengguna menginisiasi koneksi, klien Telnet menghubungi server pada port 23 perangkat jarak jauh.
3. **Autentikasi Pengguna**:
    a. Setelah koneksi berhasil dibuat, perangkat jarak jauh (host yang dituju) biasanya meminta pengguna untuk mengidentifikasi diri dengan memberikan nama pengguna dan kata sandi.
    b. Ini merupakan tahap otentikasi, di mana pengguna memberikan informasi yang diperlukan untuk mendapatkan akses ke perangkat jarak jauh.
4. **Sesi Telnet Dibuat**:
    a. Setelah pengguna berhasil diautentikasi, sesi Telnet aktif dibuat antara klien dan perangkat jarak jauh. Selama sesi

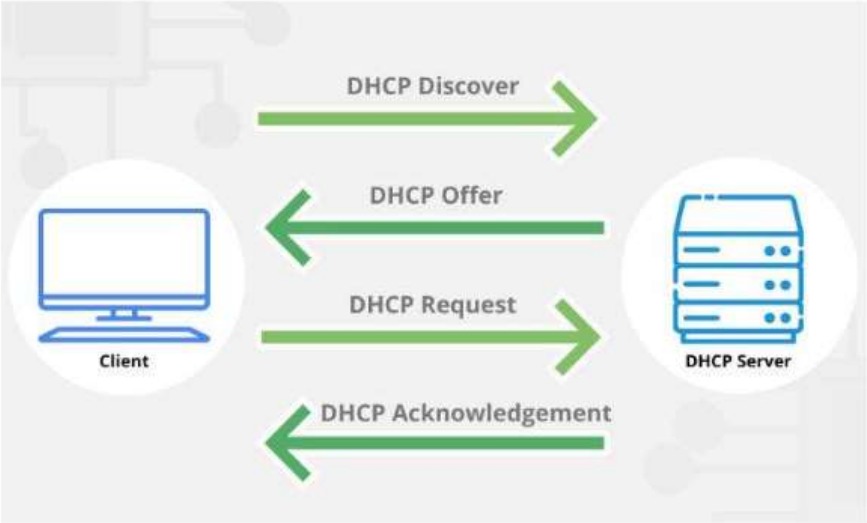
ini, perintah dan data dapat dikirimkan dari klien ke perangkat jarak jauh dan sebaliknya.

b. Semua data yang dikirimkan dalam sesi Telnet tidak dienkripsi, sehingga dapat terekspose jika ada pihak yang mencoba memantau lalu lintas jaringan.

5. **Perintah dan Komunikasi**:
   a. Selama sesi Telnet, pengguna dapat menjalankan perintah di perangkat jarak jauh seolah-olah mereka berada di depan perangkat fisik. Perintah-perintah ini dikirimkan dalam bentuk teks ke perangkat jarak jauh.
   b. Output dari perintah-perintah tersebut juga dikirimkan kembali ke klien Telnet dan ditampilkan kepada pengguna.
6. **Pemutusan Koneksi**:
   a. Sesuai kebutuhan, pengguna dapat mengakhiri sesi Telnet dengan menutup koneksi atau menghentikan perangkat lunak klien Telnet. Server juga dapat mengakhiri sesi jika diperlukan.
7. **Keamanan Telnet**:
   a. Telnet tidak memiliki fitur enkripsi bawaan, yang membuatnya rentan terhadap penyadapan data. Sebagai alternatif yang lebih aman, banyak organisasi telah beralih ke *Secure Shell* (SSH) yang menyediakan enkripsi data selama sesi jarak jauh.

Meskipun Telnet masih digunakan dalam beberapa situasi, seperti mengakses perangkat tertentu yang tidak mendukung protokol SSH, disarankan untuk menggunakan protokol yang lebih aman seperti SSH untuk mengakses dan mengendalikan perangkat jarak jauh. Ini akan membantu melindungi data sensitif dari ancaman keamanan.

5.14 Dynamic Host Configuration Protocol (DHCP)



Gambar 5.14. *Dynamic Host Configuration Protocol* (DHCP)
Sumber : https://windowstechno.com/

Dynamic Host Configuration Protocol (DHCP) adalah protokol jaringan yang digunakan untuk mengalokasikan alamat IP dan konfigurasi jaringan lainnya secara otomatis kepada perangkat dalam suatu jaringan. DHCP memungkinkan perangkat seperti komputer, printer, atau ponsel untuk mendapatkan informasi yang diperlukan untuk berkomunikasi di dalam jaringan tanpa harus dikonfigurasi secara manual. Berikut adalah cara kerja protokol DHCP dengan jelas: (Logistics 2008; Davie 2012)

1. **Permintaan DHCP dari Klien**:
    a. Ketika sebuah perangkat terhubung ke jaringan, misalnya saat dinyalakan atau saat klien memasuki jaringan yang berbeda, perangkat tersebut akan mencoba untuk

mendapatkan alamat IP dan konfigurasi jaringan lainnya melalui protokol DHCP.

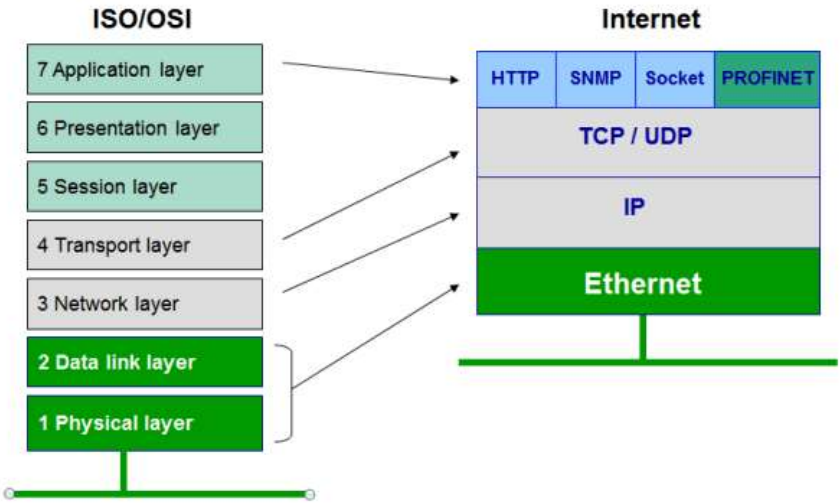
b. Perangkat klien mengirimkan pesan "DHCP Discover" ke dalam jaringan yang berisi permintaan untuk alamat IP.

2. **Pengiriman Pesan Discover ke Server DHCP**:
   a. Pesan "DHCP Discover" yang dikirim oleh perangkat klien akan diterima oleh server DHCP yang ada dalam jaringan. Server DHCP bertugas untuk mengelola dan menyediakan alamat IP yang tersedia.
3. **Penawaran dari Server DHCP**:
   a. Setelah menerima pesan "DHCP Discover", server DHCP akan merespons dengan pesan "DHCP Offer." Pesan ini berisi penawaran alamat IP yang dapat digunakan oleh perangkat klien, bersama dengan informasi konfigurasi jaringan lainnya seperti subnet mask, gateway, dan alamat DNS.
   b. Server DHCP dapat memberikan beberapa penawaran jika ada lebih dari satu alamat IP yang tersedia.
4. **Permintaan Konfirmasi dari Klien**:
   a. Perangkat klien menerima pesan "DHCP Offer" dari server DHCP dan memilih salah satu penawaran. Setelah memilih, perangkat klien mengirimkan pesan "DHCP Request" kepada server DHCP yang dipilih.
   b. Pesan "DHCP Request" berisi konfirmasi permintaan alamat IP yang dipilih oleh perangkat klien.
5. **Pengkonfirmasian dari Server DHCP**:
   a. Setelah menerima pesan "DHCP Request" dari perangkat klien, server DHCP yang dipilih akan mengirimkan pesan "DHCP Acknowledgment" (DHCP ACK). Pesan ini mengonfirmasi bahwa perangkat klien dapat menggunakan alamat IP yang telah dialokasikan, serta konfigurasi jaringan lainnya yang telah ditawarkan.

6. **Penggunaan Alamat IP oleh Klien**:
    a. Setelah menerima pesan "DHCP ACK" dari server DHCP, perangkat klien menggunakan alamat IP yang telah dialokasikan untuk berkomunikasi di dalam jaringan.
    b. Perangkat klien juga menggunakan informasi konfigurasi jaringan seperti subnet mask, gateway, dan DNS yang diberikan oleh server DHCP.
7. **Perpanjangan Sewa Alamat IP (Renewal)**:
    a. Alamat IP yang dialokasikan oleh server DHCP bersifat sewa (lease) dan memiliki batas waktu tertentu. Setelah batas waktu tersebut habis, perangkat klien harus memperpanjang sewa alamat IP dengan mengirimkan pesan "DHCP Request" kepada server DHCP yang awalnya memberikan alamat IP.
    b. Jika perangkat klien tidak dapat memperpanjang sewa, alamat IP tersebut akan dinyatakan sebagai tersedia dan dapat dialokasikan ke perangkat lain.

DHCP memungkinkan administrasi yang efisien dari jaringan, menghindari konflik alamat IP, dan memudahkan penambahan dan penghapusan perangkat dari jaringan tanpa harus mengatur konfigurasi secara manual. Ini adalah protokol penting dalam pengelolaan jaringan modern.

5.15 Ethernet Protocol



Gambar 5.15. Ethernet Protocol
Sumber : https://us.profinet.com/

Ethernet adalah protokol lapisan fisik (Layer 2) yang digunakan untuk mengatur komunikasi jaringan di dalam suatu jaringan lokal (LAN). Ini adalah salah satu protokol jaringan yang paling umum digunakan dan mendasari banyak teknologi jaringan modern. Berikut adalah cara kerja protokol Ethernet dengan jelas: (Logistics 2008; Davie 2012)

1. **Media Transmisi**:
    a. Ethernet dapat beroperasi melalui berbagai jenis media transmisi, termasuk kabel tembaga (seperti *Ethernet twisted-pair*), serat optik, dan nirkabel (Wi-Fi). Media transmisi ini menghubungkan perangkat dalam jaringan LAN.

2. **Frame Data Ethernet**:
    a. Data yang akan dikirimkan melalui jaringan Ethernet dibungkus dalam "frame data Ethernet." Ini adalah unit data dasar yang akan ditransmisikan dalam jaringan.
    b. Frame Ethernet terdiri dari beberapa bagian, termasuk header dan trailer, yang berisi informasi penting seperti alamat MAC (Media Access Control), jenis protokol, data itu sendiri, dan checksum untuk deteksi kesalahan.
3. **Alamat MAC**:
    a. Setiap perangkat yang terhubung ke jaringan Ethernet memiliki alamat MAC yang unik. Alamat MAC digunakan untuk mengidentifikasi perangkat dalam jaringan.
    b. Ketika data dikirim melalui Ethernet, alamat MAC tujuan ditentukan dalam header frame, memungkinkan data hanya diterima oleh perangkat yang sesuai dengan alamat MAC tersebut.
4. **Media Access Control (MAC) Layer**:
    a. Lapisan MAC (Lapisan 2) dalam model OSI adalah bagian penting dari Ethernet. Ini mengatur akses ke media transmisi bersama dalam jaringan.
    b. Dalam jaringan Ethernet berbasis kabel, ada protokol "*Carrier Sense Multiple Access with Collision Detection*" (CSMA/CD) yang digunakan untuk menghindari tabrakan data saat dua perangkat mencoba mengirim data pada saat yang sama. Dalam jaringan Ethernet modern, seperti Ethernet Gigabit dan lebih cepat, CSMA/CD biasanya tidak diperlukan karena kecepatan transmisi yang tinggi.
5. **Frame Transmission**:
    a. Setelah frame data Ethernet dibuat, perangkat pengirim mengirimkannya ke jaringan melalui media transmisi yang sesuai. Data ini akan melintasi kabel atau media transmisi lainnya hingga mencapai perangkat tujuan.

b. Perangkat penerima di dalam jaringan akan memeriksa alamat MAC tujuan dalam header frame. Jika alamat MAC sesuai dengan alamat MAC perangkat tersebut, data akan diterima dan diproses.

6. **Operasi Full-Duplex dan Half-Duplex**:
   a. *Ethernet* dapat beroperasi dalam mode *full-duplex* atau *half-duplex*. Dalam mode full-duplex, perangkat dapat mengirim dan menerima data secara bersamaan, sementara dalam mode half-duplex, perangkat harus berbagi media transmisi dan hanya dapat mengirim atau menerima data pada satu waktu.
7. **Kesalahan dan Retransmisi**:
   a. Selama transmisi, jika terjadi kesalahan dalam frame data, perangkat pengirim atau penerima dapat mendeteksinya menggunakan checksum yang terdapat dalam trailer frame Ethernet. Jika ada kesalahan, frame dapat ditinggalkan atau memicu permintaan ulang (retransmisi) dari perangkat pengirim.
8. **Topologi Jaringan**:
   a. Ethernet mendukung berbagai topologi jaringan, termasuk topologi bintang, bus, cincin, dan mesh, tergantung pada bagaimana perangkat dihubungkan dan diatur dalam jaringan LAN.

Ethernet adalah protokol yang sangat andal dan scalable, yang digunakan di hampir semua LAN di seluruh dunia. Ini telah berkembang seiring dengan waktu, mulai dari Ethernet berkecepatan rendah seperti 10 Mbps hingga kecepatan Gigabit dan lebih tinggi yang digunakan dalam jaringan modern. Ethernet terus berkembang untuk memenuhi kebutuhan jaringan yang semakin kompleks dan berkecepatan tinggi.

DAFTAR PUSTAKA

Davie LLP and BS. 2012. *In Praise of Computer Networks: A Systems Approach Fifth Edition*. Morgan Kaufmann is an imprint of Elsevier.

Logistics C. 2008. CS244A : An Introduction to Computer Networks. *I Can*.

BAB 6
KEAMANAN JARINGAN

Oleh Suwito Pomalingo

6.1 Pendahuluan

6.1.1 Latar Belakang

Dalam era digital yang semakin kompleks, jaringan komputer telah menjadi tulang punggung dari berbagai aktivitas bisnis, pemerintahan, dan pribadi. Namun, seiring dengan perkembangan teknologi, ancaman terhadap keamanan jaringan juga semakin meningkat. Serangan siber, peretasan, dan pelanggaran data adalah beberapa contoh ancaman yang dapat menghancurkan integritas dan kerahasiaan informasi. Oleh karena itu, pemahaman mendalam tentang keamanan jaringan menjadi sangat penting.

6.1.2 Tujuan Buku

Buku ini bertujuan untuk memberikan pandangan komprehensif tentang keamanan jaringan komputer. Mulai dari dasar-dasar keamanan, teknologi yang digunakan, hingga penerapan kecerdasan buatan dan pembelajaran mesin dalam keamanan jaringan. Buku ini dirancang untuk menjadi panduan bagi praktisi keamanan siber, peneliti, dan siapa saja yang tertarik dalam memahami dan meningkatkan keamanan jaringan.

6.1.3 Sasaran Pembaca

1. Praktisi Keamanan Siber
2. Peneliti di Bidang Keamanan Jaringan
3. Mahasiswa dan Dosen di Bidang Teknologi Informasi dan Keamanan Informasi

4. Profesional IT
5. Pecinta Teknologi

6.2 Pengenalan Keamanan Jaringan

6.2.1 Pentingnya Keamanan Jaringan

Keamanan jaringan adalah salah satu aspek kritis dalam dunia teknologi informasi yang terus berkembang. Dalam era digital ini, jaringan komputer menjadi tulang punggung hampir semua aspek kehidupan, mulai dari komunikasi dan bisnis hingga pemerintahan dan keamanan nasional. Oleh karena itu, pentingnya keamanan jaringan tidak bisa diabaikan (Schneier, 2016).

1. Perlindungan Data dan Informasi
   Data dan informasi adalah aset yang sangat berharga bagi individu, organisasi, atau negara. Keamanan jaringan memastikan bahwa data ini aman dari akses atau modifikasi yang tidak sah, sehingga menjaga integritas dan kerahasiaan informasi (Stallings and Brown, 2018). Data pelanggan, data keuangan, dan informasi strategis adalah beberapa contoh data yang sangat krusial bagi sebuah organisasi. Keamanan jaringan memastikan bahwa data ini terlindungi dari ancaman eksternal maupun internal. Tanpa keamanan yang memadai, data bisa dicuri, diubah, atau dihancurkan, yang pada akhirnya akan merusak integritas dan kerahasiaan informasi. Oleh karena itu, keamanan jaringan tidak hanya melindungi data tetapi juga menjaga kepercayaan stakeholder.
2. Dampak Finansial
   Serangan siber bisa sangat mahal. Selain kerugian langsung seperti pencurian uang atau data, ada juga biaya tambahan yang harus dikeluarkan untuk memulihkan sistem dan memperbaiki reputasi perusahaan. Serangan siber bisa menimbulkan kerugian finansial yang signifikan. Menurut sebuah studi oleh Cybersecurity Ventures, kerugian akibat

serangan siber diperkirakan akan mencapai $6 triliun secara global pada tahun 2021 (Morgan, 2020).

3. Kepercayaan Pelanggan
   Kepercayaan pelanggan adalah salah satu aset terpenting yang bisa dimiliki oleh sebuah organisasi. Jika sebuah perusahaan tidak dapat melindungi data pelanggannya, reputasinya akan tercemar dan pelanggan mungkin akan memilih untuk pergi (Romanosky, 2016). Ini tidak hanya berdampak pada pendapatan tetapi juga pada daya saing dalam jangka panjang. Kepercayaan adalah komponen penting dalam bisnis. Jika sebuah organisasi tidak dapat melindungi data pelanggannya, ini akan berdampak negatif pada reputasi dan bisa jadi akan kehilangan pelanggan.
4. Kepatuhan Hukum
   Banyak negara memiliki undang-undang yang mengharuskan organisasi untuk melindungi data pelanggan dan informasi sensitif lainnya. Kegagalan dalam mematuhi ini bisa berakibat pada sanksi hukum (Saridakis *et al.*, 2016). Kepatuhan terhadap undang-undang dan regulasi adalah suatu keharusan. Di banyak negara, ada undang-undang yang mengharuskan perusahaan untuk melindungi data pelanggan dan informasi sensitif lainnya. Kegagalan dalam mematuhi regulasi ini bisa berakibat pada denda yang besar dan tuntutan hukum yang bisa merusak bisnis.
5. Keamanan Nasional
   Dalam konteks keamanan nasional, jaringan yang tidak aman bisa menjadi target serangan oleh negara pihak ketiga untuk mengakses informasi sensitif atau bahkan melumpuhkan infrastruktur kritis (Clarke and Knake, 2011). Keamanan jaringan juga memiliki implikasi yang jauh lebih besar dalam konteks keamanan nasional. Negara-negara yang memiliki infrastruktur kritis yang rentan terhadap serangan siber berisiko menghadapi ancaman

yang bisa melumpuhkan perekonomian atau bahkan membahayakan nyawa warganya.

6. Inovasi dan Pertumbuhan
   Keamanan jaringan juga memungkinkan inovasi dan pertumbuhan ekonomi. Organisasi yang memiliki jaringan yang aman lebih cenderung untuk berinvestasi dalam teknologi baru dan solusi inovatif (Anderson *et al.*, 2013). Keamanan jaringan bukan hanya tentang melindungi aset; ini juga tentang memungkinkan inovasi dan pertumbuhan. Dengan jaringan yang aman, perusahaan lebih cenderung untuk berinvestasi dalam penelitian dan pengembangan, yang pada akhirnya akan mendorong pertumbuhan ekonomi.

6.2.2 Ancaman dan Risiko

Ancaman yang bisa datang dari banyak sumber. Ancaman eksternal, seperti yang dijelaskan oleh (Clarke and Knake, 2011), bisa melibatkan serangan dari hacker atau negara pihak ketiga yang berupaya mencuri data atau merusak infrastruktur. Di sisi lain, ancaman internal, seringkali lebih sulit dideteksi, bisa datang dari karyawan atau orang lain yang sudah memiliki akses ke jaringan.

Selain ancaman manusia, ada juga ancaman fisik yang harus diperhatikan. Bencana alam, kebakaran, atau kegagalan perangkat keras bisa merusak infrastruktur fisik dan menyebabkan kehilangan data atau downtime. Ancaman perangkat lunak seperti malware, ransomware, dan virus juga menjadi perhatian serius dalam keamanan jaringan dan bisa merusak sistem atau mencuri data.

Risiko yang terkait dengan ancaman ini sangat beragam dan bisa memiliki dampak jangka panjang. Kehilangan data adalah salah satu risiko paling serius, yang bisa berdampak tidak hanya pada operasional tetapi juga pada reputasi perusahaan. Downtime

atau kegagalan sistem adalah risiko lain yang bisa mempengaruhi produktivitas dan pendapatan.

Kerugian finansial juga menjadi perhatian utama. Biaya pemulihan dari serangan siber bisa sangat mahal, belum lagi potensi denda dari pihak berwenang jika terbukti ada kelalaian dalam melindungi data. Selain itu, rusaknya reputasi dan kepercayaan pelanggan juga menjadi risiko yang tidak bisa diabaikan dan bisa mempengaruhi daya saing perusahaan dalam jangka panjang.

Dengan demikian, pentingnya keamanan jaringan tidak bisa diabaikan. Mengidentifikasi dan mengelola ancaman serta risiko adalah langkah krusial dalam memastikan keamanan data dan kelangsungan bisnis. Oleh karena itu, keamanan jaringan harus menjadi prioritas bagi setiap organisasi yang bergantung pada teknologi informasi.

6.2.3 Aspek Keamanan Jaringan

1. Keamanan Fisik
   Keamanan fisik adalah aspek pertama dan paling dasar dalam keamanan jaringan. Ini melibatkan perlindungan terhadap perangkat keras seperti server, router, dan switch dari ancaman fisik seperti pencurian, kebakaran, atau bencana alam. Tanpa keamanan fisik yang memadai, semua upaya keamanan lainnya bisa menjadi sia-sia.
2. Keamanan Perimeter
   Keamanan perimeter melibatkan penggunaan firewall, IDS/IPS (Intrusion Detection System/Intrusion Prevention System), dan teknologi serupa untuk membatasi akses ke jaringan. Ini bertujuan untuk mencegah atau mendeteksi akses yang tidak sah dari luar jaringan.
3. Keamanan Akses
   Keamanan akses adalah tentang memastikan bahwa hanya pengguna atau sistem yang berwenang yang bisa

mengakses jaringan dan sumber daya yang ada di dalamnya. Ini melibatkan penggunaan otentikasi, otorisasi, dan akuntabilitas (AAA) untuk membatasi akses berdasarkan kebutuhan dan peran.

4. Keamanan Transmisi Data
   Keamanan transmisi data melibatkan enkripsi dan teknologi lainnya untuk melindungi data yang dikirimkan antar perangkat dalam jaringan. Ini penting untuk mencegah penyadapan data atau "man-in-the-middle" attacks yang bisa mengakses atau memodifikasi data selama transmisi.
5. Keamanan Aplikasi
   Keamanan aplikasi berfokus pada aplikasi yang berjalan di atas jaringan. Ini melibatkan penggunaan perangkat lunak yang aman, pembaruan keamanan yang tepat waktu, dan pemeriksaan keamanan kode untuk mencegah potensi eksploitasi melalui aplikasi.
6. Keamanan End-Point
   Keamanan end-point melibatkan perlindungan perangkat akhir seperti komputer, smartphone, dan tablet yang terhubung ke jaringan. Ini bisa melibatkan penggunaan antivirus, antimalware, dan kebijakan keamanan perangkat untuk mencegah kompromi dari titik akhir ini.
7. Keamanan Operasional
   Keamanan operasional adalah tentang prosedur dan kebijakan yang membantu menjaga keamanan jaringan sehari-hari. Ini bisa melibatkan pelatihan karyawan, audit keamanan, pemantauan jaringan, dan respons insiden untuk menangani potensi masalah keamanan.

Setiap aspek ini saling terkait dan perlu dikelola secara holistik untuk menciptakan lingkungan jaringan yang benar-benar aman. Tidak ada satu aspek pun yang bisa berdiri sendiri dalam

memberikan keamanan yang komprehensif; semuanya harus bekerja bersama untuk meminimalkan risiko dan melindungi aset informasi.

6.3 Dasar-dasar Keamanan Jaringan

6.3.1 Autentikasi dan Otorisasi

Autentikasi dan otorisasi adalah dua pilar utama dalam keamanan jaringan yang memastikan bahwa hanya pengguna atau sistem yang berwenang yang dapat mengakses sumber daya dalam jaringan. Meskipun keduanya sering digunakan secara bergantian, mereka memiliki fungsi yang berbeda tetapi saling melengkapi dalam konteks keamanan.

Autentikasi adalah proses verifikasi identitas. Dalam konteks jaringan, ini biasanya melibatkan pengguna memasukkan kredensial seperti nama pengguna dan kata sandi. Metode autentikasi lainnya termasuk penggunaan token keamanan, kartu pintar, atau biometrik seperti sidik jari atau pengenalan wajah. Autentikasi multi-faktor (MFA), yang menggabungkan dua atau lebih metode autentikasi, semakin populer sebagai cara untuk meningkatkan keamanan.

Sebagai contoh, saat Anda mencoba masuk ke email Anda, Anda akan diminta untuk memasukkan nama pengguna dan kata sandi. Jika Anda juga memiliki autentikasi dua faktor diaktifkan, Anda mungkin juga akan diminta untuk memasukkan kode yang dikirim ke ponsel Anda.

Setelah autentikasi berhasil, langkah selanjutnya adalah otorisasi. Ini adalah proses yang menentukan apa yang bisa dilakukan pengguna setelah mereka berhasil masuk. Misalnya, dalam sebuah perusahaan, karyawan di departemen keuangan mungkin memiliki otorisasi untuk mengakses data keuangan, tetapi tidak untuk data personil. Otorisasi biasanya dikelola oleh sistem manajemen akses berbasis peran (RBAC) atau model keamanan lainnya.

Sebagai contoh, dalam sebuah sistem manajemen basis data, seorang administrator mungkin memiliki hak untuk membaca, menulis, dan menghapus data, sementara seorang analis data mungkin hanya memiliki hak untuk membaca data.

Autentikasi dan otorisasi adalah krusial karena mereka membentuk lapisan pertama pertahanan dalam keamanan jaringan. Tanpa autentikasi yang kuat, sistem rentan terhadap serangan seperti "brute force attacks" atau "phishing attacks". Tanpa otorisasi yang tepat, pengguna yang berhasil masuk bisa melakukan apa saja, termasuk aksi-aksi yang bisa merugikan organisasi.

Autentikasi dan otorisasi adalah elemen dasar dalam keamanan jaringan yang membantu dalam memastikan bahwa sumber daya dan data hanya dapat diakses oleh mereka yang berwenang. Mereka adalah bagian dari strategi keamanan yang lebih besar yang juga harus mencakup keamanan fisik, keamanan perangkat lunak, dan kebijakan keamanan organisasi.

6.3.2 Integritas Data

Integritas data adalah salah satu pilar utama dalam keamanan informasi, bersama dengan kerahasiaan dan ketersediaan. Integritas data menjamin bahwa informasi yang disimpan, diproses, atau ditransmisikan tetap utuh dan tidak diubah tanpa otorisasi. Dalam konteks keamanan jaringan, integritas data memastikan bahwa data yang dikirim dari satu titik ke titik lain tiba dengan kondisi yang sama seperti saat dikirimkan.

Tanpa integritas data, keputusan bisnis atau operasional bisa dibuat berdasarkan informasi yang salah atau menyesatkan. Ini bisa berakibat fatal, terutama dalam aplikasi kritis seperti sistem keuangan, perawatan kesehatan, atau keamanan nasional. Selain itu, integritas data yang buruk bisa merusak reputasi sebuah organisasi dan mengakibatkan kerugian finansial.

Mekanisme untuk Menjaga Integritas Data

1. *Hashing*: Teknik ini digunakan untuk memverifikasi integritas data. Sebuah fungsi hash akan menghasilkan hash code dari data yang bisa digunakan untuk memverifikasi apakah data tersebut telah diubah atau tidak.
2. *Digital Signature*: Ini adalah bentuk lain dari hashing tetapi lebih canggih karena melibatkan penggunaan kunci pribadi untuk membuat tanda tangan digital.
3. *Version Control*: Dalam basis data, kontrol versi bisa digunakan untuk melacak perubahan pada data, memungkinkan pemulihan data ke versi sebelumnya jika terjadi perubahan yang tidak sah.
4. *Access Control*: Memastikan hanya pengguna yang berwenang yang bisa mengakses atau memodifikasi data.
5. *Regular Audits*: Audit keamanan rutin dan pemantauan jaringan bisa membantu dalam mendeteksi dan mencegah perubahan data yang tidak sah.

Sebagai contoh, dalam transaksi keuangan online, integritas data memastikan bahwa jumlah uang yang dikirim dari satu akun ke akun lainnya tidak diubah selama proses transmisi. Teknik seperti enkripsi dan digital signature sering digunakan untuk memastikan integritas data dalam kasus ini.

Salah satu tantangan utama dalam menjaga integritas data adalah kompleksitas jaringan dan sistem modern. Solusinya adalah pendekatan keamanan berlapis yang melibatkan teknologi, proses, dan kebijakan. Selain itu, pendidikan dan kesadaran keamanan bagi pengguna dan administrator juga penting.

Integritas data adalah aspek krusial dari keamanan jaringan yang memastikan keakuratan dan keandalan informasi. Tanpa integritas data, kepercayaan pada sistem dan data bisa hilang, yang pada akhirnya bisa merusak sebuah organisasi baik dari segi operasional maupun reputasi.

6.3.3 Kerahasiaan Data

Kerahasiaan data adalah salah satu dari tiga pilar utama dalam keamanan informasi, bersama dengan integritas dan ketersediaan. Kerahasiaan data berfokus pada perlindungan informasi dari akses atau pengungkapan yang tidak sah. Dalam konteks keamanan jaringan, ini berarti memastikan bahwa data yang dikirim atau disimpan hanya dapat diakses oleh pihak yang berwenang.

Kerahasiaan data adalah elemen krusial dalam menjaga kepercayaan dan memenuhi persyaratan hukum atau regulasi, seperti GDPR di Uni Eropa atau HIPAA di Amerika Serikat. Kegagalan dalam menjaga kerahasiaan data bisa berakibat pada kerugian finansial, tuntutan hukum, dan kerusakan reputasi.

Mekanisme untuk Menjaga Kerahasiaan Data

1. Enkripsi: Ini adalah metode paling umum untuk menjaga kerahasiaan data. Data dienkripsi sebelum dikirim dan didekripsi oleh penerima yang memiliki kunci yang sesuai.
2. Otentikasi dan Otorisasi: Memastikan bahwa hanya pengguna yang berwenang yang dapat mengakses data. Ini seringkali melibatkan penggunaan nama pengguna dan kata sandi, serta teknologi lain seperti autentikasi dua faktor.
3. Virtual Private Network (VPN): VPN memungkinkan pengguna untuk mengakses jaringan pribadi melalui internet dalam mode yang aman dan terenkripsi.
4. Firewall dan IDS/IPS: Ini adalah perangkat atau perangkat lunak yang memonitor dan mengontrol lalu lintas jaringan berdasarkan aturan keamanan yang telah ditentukan.
5. Data Masking: Teknik ini digunakan untuk menyembunyikan data asli dengan karakter acak atau data lain, biasanya digunakan dalam lingkungan pengujian.

Sebagai contoh, dalam sistem perawatan kesehatan, kerahasiaan data pasien adalah prioritas utama. Teknik enkripsi

dan otentikasi digunakan untuk memastikan bahwa hanya dokter atau tenaga medis yang berwenang yang dapat mengakses informasi medis pasien.

Salah satu tantangan dalam menjaga kerahasiaan data adalah serangan siber yang semakin canggih, seperti serangan "man-in-the-middle" atau "phishing". Solusinya adalah pendekatan keamanan berlapis dan kebijakan keamanan yang ketat, termasuk pelatihan keamanan untuk karyawan dan pemantauan keamanan yang berkelanjutan.

Kerahasiaan data tidak hanya adalah tentang teknologi tetapi juga tentang proses dan orang. Memastikan kerahasiaan data memerlukan kombinasi dari enkripsi yang kuat, kontrol akses yang tepat, dan kebijakan keamanan yang efektif. Dengan demikian, kerahasiaan data menjadi bagian integral dari strategi keamanan informasi suatu organisasi, yang bertujuan untuk melindungi aset paling berharga organisasi: datanya.

6.4 Teknologi Keamanan Jaringan

6.4.1 Firewall

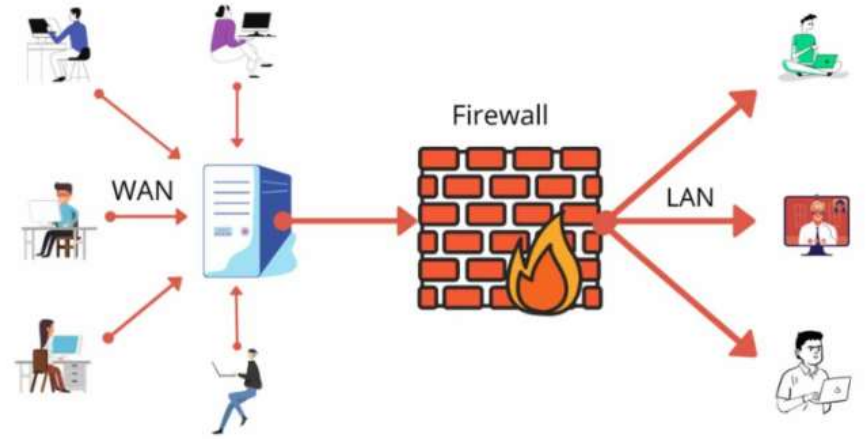
Firewall adalah salah satu komponen teknologi keamanan jaringan yang paling umum dan penting. Fungsinya adalah untuk memfilter lalu lintas jaringan antara jaringan internal (misalnya, LAN) dan jaringan eksternal (misalnya, internet), sehingga membatasi akses yang tidak sah ke atau dari jaringan (Zwicky, Cooper and Chapman, 2000). Firewall bisa berupa perangkat keras atau perangkat lunak, dan seringkali keduanya digunakan secara bersamaan untuk memberikan lapisan keamanan yang lebih kuat.

Jenis-Jenis Firewall

1. *Packet-Filtering Firewalls*: Jenis firewall ini bekerja pada lapisan jaringan dan memfilter paket data berdasarkan alamat IP, port, dan protokol. Contoh: iptables di Linux.
2. *Stateful Inspection Firewalls*: Lebih canggih daripada packet-filtering, jenis ini mempertahankan tabel status dari semua

koneksi jaringan dan membuat keputusan berdasarkan konteks.

3. *Proxy Firewalls*: Bertindak sebagai perantara antara pengguna dan layanan yang diakses, memfilter permintaan berdasarkan aturan keamanan yang telah ditentukan.
4. *Application-Layer Firewalls*: Beroperasi pada lapisan aplikasi dan bisa memfilter lalu lintas berdasarkan jenis aplikasi atau layanan yang digunakan. Contoh: *Web Application Firewall* (WAF).
5. *Next-Generation Firewalls* (NGFW): Menggabungkan fitur dari berbagai jenis firewall lainnya dan menambahkan fungsionalitas seperti identifikasi aplikasi, inspeksi deep-packet, dan lain-lain.



Gambar 6.1. Firewall
(Sumber : internet)

Sebagai contoh, sebuah perusahaan mungkin menggunakan firewall perangkat keras untuk memfilter lalu lintas yang masuk dan keluar dari jaringan perusahaan. Selain itu, firewall perangkat lunak mungkin diinstal pada setiap komputer di jaringan untuk

memberikan lapisan keamanan tambahan. Aturan firewall bisa diatur untuk memblokir akses ke situs web tertentu atau untuk membatasi akses ke sumber daya internal hanya untuk pengguna yang berwenang.

Firewall adalah garis pertahanan pertama dalam banyak jaringan terhadap ancaman eksternal. Tanpa firewall, jaringan akan terbuka lebar untuk berbagai jenis serangan, mulai dari penyadapan data hingga serangan *denial-of-service* (DoS). Selain itu, firewall juga penting untuk membatasi akses internal, sehingga membantu mencegah ancaman dari dalam, seperti kebocoran data oleh karyawan.

Meskipun firewall adalah alat yang kuat, mereka bukanlah solusi keamanan yang lengkap. Serangan yang canggih, seperti APT (Advanced Persistent Threats), sering kali bisa mengelabui firewall. Oleh karena itu, firewall sebaiknya digunakan sebagai bagian dari strategi keamanan berlapis, yang juga bisa mencakup IDS/IPS, antimalware, dan solusi keamanan lainnya.

Firewall adalah elemen krusial dalam arsitektur keamanan jaringan. Dengan memahami jenis-jenis firewall dan bagaimana mereka bekerja, organisasi bisa memilih solusi yang paling sesuai dengan kebutuhan mereka. Namun, penting untuk diingat bahwa firewall hanyalah satu bagian dari solusi keamanan yang komprehensif. Untuk keamanan yang efektif, firewall harus digunakan bersama dengan berbagai alat dan teknik keamanan lainnya.

6.4.2 VPN (*Virtual Private Network*)

VPN (*Virtual Private Network*) dalam Teknologi Keamanan Jaringan Pengantar *Virtual Private Network* (VPN) adalah teknologi yang memungkinkan pembentukan koneksi jaringan yang aman dan terenkripsi melalui internet atau jaringan lain yang tidak aman (Zeltser *et al.*, 2002). VPN digunakan untuk berbagai tujuan, mulai dari memastikan keamanan data selama transmisi hingga

mengakses sumber daya jaringan yang dibatasi secara geografis. Dalam konteks keamanan jaringan, VPN adalah salah satu alat yang paling efektif untuk menjaga kerahasiaan, integritas, dan ketersediaan data.

Jenis-Jenis VPN

1. *Site-to-Site* VPN: Biasanya digunakan untuk menghubungkan dua jaringan yang berbeda lokasi, seperti cabang perusahaan yang berbeda.
2. *Remote Access* VPN: Memungkinkan pengguna untuk mengakses jaringan perusahaan atau sumber daya lainnya dari lokasi yang jauh.
3. PPTP, L2TP, OpenVPN, IKEv2/IPsec: Ini adalah beberapa protokol yang digunakan dalam VPN, masing-masing dengan tingkat keamanan dan kompleksitasnya sendiri.

Sebagai contoh, seorang karyawan yang bekerja dari rumah dapat menggunakan VPN untuk mengakses file dan aplikasi yang tersimpan di jaringan perusahaan. Atau, seseorang yang menggunakan Wi-Fi publik bisa menggunakan VPN untuk memastikan bahwa data mereka aman dari penyadapan.

Pentingnya VPN :

1. Kerahasiaan Data: VPN melindungi data dengan cara mengenkripsi lalu lintas internet, sehingga membuatnya hampir mustahil untuk disadap.
2. Integritas Data: VPN juga memastikan integritas data selama transmisi dengan menggunakan teknologi seperti hashing dan digital signatures.
3. Akses Terbatas: VPN memungkinkan akses ke sumber daya yang dibatasi berdasarkan lokasi atau jaringan, seperti layanan streaming atau database perusahaan.
4. Anonimitas: Dengan menyembunyikan alamat IP asli pengguna, VPN juga bisa digunakan untuk menjaga anonimitas online.

Tantangan dan Solusi

1. Kecepatan: Penggunaan VPN seringkali menurunkan kecepatan internet karena proses enkripsi. Solusinya adalah menggunakan server VPN yang lebih dekat atau protokol yang lebih cepat.
2. Kompatibilitas: Tidak semua perangkat atau jaringan mendukung semua jenis VPN atau protokol. Solusinya adalah memilih solusi VPN yang kompatibel dengan infrastruktur yang ada.
3. Keamanan: Meskipun VPN aman, mereka tidak sepenuhnya tahan terhadap serangan seperti "man-in-the-middle" atau kelemahan protokol. Solusinya adalah selalu memperbarui perangkat lunak VPN dan menggunakan teknologi keamanan tambahan seperti firewall atau antimalware.

VPN adalah teknologi keamanan jaringan yang sangat penting dan serbaguna. Dengan memahami berbagai jenis, kegunaan, dan keamanan yang terkait dengan VPN, organisasi dan individu dapat membuat keputusan yang lebih tepat tentang bagaimana dan kapan menggunakan teknologi ini. Seperti halnya dengan semua solusi keamanan, VPN harus digunakan sebagai bagian dari strategi keamanan yang lebih luas untuk memastikan keamanan dan privasi data.

6.4.3 IDS/IPS (*Intrusion Detection System/Intrusion Prevention System*)

Intrusion Detection System (IDS) dan *Intrusion Prevention System* (IPS) adalah dua komponen krusial dalam arsitektur keamanan jaringan. Keduanya berfungsi untuk memonitor dan menganalisis lalu lintas jaringan untuk mendeteksi dan, dalam kasus IPS, menghalau aktivitas yang mencurigakan atau berbahaya (Ring *et al.*, 2019). Meskipun serupa, IDS lebih fokus pada deteksi

dan pelaporan, sementara IPS aktif dalam mengambil tindakan untuk mencegah atau memitigasi serangan.

Jenis-Jenis IDS/IPS

1. *Network-based* IDS/IPS (NIDS/NIPS): Diinstal pada titik-titik strategis dalam jaringan dan memonitor lalu lintas yang melewati jaringan tersebut.
2. *Host-based* IDS/IPS (HIDS/HIPS): Diinstal pada host individu dan memonitor aktivitas pada host tersebut, termasuk akses file dan operasi sistem.
3. Signature-based Detection: Menggunakan basis data dari tanda tangan serangan yang diketahui untuk mendeteksi ancaman.
4. *Anomaly-based Detection*: Menggunakan model dari aktivitas jaringan yang normal untuk mendeteksi perilaku yang tidak biasa.

Sebagai contoh, sebuah perusahaan mungkin menggunakan NIDS untuk memonitor lalu lintas yang masuk dan keluar dari jaringan perusahaan. Jika sistem mendeteksi lalu lintas yang mencurigakan, seperti percobaan akses ke port yang seharusnya tidak terbuka, IDS akan mengirimkan peringatan ke administrator, sementara IPS akan langsung memblokir lalu lintas tersebut.

Pentingnya IDS/IPS

1. Deteksi Dini: IDS/IPS memungkinkan organisasi untuk mendeteksi ancaman potensial sebelum mereka bisa melakukan kerusakan, memberikan waktu yang berharga untuk merespons.
2. Pelaporan dan Forensik: IDS menyediakan data yang sangat berguna untuk analisis forensik setelah serangan, membantu organisasi memahami bagaimana serangan terjadi dan bagaimana mencegahnya di masa depan.
3. Kepatuhan Regulasi: Banyak standar keamanan dan regulasi industri mengharuskan penggunaan IDS/IPS.

4. Mitigasi Serangan: IPS bisa mengkonfigurasi ulang jaringan atau mengubah aturan firewall secara real-time untuk menghalau serangan.

Tantangan dan Solusi

1. *False Positives/Negatives*: Salah satu tantangan terbesar adalah mengurangi false positives dan false negatives. Solusinya adalah tuning yang cermat dari sistem dan pembaruan reguler dari basis data tanda tangan serangan.
2. *Overhead* dan Latensi: IDS/IPS bisa menambah beban pada jaringan dan perangkat. Solusinya adalah perangkat keras yang lebih kuat dan algoritma deteksi yang lebih efisien.
3. Evasi: Beberapa serangan dirancang untuk mengelabui IDS/IPS. Solusinya adalah pendekatan keamanan berlapis, di mana IDS/IPS hanya satu dari banyak lapisan keamanan.

IDS dan IPS adalah instrumen penting dalam toolkit keamanan jaringan. Mereka tidak hanya membantu dalam mendeteksi dan mencegah serangan tetapi juga berfungsi sebagai alat forensik yang berharga. Seperti semua solusi keamanan, efektivitas mereka tergantung pada konfigurasi, pemeliharaan, dan integrasi dengan solusi keamanan lainnya. Oleh karena itu, mereka harus dianggap sebagai bagian dari strategi keamanan jaringan yang lebih luas dan komprehensif.

6.4.4 Enkripsi Data

Enkripsi data adalah proses mengubah informasi dari bentuk yang dapat dibaca menjadi bentuk yang tidak dapat dibaca tanpa kunci dekripsi. Ini adalah salah satu metode keamanan yang paling efektif untuk melindungi data selama transmisi maupun penyimpanan. Dalam konteks keamanan jaringan, enkripsi adalah salah satu alat utama untuk memastikan kerahasiaan dan integritas data.

Jenis-Jenis Enkripsi

1. Enkripsi Simetris: Menggunakan kunci yang sama untuk enkripsi dan dekripsi. Contoh algoritma: AES, DES.
2. Enkripsi Asimetris: Menggunakan sepasang kunci, satu untuk enkripsi dan satu untuk dekripsi. Contoh algoritma: RSA, ECC.
3. Enkripsi pada Tingkat Transport: Seperti SSL/TLS yang digunakan untuk mengamankan komunikasi web.
4. Enkripsi pada Tingkat Aplikasi: Enkripsi yang dilakukan oleh aplikasi itu sendiri, seperti enkripsi email dengan PGP.

Sebagai contoh, saat Anda mengakses situs web yang aman (HTTPS), enkripsi SSL/TLS digunakan untuk mengamankan data antara browser Anda dan server. Dalam komunikasi email, protokol seperti PGP atau S/MIME dapat digunakan untuk mengenkripsi pesan.

Pentingnya Enkripsi

1. Kerahasiaan: Enkripsi melindungi data dari akses yang tidak sah, menjaga kerahasiaan informasi.
2. Integritas: Teknik enkripsi canggih juga memastikan bahwa data tidak diubah selama transmisi.
3. Otentikasi: Dalam kasus enkripsi asimetris, enkripsi juga bisa digunakan untuk memverifikasi identitas pengirim atau penerima.
4. Non-Repudiation: Enkripsi asimetris, ketika digabungkan dengan tanda tangan digital, dapat digunakan untuk memastikan bahwa pengirim tidak dapat menyangkal pengiriman pesan atau transaksi.

Tantangan dan Solusi

1. Kompleksitas Manajemen Kunci: Mengelola kunci enkripsi, terutama pada skala besar, bisa menjadi tantangan.

Solusinya adalah menggunakan sistem manajemen kunci yang efisien.
2. Overhead Performa: Enkripsi dan dekripsi memerlukan sumber daya komputasi, yang bisa mempengaruhi performa.
3. Solusinya adalah hardware khusus atau algoritma yang lebih efisien.
4. Keamanan Kunci: Jika kunci kompromi, maka keamanan seluruh sistem bisa terancam. Solusinya adalah penyimpanan kunci yang aman dan rotasi kunci yang teratur.

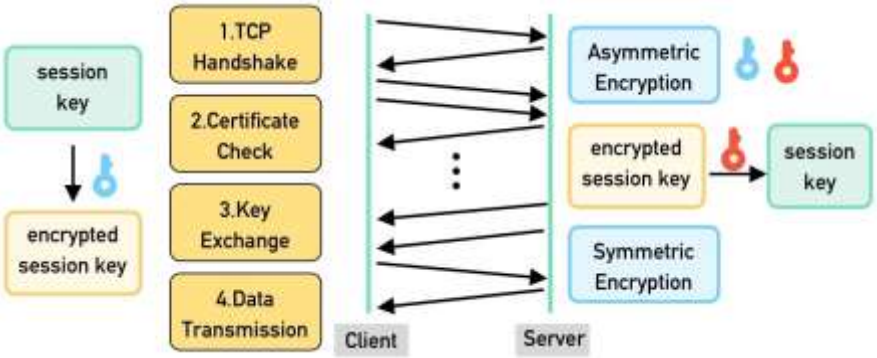
Enkripsi adalah salah satu pilar utama dalam keamanan jaringan dan informasi. Meskipun memiliki beberapa tantangan, manfaat yang ditawarkan oleh enkripsi dalam menjaga kerahasiaan, integritas, dan otentikasi data membuatnya menjadi komponen keamanan yang tak tergantikan. Untuk keamanan yang efektif, enkripsi harus digunakan sebagai bagian dari strategi keamanan yang lebih luas, yang juga mencakup teknologi dan prinsip keamanan lainnya.

6.4.5 Protokol Keamanan

Protokol keamanan memainkan peran krusial dalam menjaga integritas dan keamanan data dalam komunikasi jaringan. SSL/TLS, misalnya, adalah protokol kriptografi yang digunakan untuk mengamankan komunikasi antara dua sistem. Meskipun SSL adalah pendahulunya TLS, keduanya sering digunakan secara bergantian dan berfungsi untuk mengenkripsi data, otentikasi server, serta memastikan integritas data selama transmisi. Protokol ini umumnya digunakan dalam layanan email, perbankan online, dan aplikasi lain yang memerlukan enkripsi data. Di sisi lain, HTTPS adalah ekstensi dari HTTP yang digunakan untuk komunikasi web yang aman. HTTPS mengamankan transmisi data

antara browser dan server dan melindungi terhadap serangan seperti "*man-in-the-middle*" dan "eavesdropping". Ini adalah standar keamanan untuk hampir semua situs web yang memerlukan keamanan, termasuk perbankan online dan e-commerce.

Selain itu, ada juga berbagai protokol VPN seperti PPTP, L2TP, dan OpenVPN, yang masing-masing memiliki kelebihan dan kekurangannya. PPTP adalah salah satu protokol VPN tertua yang menawarkan kecepatan tetapi kurang dalam hal keamanan. L2TP, di sisi lain, lebih aman tetapi memerlukan lebih banyak sumber daya komputasi. OpenVPN adalah pilihan yang sangat aman dan fleksibel tetapi memerlukan instalasi perangkat lunak tambahan. Protokol VPN ini digunakan untuk mengamankan koneksi internet, menyembunyikan lokasi geografis, dan memungkinkan akses ke jaringan pribadi dari jarak jauh.



Gambar 6.2. Cara Kerja HTTPS
(Sumber : www.geeksforgeeks.org)

Memahami nuansa dari masing-masing protokol ini sangat penting untuk keamanan jaringan. Setiap protokol memiliki aplikasi, kelebihan, dan kekurangan yang unik, dan memilih yang paling sesuai tergantung pada kebutuhan spesifik dan konteks

keamanan. Dengan demikian, baik praktisi maupun peneliti di bidang keamanan jaringan perlu mempertimbangkan berbagai faktor ini saat merancang atau meneliti solusi keamanan.

6.5 Keamanan Fisik dan Operasional

6.5.1 Keamanan Perangkat

Keamanan perangkat adalah aspek keamanan jaringan yang seringkali diabaikan tetapi sangat krusial. Ini mencakup perlindungan fisik dan keamanan operasional dari perangkat keras yang digunakan dalam jaringan, termasuk server, switch, router, dan perangkat endpoint seperti komputer dan ponsel. Keamanan perangkat adalah komponen penting dari strategi keamanan jaringan yang komprehensif dan berfungsi sebagai lapisan pertahanan pertama terhadap ancaman fisik dan operasional.

Jenis-Jenis Perangkat dan Ancaman

1. Server: Ancaman termasuk akses fisik yang tidak sah, sabotase, dan pencurian.
2. Router dan Switch: Ancaman termasuk manipulasi konfigurasi, akses tidak sah, dan serangan DoS.
3. Endpoint (PC, Laptop, Ponsel): Ancaman termasuk malware, akses fisik, dan kehilangan data.

Contoh Keamanan Perangkat

1. Server: Menggunakan kunci keamanan fisik dan memonitor akses ke ruang server. Menggunakan sistem manajemen identitas untuk membatasi akses ke sistem operasi.
2. Router dan Switch: Mengubah kata sandi default, membatasi akses administratif, dan memonitor log untuk aktivitas yang mencurigakan.
3. Endpoint: Menggunakan enkripsi disk penuh, memasang antivirus, dan membatasi akses pengguna melalui kebijakan keamanan.

Pentingnya Keamanan Perangkat

1. Integritas Data: Keamanan perangkat memastikan bahwa data yang disimpan atau diproses oleh perangkat tetap utuh dan bebas dari manipulasi.
2. Kerahasiaan: Menghindari akses fisik yang tidak sah ke perangkat membantu menjaga kerahasiaan data.
3. Ketersediaan: Keamanan fisik dan operasional memastikan bahwa perangkat tetap berfungsi dengan benar, memastikan ketersediaan jaringan dan data.

Tantangan dan Solusi

1. Kesadaran Pengguna: Pengguna sering kali adalah titik kelemahan dalam keamanan perangkat. Solusinya adalah pelatihan dan kesadaran keamanan.
2. Manajemen Perangkat Skala Besar: Dalam jaringan besar, manajemen perangkat bisa menjadi sangat kompleks. Solusinya adalah menggunakan alat manajemen perangkat terpusat.
3. Pembaruan dan Patching: Menjaga perangkat tetap up-to-date adalah tantangan tetapi sangat penting. Solusinya adalah otomatisasi proses pembaruan dan patching.

Keamanan perangkat adalah aspek keamanan jaringan yang sering diabaikan tetapi sangat penting. Ini mencakup berbagai tindakan, mulai dari keamanan fisik seperti kunci dan sistem akses, hingga keamanan operasional seperti enkripsi dan kebijakan akses. Tanpa keamanan perangkat yang efektif, semua upaya keamanan lainnya bisa menjadi sia-sia jika perangkat fisiknya sendiri rentan terhadap ancaman.

6.5.2 Keamanan Ruang Server

Ruang server adalah jantung dari banyak infrastruktur TI, menyimpan data dan menjalankan aplikasi yang krusial bagi operasional sebuah organisasi. Oleh karena itu, keamanan ruang server adalah salah satu aspek paling penting dalam keamanan jaringan. Ini mencakup perlindungan fisik ruang dan perangkat di dalamnya, serta keamanan operasional yang melibatkan akses dan manajemen data.

Aspek Fisik Keamanan Ruang Server

1. Kontrol Akses Fisik: Menggunakan kartu akses, pemindai sidik jari, atau teknologi biometrik lainnya untuk membatasi siapa saja yang bisa masuk ke ruang server.
2. Pemantauan Video: Menggunakan kamera CCTV untuk memantau aktivitas di dalam dan sekitar ruang server.
3. Deteksi dan Pencegahan Kebakaran: Menggunakan detektor asap dan sistem pemadam kebakaran otomatis.
4. Sistem Keamanan Multi-Lapis: Menggunakan beberapa lapisan keamanan fisik, seperti pintu keamanan ganda dan jendela yang tahan tembus.

Aspek Operasional Keamanan Ruang Server

1. Manajemen Energi: Memastikan bahwa ada pasokan energi yang stabil dan redundan untuk mencegah downtime.
2. Pemantauan Lingkungan: Menggunakan sensor untuk memantau suhu, kelembapan, dan kondisi lain yang bisa mempengaruhi perangkat.
3. Manajemen Patch dan Pembaruan: Memastikan bahwa semua perangkat keras dan perangkat lunak di ruang server selalu up-to-date.
4. Pengawasan Jaringan: Menggunakan IDS/IPS dan solusi keamanan lainnya untuk memantau lalu lintas jaringan dan mendeteksi ancaman.

Sebagai contoh, sebuah perusahaan mungkin membatasi akses ke ruang server hanya untuk staf TI yang telah melalui verifikasi latar belakang dan pelatihan keamanan. Selain itu, semua akses ke ruang server bisa dicatat dan dipantau secara real-time oleh tim keamanan.

Pentingnya Keamanan Ruang Server

1. Integritas Data: Keamanan fisik dan operasional ruang server adalah krusial untuk memastikan integritas data dan sistem.
2. Ketersediaan: Downtime bisa sangat mahal, baik dari segi finansial maupun reputasi. Keamanan ruang server memastikan ketersediaan sistem.
3. Kepatuhan: Banyak regulasi keamanan data, seperti GDPR atau HIPAA, memerlukan keamanan fisik dan operasional yang ketat untuk ruang server.

Tantangan dan Solusi

1. Biaya: Keamanan ruang server bisa menjadi investasi yang mahal. Namun, biaya dari kegagalan keamanan bisa jauh lebih tinggi.
2. Kompleksitas: Dengan banyaknya perangkat dan teknologi yang terlibat, manajemen keamanan bisa menjadi kompleks. Solusinya adalah menggunakan alat manajemen terpusat dan otomatisasi.
3. Insider Threats: Bahkan dengan keamanan fisik yang ketat, ancaman dari dalam organisasi tetap ada. Solusinya adalah kebijakan akses yang ketat dan pemantauan aktivitas.

Keamanan ruang server adalah aspek krusial dari keamanan jaringan yang sering diabaikan. Ini mencakup berbagai tindakan, mulai dari keamanan fisik seperti kontrol akses dan pemantauan, hingga keamanan operasional seperti manajemen

energi dan pemantauan jaringan. Tanpa keamanan ruang server yang efektif, semua upaya keamanan lainnya bisa menjadi sia-sia.

6.5.3 Keamanan Nirkabel

Keamanan nirkabel telah menjadi salah satu topik yang paling penting dalam keamanan jaringan, terutama karena peningkatan penggunaan perangkat mobile dan *Internet of Things* (IoT). Dalam konteks ini, protokol keamanan seperti WEP (*Wired Equivalent Privacy*), WPA (*Wi-Fi Protected Access*), dan WPA2 memainkan peran yang sangat krusial. WEP adalah salah satu protokol keamanan nirkabel tertua dan, meskipun mudah diimplementasikan, ia memiliki banyak kelemahan keamanan, termasuk rentan terhadap serangan "*man-in-the-middle*". WPA datang sebagai peningkatan dari WEP dengan menawarkan enkripsi yang lebih kuat dan otentikasi pengguna. Namun, WPA2 adalah standar industri saat ini yang menawarkan enkripsi dan keamanan yang lebih tinggi, termasuk penggunaan enkripsi AES yang lebih kuat dan protokol otentikasi yang lebih aman.

Gambar 6.3. Interkoneksi Jaringan Nirkabel
(Sumber : internet)

Namun, keamanan nirkabel tidak hanya terbatas pada pemilihan protokol yang tepat. Ada berbagai risiko yang harus dihadapi, termasuk risiko dari penggunaan jaringan Wi-Fi publik, serangan "*Rogue Access Point*", dan potensi risiko keamanan dari perangkat yang tidak aman. Mitigasi dari risiko ini termasuk penggunaan VPN saat mengakses jaringan publik, memastikan semua perangkat nirkabel mendukung enkripsi WPA2 atau lebih tinggi, dan melakukan audit keamanan jaringan secara rutin untuk mendeteksi potensi akses poin yang mencurigakan.

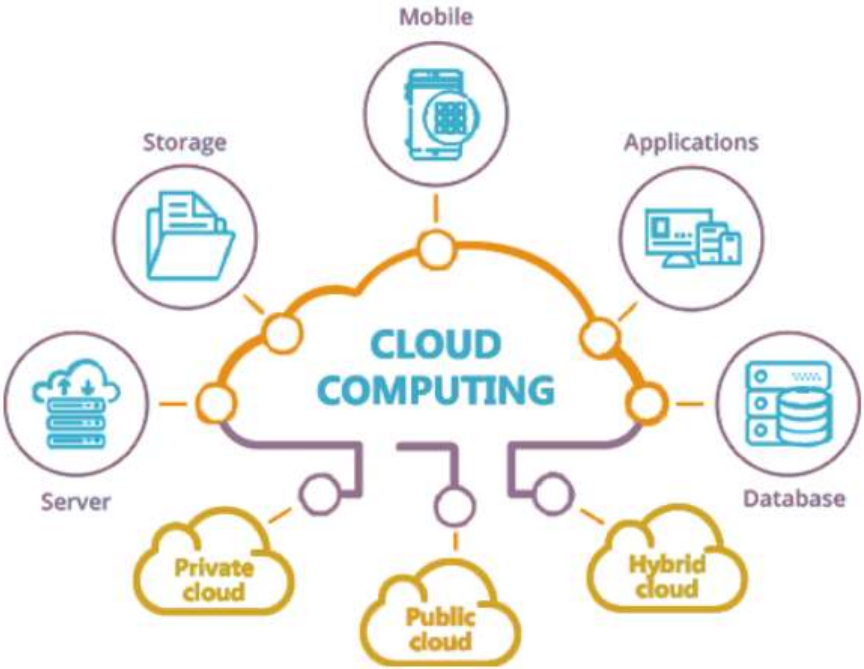
Selain itu, peningkatan penggunaan IoT telah menambah lapisan kompleksitas baru dalam keamanan nirkabel. Perangkat IoT sering kali dirancang dengan fokus pada fungsionalitas daripada keamanan, membuat mereka menjadi target yang menarik untuk penyerang. Keamanan nirkabel dalam konteks IoT melibatkan memastikan bahwa semua perangkat terhubung melalui protokol yang aman, memperbarui perangkat lunak perangkat secara rutin, dan membatasi akses ke perangkat IoT ke jaringan yang aman dan terisolasi.

Dengan demikian, keamanan nirkabel adalah suatu bidang yang memerlukan perhatian khusus, baik dari praktisi keamanan jaringan maupun peneliti. Selain memilih protokol keamanan yang tepat, penting juga untuk mempertimbangkan berbagai risiko lain dan potensi titik kelemahan, terutama dengan semakin populernya perangkat IoT. Ini memerlukan pendekatan yang holistik yang mencakup teknologi, kebijakan, dan edukasi pengguna untuk memitigasi risiko dan memperkuat postur keamanan jaringan nirkabel.

6.5.4 Keamanan Cloud

Keamanan cloud adalah salah satu aspek krusial dalam dunia keamanan siber modern, terutama karena semakin banyak organisasi yang beralih ke solusi berbasis cloud untuk operasional dan penyimpanan data mereka. Salah satu konsep penting dalam keamanan cloud adalah model tanggung jawab keamanan, yang biasanya dibagi antara penyedia layanan cloud dan pengguna. Dalam model ini, penyedia layanan biasanya bertanggung jawab atas keamanan "*of the cloud*", termasuk infrastruktur fisik dan perangkat keras, sedangkan pengguna bertanggung jawab atas keamanan "*in the cloud*", yang mencakup data dan aplikasi yang mereka simpan. Memahami peran dan tanggung jawab ini adalah kunci untuk memitigasi risiko dan memastikan keamanan data.

Keamanan data di cloud adalah area lain yang memerlukan perhatian khusus. Meskipun penyedia layanan cloud seringkali menawarkan tingkat enkripsi yang tinggi, tanggung jawab untuk melindungi data tetap berada di tangan pengguna. Ini termasuk memastikan bahwa data yang disimpan di cloud dienkripsi dan bahwa kebijakan akses yang tepat diterapkan. Selain itu, penting untuk mempertimbangkan lokasi geografis dari pusat data cloud, karena ini dapat mempengaruhi kepatuhan terhadap regulasi privasi data dan keamanan siber.



Gambar 6.4. Cloud Computing
(Sumber : internet)

Virtualisasi dan isolasi sumber daya adalah teknologi lain yang memainkan peran penting dalam keamanan cloud. Virtualisasi memungkinkan untuk memisahkan sumber daya fisik

menjadi beberapa lingkungan virtual yang terisolasi, yang masing-masing dapat dijalankan dengan konfigurasi keamanan yang berbeda. Ini tidak hanya meningkatkan efisiensi tetapi juga memungkinkan untuk isolasi yang lebih baik dari aplikasi dan data yang sensitif. Teknologi ini memungkinkan organisasi untuk menjalankan aplikasi yang berbeda dengan tingkat keamanan yang berbeda dalam lingkungan yang sama, tanpa risiko saling mengganggu.

Dengan demikian, keamanan cloud adalah suatu bidang yang kompleks yang memerlukan pemahaman mendalam tentang berbagai teknologi, model tanggung jawab, dan potensi risiko. Baik praktisi maupun peneliti di bidang keamanan siber perlu mempertimbangkan semua aspek ini saat merancang, mengimplementasikan, atau meneliti solusi keamanan untuk infrastruktur berbasis cloud. Ini memerlukan pendekatan multi-disiplin yang mencakup teknologi, kebijakan, dan kepatuhan untuk memastikan bahwa data dan aplikasi yang disimpan di cloud tetap aman dan terlindungi.

6.5.5 Keamanan End-Point

Keamanan *end-point* adalah salah satu pilar utama dalam strategi keamanan siber yang efektif, terutama di era digital saat ini di mana perangkat mobile dan remote working menjadi semakin umum. Keamanan perangkat mobile, sebagai contoh, adalah isu yang sangat penting karena perangkat ini sering digunakan untuk mengakses data dan aplikasi perusahaan dari lokasi yang berbeda. Risiko termasuk, tetapi tidak terbatas pada, kehilangan fisik perangkat, serangan malware, dan risiko keamanan data saat terhubung ke jaringan Wi-Fi publik. Oleh karena itu, solusi seperti enkripsi perangkat, otentikasi multi-faktor, dan kebijakan keamanan mobile yang ketat harus diimplementasikan.

Manajemen perangkat juga merupakan komponen krusial dari keamanan end-point. Ini melibatkan pelacakan, pemantauan,

dan pemeliharaan semua perangkat yang terhubung ke jaringan perusahaan. Solusi Manajemen Perangkat Mobile (MDM) atau Manajemen Perangkat Endpoint (EDM) sering digunakan untuk ini, memungkinkan tim IT untuk mengontrol perangkat dari pusat, menerapkan kebijakan keamanan, dan bahkan menghapus data dari perangkat yang hilang atau dicuri.

Sandboxing dan virtualisasi adalah teknik lain yang digunakan untuk meningkatkan keamanan end-point. Sandboxing memungkinkan aplikasi atau proses untuk dijalankan dalam lingkungan yang terisolasi, sehingga membatasi aksesnya ke sistem secara keseluruhan dan mencegah penyebaran malware atau eksploitasi kerentanan keamanan. Virtualisasi, di sisi lain, memungkinkan untuk menjalankan sistem operasi atau aplikasi dalam lingkungan virtual, memberikan lapisan tambahan keamanan dan memungkinkan untuk tes keamanan yang lebih mudah dan efektif.

Dengan demikian, keamanan end-point adalah suatu bidang yang memerlukan pendekatan holistik yang mencakup berbagai teknologi, kebijakan, dan praktek terbaik. Ini adalah tantangan yang memerlukan koordinasi antara tim IT, manajemen, dan pengguna akhir, serta pemahaman yang mendalam tentang potensi risiko dan solusi yang tersedia. Baik praktisi maupun peneliti di bidang keamanan siber perlu mempertimbangkan semua faktor ini saat merancang atau meneliti strategi keamanan end-point, karena ini adalah salah satu area yang paling rentan terhadap serangan dalam ekosistem keamanan siber.

6.5.6 Kebijakan Keamanan

Kebijakan keamanan adalah dokumen formal yang merinci langkah-langkah, prosedur, dan pedoman yang harus diikuti oleh individu dan sistem dalam sebuah organisasi untuk memastikan keamanan informasi. Ini adalah fondasi dari setiap program keamanan yang efektif dan berfungsi sebagai kerangka kerja untuk

membuat, mengimplementasikan, dan memantau keamanan di seluruh organisasi.

Jenis-Jenis Kebijakan Keamanan

1. Kebijakan Akses: Menentukan siapa yang memiliki akses ke apa, dan dalam konteks apa.
2. Kebijakan Penggunaan yang Layak: Menentukan apa yang dianggap sebagai penggunaan sumber daya IT yang layak dan etis.
3. Kebijakan Keamanan Fisik: Menentukan langkah-langkah untuk melindungi aset fisik, seperti perangkat dan ruang server.
4. Kebijakan Keamanan Data: Menentukan bagaimana data harus disimpan, ditransfer, dan dihapus.

Contoh Kebijakan Keamanan

1. *Multi-Factor Authentication* (MFA): Kebijakan ini bisa memerlukan semua karyawan untuk menggunakan MFA saat mengakses sumber daya perusahaan.
2. BYOD (*Bring Your Own Device*): Kebijakan ini akan menentukan persyaratan keamanan untuk perangkat pribadi yang digunakan untuk tujuan kerja.

Pentingnya Kebijakan Keamanan

1. Konsistensi: Kebijakan keamanan memastikan bahwa ada pedoman yang konsisten yang harus diikuti oleh semua orang dalam organisasi.
2. Akuntabilitas: Dengan kebijakan yang jelas, lebih mudah untuk menentukan siapa yang bertanggung jawab jika terjadi pelanggaran keamanan.
3. Kepatuhan: Banyak regulasi, seperti GDPR atau HIPAA, memerlukan kebijakan keamanan yang formal sebagai bagian dari kepatuhan.

Tantangan dan Solusi

1. Penerapan: Menerapkan kebijakan keamanan di seluruh organisasi bisa menjadi tantangan. Solusinya adalah pelatihan dan kesadaran keamanan.
2. Pembaruan: Ancaman keamanan selalu berubah, dan kebijakan keamanan harus diperbarui secara reguler. Solusinya adalah audit keamanan yang rutin dan tinjauan kebijakan.
3. Kompleksitas: Kebijakan yang terlalu kompleks atau teknis mungkin tidak mudah dipahami oleh semua karyawan. Solusinya adalah membuat kebijakan yang jelas dan mudah diakses.

Kebijakan keamanan adalah elemen penting dari setiap strategi keamanan yang efektif. Ini tidak hanya menetapkan aturan dan prosedur yang harus diikuti tetapi juga membantu dalam memantau dan mengevaluasi efektivitas program keamanan. Tanpa kebijakan keamanan yang kuat, organisasi berisiko menghadapi inkonsistensi dalam praktek keamanan, kurangnya akuntabilitas, dan potensi pelanggaran regulasi.

6.6 Keamanan Aplikasi dan Data

6.6.1 Keamanan Database

Database adalah repositori informasi yang seringkali berisi data yang sangat sensitif dan berharga. Oleh karena itu, keamanan database adalah salah satu aspek krusial dalam keamanan aplikasi dan data. Ini mencakup berbagai elemen, mulai dari kontrol akses hingga enkripsi data, dan memerlukan pendekatan yang komprehensif untuk memitigasi berbagai jenis risiko.

Jenis-Jenis Ancaman terhadap Database

1. SQL Injection: Serangan ini terjadi ketika perintah SQL yang berbahaya disisipkan ke dalam query database.

2. Data Breach: Akses yang tidak sah ke data, biasanya melalui kelemahan dalam sistem keamanan.
3. *Denial of Service* (DoS): Serangan yang membuat database menjadi tidak tersedia untuk pengguna yang sah.

Contoh Keamanan Database

1. Kontrol Akses: Hanya memberikan akses ke database kepada pengguna atau sistem yang memerlukan akses tersebut, dan membatasi jenis akses yang mereka miliki (misalnya, *read-only, read-write*).
2. Enkripsi Data: Menggunakan enkripsi untuk melindungi data yang disimpan, serta data yang sedang ditransfer antara database dan aplikasi lain.
3. Monitoring dan Auditing: Menggunakan alat untuk memantau akses dan query ke database, serta melakukan audit keamanan secara berkala.

Pentingnya Keamanan Database

1. Integritas Data: Keamanan database yang efektif memastikan bahwa data tidak dapat diubah tanpa otorisasi.
2. Kerahasiaan: Melindungi data dari akses yang tidak sah, sehingga menjaga kerahasiaan informasi yang sensitif.
3. Ketersediaan: Memastikan bahwa database selalu tersedia untuk pengguna yang sah, yang krusial untuk operasional sehari-hari dari banyak organisasi.

Tantangan dan Solusi

1. Kompleksitas: Database modern sangat kompleks dan seringkali terintegrasi dengan berbagai aplikasi dan layanan lain. Solusinya adalah pendekatan keamanan berlapis dan komprehensif.
2. Performa: Beberapa langkah keamanan, seperti enkripsi data, dapat mempengaruhi performa. Solusinya adalah

menyeimbangkan kebutuhan keamanan dengan kebutuhan performa.
3. Insider Threats: Kadang-kadang ancaman bisa datang dari dalam organisasi. Solusinya adalah prinsip "hak akses minimal" dan pemantauan aktivitas.

Keamanan database adalah salah satu aspek paling penting dari keamanan aplikasi dan data. Tanpa langkah-langkah keamanan yang tepat, data sensitif dan berharga bisa menjadi target yang mudah untuk berbagai jenis serangan. Oleh karena itu, keamanan database harus menjadi prioritas utama dalam setiap strategi keamanan informasi, dan memerlukan pendekatan yang komprehensif yang mempertimbangkan berbagai jenis ancaman dan risiko.

6.6.2 Keamanan Aplikasi Web

Aplikasi web telah menjadi bagian integral dari kehidupan sehari-hari dan bisnis, tetapi mereka juga menawarkan vektor serangan yang menarik bagi pelaku kejahatan siber. Keamanan aplikasi web adalah disiplin yang berfokus pada identifikasi dan mitigasi risiko yang terkait dengan aplikasi yang diakses melalui web browser.

Jenis-Jenis Ancaman terhadap Aplikasi Web

1. *Cross-Site Scripting* (XSS): Serangan ini memanipulasi aplikasi web untuk mengeksekusi skrip yang berbahaya di sisi klien.
2. *Cross-Site Request Forgery* (CSRF): Serangan ini memanfaatkan kepercayaan antara browser pengguna dan aplikasi web untuk melakukan tindakan yang tidak sah.
3. *Insecure Direct Object References* (IDOR): Serangan ini terjadi ketika pengguna dapat mengakses objek yang seharusnya tidak bisa mereka akses.

Contoh Keamanan Aplikasi Web

1. *Input Validation*: Memastikan bahwa semua input dari pengguna divalidasi sebelum diproses oleh aplikasi.
2. *Authentication and Authorization*: Menggunakan metode otentikasi yang kuat dan memastikan bahwa pengguna hanya dapat mengakses sumber daya yang mereka berhak akses.
3. *Web Application Firewall* (WAF): Menggunakan firewall khusus yang dirancang untuk melindungi aplikasi web dari berbagai jenis serangan.

Pentingnya Keamanan Aplikasi Web

1. Integritas Data: Melindungi data dari manipulasi yang tidak sah, yang bisa merusak reputasi dan operasional sebuah organisasi.
2. Kerahasiaan: Melindungi informasi sensitif dari akses yang tidak sah, termasuk data pelanggan dan informasi bisnis.
3. Ketersediaan: Memastikan bahwa aplikasi web tetap dapat diakses oleh pengguna yang sah, bahkan di tengah upaya serangan.

Tantangan dan Solusi

1. Kompleksitas dan Evolusi Cepat: Aplikasi web seringkali kompleks dan diperbarui secara reguler, yang bisa memperkenalkan kelemahan baru. Solusinya adalah pengujian keamanan yang berkelanjutan.
2. Integrasi dengan Sistem Lain: Aplikasi web seringkali terintegrasi dengan database atau sistem lain, yang bisa menjadi titik kelemahan. Solusinya adalah memastikan keamanan di seluruh rantai suplai data dan aplikasi.
3. Human Error: Kesalahan konfigurasi atau kode yang buruk bisa memperkenalkan risiko. Solusinya adalah pelatihan dan kesadaran keamanan, serta review kode yang ketat.

Keamanan aplikasi web adalah salah satu aspek krusial dari keamanan informasi yang memerlukan perhatian khusus. Dari validasi input hingga otentikasi dan otorisasi, setiap elemen dari aplikasi web harus dirancang dengan keamanan dalam pikiran. Tanpa pendekatan keamanan yang komprehensif, aplikasi web bisa menjadi titik kelemahan yang serius dalam infrastruktur keamanan sebuah organisasi.

6.6.3 Keamanan Email

Email adalah salah satu bentuk komunikasi yang paling sering digunakan dalam dunia bisnis dan pribadi, tetapi juga merupakan salah satu vektor serangan yang paling umum dalam keamanan siber. Keamanan email melibatkan serangkaian teknik dan teknologi yang dirancang untuk mengamankan akses dan konten email.

Jenis-Jenis Ancaman terhadap Email

1. *Phishing*: Serangan ini melibatkan pengiriman email palsu yang tampaknya berasal dari sumber tepercaya untuk memanipulasi penerima agar memberikan informasi sensitif.
2. *Man-in-the-Middle* (MitM): Serangan ini terjadi ketika pihak ketiga tidak sah memantau atau memanipulasi komunikasi email antara dua pihak.
3. *Malware* dan *Ransomware*: Email sering digunakan sebagai metode pengiriman perangkat lunak berbahaya.

Contoh Keamanan Email

1. Autentikasi: Menggunakan metode seperti SPF, DKIM, dan DMARC untuk memverifikasi identitas pengirim.
2. Enkripsi: Menggunakan protokol seperti S/MIME atau PGP untuk mengenkripsi isi email.

3. *Filtering* dan *Scanning*: Menggunakan solusi keamanan email yang dapat memfilter spam dan memindai lampiran untuk malware.

Pentingnya Keamanan Email

1. Kerahasiaan: Melindungi isi email dari akses yang tidak sah adalah krusial, terutama ketika berkomunikasi mengenai informasi sensitif.
2. Integritas: Memastikan bahwa email yang diterima adalah asli dan belum diubah selama transit.
3. Ketersediaan: Sistem email yang aman juga harus dapat melawan serangan yang bertujuan untuk membuat layanan tidak tersedia, seperti serangan DDoS.

Tantangan dan Solusi

1. Kesadaran Pengguna: Salah satu titik kelemahan terbesar dalam keamanan email adalah pengguna itu sendiri. Solusinya adalah pelatihan keamanan dan kesadaran.
2. Kompleksitas Teknologi: Banyak organisasi menggunakan berbagai solusi keamanan email yang bisa menjadi kompleks. Solusinya adalah integrasi dan otomatisasi.
3. Pembaruan dan Pemeliharaan: Ancaman terhadap keamanan email selalu berubah, memerlukan pembaruan dan pemeliharaan yang konstan. Solusinya adalah monitoring dan audit keamanan yang berkelanjutan.

Keamanan email adalah aspek krusial dari keamanan informasi dan seringkali merupakan titik awal dari berbagai jenis serangan siber. Dari autentikasi pengirim hingga enkripsi isi dan pelatihan pengguna, ada banyak langkah yang harus diambil untuk memastikan keamanan email. Tanpa strategi keamanan email yang efektif, organisasi dan individu berisiko kehilangan data, uang, dan reputasi.

6.7 Pembelajaran Mesin dalam Keamanan Jaringan

6.7.1 Anomali Deteksi

Deteksi anomali adalah salah satu aplikasi paling menjanjikan dari pembelajaran mesin (Machine Learning, ML) dalam keamanan jaringan. Teknik ini melibatkan penggunaan algoritma ML untuk mengidentifikasi pola atau aktivitas yang tidak biasa dalam data jaringan, yang bisa menunjukkan adanya serangan atau kelemahan keamanan.

Jenis-Jenis Anomali

1. Anomali Struktural: Melibatkan perubahan mendadak dalam topologi jaringan atau konfigurasi sistem.
2. Anomali Perilaku: Melibatkan aktivitas yang tidak biasa dari pengguna atau sistem, seperti akses ke banyak file dalam waktu singkat.
3. Anomali Statistik: Melibatkan fluktuasi yang tidak biasa dalam metrik jaringan, seperti lalu lintas data atau latensi.

Contoh Anomali Deteksi

1. Deteksi Serangan DDoS: Algoritma ML dapat dilatih untuk mengenali pola lalu lintas jaringan yang konsisten dengan serangan DDoS.
2. Deteksi Insider Threat: Algoritma dapat mengidentifikasi aktivitas pengguna yang tidak biasa, seperti mengakses data sensitif di luar jam kerja.
3. Deteksi Malware: ML dapat digunakan untuk menganalisis pola dalam lalu lintas jaringan untuk mendeteksi tanda-tanda komunikasi dengan *server Command and Control* (C2).

Pentingnya Anomali Deteksi

1. Deteksi Dini: ML memungkinkan deteksi ancaman dalam tahap awal, seringkali sebelum mereka bisa menyebabkan kerusakan yang signifikan.

2. Otomatisasi: ML dapat memproses volume data yang besar dalam waktu nyata, memungkinkan respon yang lebih cepat terhadap ancaman.
3. Adaptabilitas: Algoritma ML dapat "belajar" dari data baru, memungkinkan mereka untuk beradaptasi dengan ancaman yang berubah.

Tantangan dan Solusi

1. Data yang Tidak Seimbang: Anomali secara alami jarang terjadi, yang bisa membuat algoritma ML sulit untuk mengidentifikasinya. Solusinya adalah teknik resampling atau penggunaan metrik evaluasi yang lebih sesuai.
2. False Positives: Deteksi anomali bisa menghasilkan alarm palsu. Solusinya adalah tuning model dan integrasi dengan sistem keamanan lain untuk verifikasi.
3. Kompleksitas dan Overhead: Algoritma ML yang kompleks bisa memerlukan sumber daya komputasi yang signifikan. Solusinya adalah optimasi algoritma dan hardware yang sesuai.

Anomali deteksi melalui pembelajaran mesin menawarkan pendekatan yang sangat efektif untuk mengidentifikasi ancaman keamanan dalam jaringan. Meskipun ada beberapa tantangan yang harus diatasi, seperti data yang tidak seimbang dan false positives, keuntungan yang ditawarkan membuatnya menjadi komponen penting dari strategi keamanan jaringan modern.

6.7.2 Prediksi Serangan

Prediksi serangan adalah salah satu aplikasi paling inovatif dari pembelajaran mesin dalam keamanan jaringan. Tujuannya adalah untuk memanfaatkan data historis dan analisis perilaku untuk memprediksi jenis serangan yang mungkin terjadi di masa

depan, sehingga memungkinkan organisasi untuk mengambil tindakan pencegahan sebelum serangan benar-benar terjadi.

Jenis-Jenis Data untuk Prediksi

1. Data Historis: Melibatkan analisis data serangan yang telah terjadi di masa lalu untuk mengidentifikasi pola.
2. Data Real-Time: Melibatkan analisis data jaringan dan sistem dalam waktu nyata untuk mendeteksi anomali atau tanda-tanda serangan yang sedang berlangsung.
3. Data Kontekstual: Melibatkan informasi tambahan seperti berita keamanan, laporan intelijen ancaman, atau data dari sensor keamanan lainnya.

Contoh Prediksi Serangan

1. Prediksi Serangan Phishing: Algoritma ML dapat dilatih untuk mengidentifikasi email atau situs web yang tampak mencurigakan berdasarkan karakteristik yang sering ditemukan dalam upaya phishing.
2. Prediksi Serangan DDoS: ML dapat digunakan untuk memonitor lalu lintas jaringan dan memprediksi kemungkinan serangan DDoS berdasarkan pola lalu lintas yang tidak biasa.
3. Prediksi Insider Threat: Algoritma dapat memonitor aktivitas pengguna dan memprediksi risiko serangan dari dalam berdasarkan perubahan perilaku.

Pentingnya Prediksi Serangan

1. Proaktif vs Reaktif: Kemampuan untuk memprediksi serangan memungkinkan tim keamanan untuk bergerak dari posisi reaktif menjadi proaktif.
2. Pengurangan Risiko: Dengan memprediksi serangan, organisasi dapat mengambil langkah-langkah pencegahan untuk mengurangi risiko atau dampak dari serangan tersebut.

3. Efisiensi Sumber Daya: Prediksi yang akurat memungkinkan alokasi sumber daya keamanan yang lebih efisien.

Tantangan dan Solusi

1. Kualitas Data: Prediksi yang akurat memerlukan data yang berkualitas tinggi. Solusinya adalah validasi data dan pembersihan.
2. False Positives/Negatives: Seperti deteksi anomali, prediksi serangan juga rentan terhadap alarm palsu. Solusinya adalah fine-tuning model dan validasi silang.
3. Kompleksitas Model: Model ML yang sangat kompleks bisa sulit diinterpretasikan dan memerlukan banyak sumber daya komputasi. Solusinya adalah pemilihan model yang tepat dan optimasi.

Prediksi serangan adalah salah satu langkah maju paling signifikan dalam keamanan jaringan, memungkinkan organisasi untuk beroperasi dengan lebih proaktif dalam menghadapi ancaman. Meskipun ada beberapa tantangan yang harus diatasi, potensi untuk mengurangi risiko dan meningkatkan efisiensi membuatnya menjadi komponen penting dari strategi keamanan jaringan modern.

6.7.3 Otomasi Respons Keamanan

Otomasi respons keamanan adalah pendekatan yang memanfaatkan teknologi untuk secara otomatis menanggapi dan mengelola ancaman keamanan tanpa intervensi manusia. Ini adalah evolusi dari sistem keamanan tradisional yang memerlukan intervensi manusia dan analisis manual, dan menjadi semakin penting dalam lingkungan keamanan yang semakin kompleks dan dinamis.

Jenis-Jenis Otomasi Respons

1. Otomasi Deteksi: Melibatkan penggunaan algoritma dan teknologi canggih untuk mendeteksi ancaman atau anomali dalam waktu nyata.
2. Otomasi Analisis: Menggunakan teknologi seperti pembelajaran mesin untuk menganalisis data dan konteks sekitar ancaman.
3. Otomasi Tindakan: Melibatkan langkah-langkah otomatis untuk mengisolasi atau memitigasi ancaman.

Contoh Otomasi Respons Keamanan

1. Isolasi Sistem: Jika sistem terdeteksi terinfeksi malware, otomasi bisa digunakan untuk segera mengisolasi sistem dari jaringan.
2. Pemberitahuan dan Eskalasi: Sistem otomatis bisa mengirim pemberitahuan ke tim keamanan atau bahkan memulai prosedur eskalasi jika ancaman serius terdeteksi.
3. Pembaruan dan Patching: Sistem otomatis bisa digunakan untuk menerapkan patch keamanan secara real-time.

Pentingnya Otomasi Respons Keamanan

1. Kecepatan: Dalam dunia keamanan, waktu adalah esensi. Otomasi memungkinkan deteksi dan respons yang hampir instan terhadap ancaman.
2. Efisiensi: Otomasi memungkinkan tim keamanan untuk fokus pada tugas yang lebih kompleks sementara tugas-tugas rutin diotomatisasi.
3. Konsistensi: Otomasi memastikan bahwa prosedur keamanan diikuti dengan konsisten, mengurangi risiko kesalahan manusia.

Tantangan dan Solusi

1. Kompleksitas: Implementasi otomasi memerlukan pemahaman mendalam tentang jaringan dan potensi ancaman. Solusinya adalah pendidikan dan pelatihan tim keamanan.
2. False Positives: Otomasi bisa memicu tindakan yang tidak perlu jika terjadi false positive. Solusinya adalah tuning dan validasi model keamanan.
3. Biaya: Implementasi solusi otomasi bisa mahal. Namun, biaya ini seringkali dapat dibenarkan oleh peningkatan efisiensi dan keamanan.

Otomasi respons keamanan adalah komponen krusial dari strategi keamanan jaringan modern. Meskipun ada beberapa tantangan yang harus diatasi, keuntungan yang ditawarkan oleh otomasi dalam hal kecepatan, efisiensi, dan konsistensi membuatnya menjadi investasi yang berharga.

6.8 Studi Kasus dan Analisis

6.8.1 Studi Kasus Serangan Jaringan

Studi kasus serangan jaringan adalah salah satu cara terbaik untuk memahami bagaimana ancaman keamanan aktual beroperasi dan bagaimana mereka bisa dicegah atau diatasi. Melalui analisis mendalam tentang insiden keamanan yang telah terjadi, kita bisa memperoleh wawasan berharga tentang kelemahan dalam sistem keamanan dan bagaimana mengatasi mereka.

Jenis-Jenis Serangan dalam Studi Kasus

1. Serangan DDoS: Serangan ini bertujuan untuk membuat layanan online menjadi tidak tersedia dengan membanjiri mereka dengan lalu lintas dari banyak sumber.

2. Serangan Phishing: Serangan ini menggunakan pesan palsu untuk memanipulasi individu agar mengungkapkan informasi pribadi atau kredensial keamanan.
3. Serangan Insider: Serangan ini dilakukan oleh individu di dalam organisasi dan bisa sangat merusak karena akses yang mereka miliki.

Contoh Studi Kasus

1. Serangan DDoS pada Dyn: Pada tahun 2016, perusahaan DNS Dyn menjadi target serangan DDoS yang masif, yang mengakibatkan banyak situs web besar menjadi tidak dapat diakses. Ini adalah contoh bagus tentang bagaimana serangan terhadap satu entitas bisa memiliki dampak yang meluas.
2. *Sony Pictures Hack*: Pada tahun 2014, Sony Pictures Entertainment mengalami serangan siber yang mengakibatkan kebocoran data besar-besaran, termasuk email dan informasi karyawan. Ini adalah contoh dari bagaimana serangan siber bisa memiliki konsekuensi finansial dan reputasional yang serius.
3. Serangan SolarWinds: Pada tahun 2020, perusahaan perangkat lunak SolarWinds menjadi korban serangan supply chain yang mempengaruhi ribuan pelanggannya. Ini adalah contoh dari bagaimana serangan bisa meretas melalui rantai pasokan dan mempengaruhi banyak entitas.

Untuk mempelajari Analisa dari studi kasus, maka kita contohkan adanya serangan DDOS pada web E-Commerce. Perusahaan E-commerce "XYZ" adalah salah satu pemain besar di industri ritel online. Pada kuartal keempat tahun 2022, perusahaan ini menjadi target serangan DDoS yang masif, mengakibatkan downtime selama 48 jam dan kerugian finansial yang signifikan.

Kronologi Serangan

1. Fase Pendahuluan: Pada awal Oktober 2022, tim keamanan "XYZ" mulai melihat peningkatan lalu lintas yang tidak biasa tetapi tidak mengidentifikasinya sebagai ancaman serius.
2. Puncak Serangan: Pada 15 Oktober, lalu lintas mencapai puncaknya, membanjiri server dan membuat situs web tidak dapat diakses.
3. Masa Recovery: Meskipun serangan berhenti setelah 48 jam, dampaknya terasa selama beberapa minggu berikutnya dalam bentuk penurunan penjualan dan kepercayaan pelanggan.

Teknik Serangan: Serangan ini menggunakan botnet yang terdiri dari ribuan perangkat IoT yang dikompromi untuk mengirim permintaan ke server "XYZ", sehingga membanjirinya dengan lalu lintas yang tidak dapat dihandle.

Respons dan Mitigasi

1. Identifikasi: Setelah menyadari bahwa ini adalah serangan DDoS, tim keamanan mulai bekerja untuk mengidentifikasi sumber lalu lintas.
2. Mitigasi: Menggunakan Web Application Firewall (WAF) dan layanan mitigasi DDoS eksternal untuk memfilter lalu lintas yang mencurigakan.
3. Pemulihan: Setelah serangan, tim keamanan memperkuat infrastruktur dan memperbarui protokol keamanan untuk mencegah serangan di masa depan.

Dampak

1. Kerugian Finansial: Perusahaan kehilangan sekitar $2 juta dalam penjualan selama periode downtime.
2. Reputasi: Kepercayaan pelanggan menurun, yang terlihat dari penurunan 15% dalam tingkat konversi selama dua minggu berikutnya.

3. Biaya Tambahan: Biaya untuk layanan mitigasi DDoS dan peningkatan infrastruktur keamanan.

Pelajaran yang Dipetik

1. Kesiapsiagaan: Pentingnya memiliki rencana respons keamanan yang efektif dan diuji.
2. Monitoring: Kebutuhan untuk sistem pemantauan yang lebih baik untuk mendeteksi ancaman sebelum mereka menjadi kritis.
3. Redundansi: Pentingnya memiliki infrastruktur yang kuat dan fleksibel yang bisa menangani lonjakan lalu lintas.

Serangan DDoS pada perusahaan "XYZ" menunjukkan betapa pentingnya kesiapsiagaan dan respons yang cepat dalam menghadapi ancaman keamanan. Meskipun perusahaan ini akhirnya bisa pulih, dampaknya terasa dalam bentuk kerugian finansial dan reputasi. Studi kasus ini berfungsi sebagai peringatan keras tentang risiko yang dihadapi oleh perusahaan dalam era digital saat ini.

6.8.2 Analisis Forensik Jaringan

Analisis forensik jaringan adalah proses pengumpulan, pemantauan, dan analisis data jaringan untuk mendeteksi dan/atau menyelidiki kejadian keamanan yang mencurigakan. Ini adalah salah satu aspek krusial dari keamanan siber dan sering digunakan dalam respons insiden untuk memahami sifat dan dampak dari ancaman keamanan.

Tujuan Forensik Jaringan

1. Identifikasi Ancaman: Menentukan jenis serangan atau ancaman yang telah atau sedang terjadi.
2. Atribusi: Menentukan asal-usul serangan, jika memungkinkan.

3. Pemulihan: Memahami bagaimana serangan dilakukan untuk memperbaiki kelemahan dan mencegah insiden di masa depan.

Metodologi

1. Pengumpulan Data: Ini melibatkan pengumpulan log jaringan, paket data, dan informasi lain yang relevan.
2. Pemeriksaan: Analisis awal dari data yang dikumpulkan untuk identifikasi kegiatan yang mencurigakan.
3. Analisis Mendalam: Ini melibatkan penggunaan alat dan teknik forensik untuk memahami sifat dan dampak dari ancaman.
4. Laporan: Membuat laporan yang mendetail tentang temuan, termasuk bukti, kronologi kejadian, dan rekomendasi untuk tindakan lebih lanjut.

Alat dan Teknologi

1. Wireshark: Salah satu alat paling populer untuk analisis paket jaringan.
2. Sysmon: Alat pemantauan dan koleksi data untuk Windows.
3. ELK Stack: Solusi untuk mencari, menganalisis, dan memvisualisasikan data log dalam waktu nyata.

Tantangan dan Solusi

1. Volume Data: Besarnya volume data yang harus dianalisis bisa menjadi tantangan. Solusinya adalah menggunakan alat yang dapat memproses data dalam skala besar.
2. Privasi: Menangani data sensitif memerlukan kepatuhan terhadap regulasi privasi. Solusinya adalah enkripsi dan kontrol akses yang ketat.
3. Keahlian Teknis: Analisis forensik memerlukan keahlian teknis yang signifikan. Solusinya adalah pelatihan dan sertifikasi untuk tim forensik.

Analisis forensik jaringan adalah elemen penting dalam strategi keamanan siber. Dari identifikasi ancaman hingga pemulihan dan pencegahan, forensik jaringan memainkan peran krusial dalam memahami dan mitigasi risiko keamanan. Meskipun ada beberapa tantangan yang harus diatasi, keuntungan yang ditawarkan dalam hal deteksi dan respons terhadap ancaman membuatnya menjadi investasi yang berharga.

Contoh kasus Analisa forensic pada jaringan komputer:

Perusahaan finansial "ABC" mengalami kebocoran data yang mempengaruhi ribuan pelanggannya. Data yang bocor termasuk informasi pribadi dan data transaksi. Tim keamanan internal memutuskan untuk melakukan analisis forensik jaringan untuk mengetahui sumber dan lingkup kebocoran tersebut.

Kronologi Kejadian

1. Deteksi Awal: Sistem keamanan internal melaporkan akses yang tidak sah ke database pelanggan pada tanggal 5 Mei 2023.
2. Pemberitahuan: Tim keamanan diberitahu dan mulai mengumpulkan data untuk analisis forensik.
3. Investigasi: Dari tanggal 6 Mei hingga 20 Mei, tim forensik melakukan analisis mendalam untuk menentukan sumber dan dampak kebocoran.

Metodologi Analisis

1. Pengumpulan Data: Log jaringan, log akses database, dan snapshot trafik jaringan dikumpulkan.
2. Pemeriksaan Awal: Alat seperti Wireshark dan Sysmon digunakan untuk memfilter aktivitas yang mencurigakan.
3. Analisis Mendalam: ELK Stack digunakan untuk analisis data log dalam skala besar.

Temuan

1. Sumber Penetrasi: Ditemukan bahwa akses tidak sah berasal dari alamat IP yang terletak di luar negeri.
2. Metode Serangan: Serangan dilakukan menggunakan teknik SQL Injection.
3. Data yang Terpengaruh: Sekitar 10.000 pelanggan terpengaruh, dengan data yang bocor termasuk nama, alamat email, dan riwayat transaksi.

Tindakan yang Diambil

1. Isolasi dan Mitigasi: Alamat IP yang mencurigakan segera diblokir dan patch keamanan diterapkan untuk menutup celah SQL Injection.
2. Pemberitahuan Pelanggan: Semua pelanggan yang terpengaruh diberitahu dan diminta untuk mengubah kredensial mereka.
3. Perbaikan Keamanan: Protokol keamanan ditingkatkan, termasuk penerapan multi-factor authentication dan pemantauan jaringan yang lebih ketat.

Pelajaran yang Dipetik

1. Kesiapsiagaan: Kebutuhan untuk rencana respons insiden yang lebih efektif.
2. Pemantauan: Pentingnya memiliki alat pemantauan yang dapat mendeteksi ancaman secara real-time.
3. Edukasi: Kebutuhan untuk pelatihan keamanan siber yang lebih baik bagi tim IT dan karyawan lainnya.

Studi kasus ini menunjukkan bagaimana analisis forensik jaringan dapat digunakan untuk mengidentifikasi, memahami, dan merespons insiden keamanan. Meskipun perusahaan "ABC" mengalami kerugian finansial dan reputasional, langkah-langkah yang diambil setelah analisis forensik membantu memitigasi

dampak lebih lanjut dan memperkuat keamanan mereka untuk masa depan.

6.8.3 Solusi dan Rekomendasi

Dalam konteks keamanan jaringan, solusi dan rekomendasi adalah langkah-langkah yang dirancang untuk memitigasi risiko dan memperkuat postur keamanan sebuah organisasi. Berikut adalah beberapa solusi dan rekomendasi yang umumnya dianggap penting dalam industri keamanan jaringan.

Solusi Teknis

1. Firewall: Menggunakan firewall tingkat lanjut yang dapat memfilter lalu lintas berdasarkan aturan yang ditentukan.
2. Antivirus dan Antimalware: Memastikan bahwa semua perangkat dilengkapi dengan perangkat lunak antivirus dan antimalware yang selalu diperbarui.
3. Enkripsi Data: Menggunakan enkripsi untuk melindungi data sensitif, baik saat disimpan maupun saat ditransmisikan.

Solusi Operasional

1. Pemantauan Jaringan: Mengimplementasikan solusi pemantauan jaringan yang dapat mendeteksi aktivitas yang mencurigakan dalam waktu nyata.
2. Pendidikan dan Pelatihan: Melakukan sesi pelatihan keamanan siber untuk karyawan dan tim IT.
3. Pengujian Keamanan: Melakukan pengujian penetrasi dan audit keamanan secara rutin untuk menilai keefektifan langkah-langkah keamanan.

Rekomendasi

1. *Multi-Factor Authentication* (MFA): Mengimplementasikan MFA untuk menambah lapisan keamanan saat mengakses sistem dan data sensitif.

2. Manajemen Patch: Menjaga semua perangkat lunak dan sistem operasi tetap *up-to-date* dengan patch keamanan terbaru.
3. Backup dan Recovery: Membuat dan memelihara rencana backup dan pemulihan data yang komprehensif.

Tantangan dan Solusi

1. Kompleksitas Teknis: Menggunakan alat dan solusi yang user-friendly namun tetap kuat dalam fitur keamanannya.
2. Biaya: Mengalokasikan anggaran yang cukup untuk keamanan siber, mempertimbangkan bahwa biaya serangan bisa jauh lebih besar.
3. Kepatuhan: Memastikan bahwa semua solusi dan rekomendasi mematuhi standar dan regulasi industri yang relevan.

Mengimplementasikan solusi dan rekomendasi yang tepat adalah kunci untuk memitigasi risiko dan memperkuat keamanan jaringan. Ini melibatkan kombinasi dari solusi teknis, operasional, dan kebijakan yang harus disesuaikan dengan kebutuhan dan tantangan unik dari setiap organisasi.

6.9 Analisis Risiko dan Penilaian Keamanan

6.9.1 Metodologi penilaian risiko

Analisis risiko dan penilaian keamanan adalah komponen krusial dalam manajemen keamanan informasi dan seringkali merupakan langkah pertama dalam merancang strategi keamanan yang efektif. Salah satu aspek penting dari proses ini adalah metodologi penilaian risiko, yang memberikan kerangka kerja untuk mengidentifikasi, mengukur, dan memprioritaskan risiko. Metodologi ini biasanya melibatkan beberapa langkah kunci, yang dimulai dengan identifikasi aset dan sumber daya yang perlu

dilindungi. Ini bisa berupa informasi sensitif, perangkat keras, perangkat lunak, atau bahkan reputasi perusahaan.

Setelah aset diidentifikasi, langkah selanjutnya adalah menilai potensi ancaman dan kerentanannya. Ancaman bisa berupa aktor jahat, kesalahan manusia, atau bencana alam, sementara kerentanannya bisa berupa kelemahan keamanan dalam sistem atau proses. Menggabungkan informasi tentang ancaman dan kerentanannya memungkinkan perusahaan untuk menghitung risiko potensial, biasanya dalam bentuk skor atau peringkat.

Selanjutnya, mitigasi risiko perlu diidentifikasi dan diprioritaskan berdasarkan tingkat risiko dan dampak potensial terhadap organisasi. Ini bisa berupa langkah-langkah teknis seperti memperbarui perangkat lunak keamanan, atau kebijakan organisasional seperti pelatihan keamanan untuk karyawan. Setelah langkah mitigasi diidentifikasi, mereka perlu diimplementasikan dan dipantau untuk efektivitasnya, yang seringkali melibatkan audit keamanan dan pemantauan berkelanjutan.

Metodologi penilaian risiko adalah proses terstruktur yang digunakan untuk mengidentifikasi, mengukur, dan memprioritaskan risiko keamanan dalam suatu organisasi atau sistem. Proses ini adalah bagian integral dari manajemen risiko dan keamanan informasi, dan biasanya melibatkan beberapa langkah kunci untuk memastikan bahwa semua aspek keamanan telah dipertimbangkan secara menyeluruh.

1. Identifikasi Aset dan Sumber Daya
   Langkah pertama dalam metodologi penilaian risiko adalah mengidentifikasi aset dan sumber daya yang perlu dilindungi. Ini bisa berupa data pelanggan, kode sumber, perangkat keras, atau bahkan reputasi dan keberlanjutan bisnis. Mengidentifikasi aset ini membantu organisasi

memahami apa yang paling berharga dan rentan terhadap ancaman.

2. Identifikasi Ancaman dan Kerentanan
   Setelah aset diidentifikasi, langkah selanjutnya adalah menilai ancaman dan kerentanannya. Ancaman bisa berupa serangan siber, kesalahan manusia, bencana alam, atau kegagalan sistem. Kerentanan adalah kelemahan dalam sistem atau prosedur yang bisa dieksploitasi oleh ancaman. Mengidentifikasi ancaman dan kerentanan ini memungkinkan organisasi untuk memahami risiko yang dihadapi.
3. Kuantifikasi Risiko
   Langkah ini melibatkan penggunaan metrik atau skala untuk mengukur risiko. Ini bisa berupa skor numerik, peringkat (tinggi, sedang, rendah), atau bahkan model matematika yang lebih kompleks. Tujuannya adalah untuk memberikan ukuran kuantitatif dari risiko yang memungkinkan untuk memprioritaskan tindakan.
4. Identifikasi dan Evaluasi Kontrol Keamanan
   Setelah risiko diidentifikasi dan diukur, langkah selanjutnya adalah mengevaluasi kontrol keamanan yang ada atau yang mungkin diterapkan untuk memitigasi risiko tersebut. Ini bisa berupa kontrol teknis seperti firewall atau enkripsi, kontrol administratif seperti kebijakan dan prosedur, atau kontrol fisik seperti kunci dan akses terbatas.
5. Implementasi dan Pemantauan
   Setelah kontrol keamanan dipilih, mereka perlu diimplementasikan dan dipantau untuk efektivitasnya. Ini seringkali melibatkan pengujian keamanan, audit, dan pemantauan berkelanjutan untuk memastikan bahwa kontrol bekerja seperti yang diharapkan dan bahwa risiko tetap terkendali.

6. Ulasan dan Pembaruan
   Keamanan adalah proses berkelanjutan, dan sebagai bagian dari metodologi penilaian risiko, penting untuk secara rutin meninjau dan memperbarui penilaian. Ini memastikan bahwa penilaian tetap relevan di tengah perubahan lingkungan keamanan dan bisnis.

Dengan demikian, metodologi penilaian risiko adalah alat yang sangat penting dalam keamanan informasi, memungkinkan organisasi untuk membuat keputusan yang terinformasi tentang bagaimana terbaik untuk melindungi aset dan sumber daya mereka. Ini adalah proses yang memerlukan keahlian teknis dan pemahaman yang mendalam tentang bisnis dan lingkungan operasional perusahaan, serta kemampuan untuk memprioritaskan dan membuat keputusan di bawah ketidakpastian. Baik praktisi maupun peneliti di bidang keamanan siber akan menemukan nilai yang besar dalam memahami dan menerapkan metodologi penilaian risiko yang solid sebagai bagian dari strategi keamanan yang lebih luas.

6.9.2 Alat dan teknik

Dalam konteks metodologi penilaian risiko dan keamanan informasi, berbagai alat dan teknik digunakan untuk memfasilitasi proses dari identifikasi risiko hingga implementasi kontrol keamanan. Berikut adalah beberapa alat dan teknik yang umum digunakan:

Alat Analisis Risiko

1. Software Penilaian Risiko: Alat seperti RiskWatch atau FAIR (*Factor Analysis of Information Risk*) digunakan untuk mengkalkulasi dan memodelkan risiko berdasarkan data yang dimasukkan.

2. Matriks Risiko: Ini adalah tabel dua dimensi yang digunakan untuk menilai dan memprioritaskan risiko berdasarkan probabilitas dan dampak.

Teknik Identifikasi Aset dan Ancaman

1. Daftar Periksa (*Checklists*): Daftar periksa keamanan digunakan untuk memastikan bahwa semua aset dan potensi ancaman telah diidentifikasi.
2. Wawancara dan Kuesioner: Menggunakan wawancara atau kuesioner untuk mengumpulkan informasi dari karyawan atau pihak ketiga tentang aset dan ancaman.

Teknik Kuantifikasi Risiko

1. Analisis Biaya-Manfaat (*Cost-Benefit Analysis*): Teknik ini digunakan untuk membandingkan biaya dari kontrol keamanan dengan manfaat yang akan diperoleh dari mitigasi risiko.
2. Metode Monte Carlo: Ini adalah teknik simulasi yang digunakan untuk memodelkan probabilitas dari berbagai hasil dalam proses yang tidak dapat diprediksi dengan pasti.

Teknik Evaluasi Kontrol

1. Pengujian Penetrasi (*Penetration Testing*): Ini adalah pendekatan aktif untuk menguji keamanan suatu sistem dengan mencoba mengeksploitasi kelemahannya.
2. Audit Keamanan: Ini melibatkan pemeriksaan sistematis dari kebijakan keamanan, prosedur, dan kontrol untuk memastikan mereka diimplementasikan dan efektif.

Teknik Pemantauan dan Ulasan

1. Dashboard Keamanan: Ini adalah antarmuka visual yang menampilkan metrik keamanan kunci secara real-time.

2. Log Analisis: Menggunakan alat seperti SIEM (*Security Information and Event Management)* untuk menganalisis log keamanan dan mendeteksi aktivitas yang mencurigakan.

Menggunakan kombinasi dari alat dan teknik ini memungkinkan organisasi untuk melakukan penilaian risiko yang lebih komprehensif dan akurat. Selain itu, mereka juga membantu dalam memonitor efektivitas dari kontrol keamanan yang telah diimplementasikan dan memberikan wawasan untuk perbaikan berkelanjutan. Baik praktisi maupun peneliti di bidang keamanan siber akan menemukan nilai yang besar dalam memahami dan menerapkan alat dan teknik ini sebagai bagian dari metodologi penilaian risiko dan manajemen keamanan informasi.

6.9.3 Kebijakan dan prosedur

Kebijakan dan prosedur keamanan informasi adalah elemen penting dalam membangun dan mempertahankan postur keamanan yang kuat dalam suatu organisasi. Mereka berfungsi sebagai kerangka kerja yang mengatur bagaimana aset informasi dikelola, dilindungi, dan didistribusikan.

Kebijakan Keamanan

Kebijakan keamanan adalah dokumen formal yang merinci prinsip-prinsip, kerangka kerja, dan tanggung jawab keamanan dalam organisasi. Ini biasanya mencakup:

1. Tujuan Keamanan: Menjelaskan tujuan dan sasaran keamanan informasi.
2. Tanggung Jawab: Menentukan siapa yang bertanggung jawab untuk apa, mulai dari tim IT hingga karyawan biasa.
3. Standar dan Pedoman: Menetapkan standar yang harus diikuti, seperti penggunaan enkripsi atau jenis autentikasi yang diperlukan.

4. Kepatuhan: Menjelaskan kebutuhan hukum dan regulasi yang harus dipatuhi oleh organisasi.

Prosedur Keamanan

Sedangkan prosedur keamanan adalah instruksi langkah-demi-langkah yang menjelaskan bagaimana kebijakan harus diimplementasikan dalam praktek sehari-hari. Prosedur biasanya lebih teknis dan spesifik, misalnya:

1. Prosedur Otentikasi: Bagaimana karyawan harus login ke sistem dan jenis otentikasi yang diperlukan.
2. Prosedur Backup Data: Kapan dan bagaimana data harus dibackup, serta siapa yang bertanggung jawab.
3. Prosedur Respon Insiden: Langkah-langkah yang harus diambil jika terjadi pelanggaran keamanan atau insiden lainnya.

Pentingnya Kebijakan dan Prosedur

1. Konsistensi: Mereka membantu memastikan bahwa tindakan keamanan diimplementasikan secara konsisten di seluruh organisasi.
2. Akuntabilitas: Dengan menetapkan tanggung jawab, kebijakan dan prosedur membantu dalam menentukan akuntabilitas jika terjadi pelanggaran keamanan.
3. Kepatuhan: Mereka membantu organisasi memenuhi kebutuhan kepatuhan regulasi dan standar industri.

Kebijakan dan prosedur harus secara rutin ditinjau dan diperbarui untuk memastikan bahwa mereka tetap relevan dan efektif. Ini terutama penting mengingat ancaman keamanan dan teknologi terus berkembang.

Dengan demikian, kebijakan dan prosedur keamanan adalah alat yang sangat berharga untuk praktisi dan peneliti di bidang keamanan siber. Mereka tidak hanya membentuk dasar

dari strategi keamanan informasi tetapi juga memfasilitasi implementasi dan pemantauan keamanan di tingkat operasional.

6.10 Kesimpulan

Buku ini telah membahas berbagai aspek keamanan jaringan, mulai dari dasar-dasar seperti autentikasi dan otorisasi, hingga topik yang lebih kompleks seperti analisis forensik jaringan dan pembelajaran mesin dalam keamanan jaringan. Materi ini dirancang untuk memberikan pemahaman yang komprehensif tentang tantangan, solusi, dan teknologi terkini dalam bidang ini.

Rekomendasi untuk Praktisi

1. Pemantauan Proaktif: Menggunakan alat pemantauan jaringan untuk deteksi ancaman dalam waktu nyata.
2. Pelatihan dan Sertifikasi: Menyediakan pelatihan keamanan siber yang berkelanjutan dan mempertimbangkan untuk mendapatkan sertifikasi dari badan yang diakui.
3. Pengujian Keamanan: Melakukan pengujian penetrasi dan audit keamanan secara rutin untuk mengevaluasi dan memperkuat postur keamanan.

Rekomendasi untuk Peneliti

1. Fokus pada Teknologi Emergent: Melakukan penelitian pada teknologi keamanan baru, seperti blockchain atau AI, yang memiliki potensi untuk mempengaruhi keamanan jaringan.
2. Studi Kasus dan Analisis: Membuat dan mempublikasikan studi kasus tentang insiden keamanan nyata untuk memberikan wawasan praktis dan teoretis.
3. Kolaborasi Interdisipliner: Bekerja sama dengan ahli dari disiplin ilmu lain, seperti psikologi atau hukum, untuk mendapatkan perspektif yang lebih holistik tentang keamanan siber.

Keamanan jaringan adalah bidang yang terus berkembang, dengan ancaman dan solusi yang selalu berubah. Baik praktisi maupun peneliti memainkan peran penting dalam memahami dan mengatasi tantangan ini. Melalui pemahaman yang mendalam dan penerapan solusi yang tepat, kita bisa membuat langkah besar menuju dunia digital yang lebih aman dan terlindungi.

DAFTAR PUSTAKA

Anderson, R. *et al.* 2013. 'Measuring the Cost of Cybercrime', in *The Economics of Information Security and Privacy*. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 265–300. Available at: https://doi.org/10.1007/978-3-642-39498-0_12.

Clarke, R.A. and Knake, R. 2011. *Cyber War: The Next Threat to National Security and What to Do About It*. Ecco.

Morgan, S. 2020. *Cybercrime Damages $6 Trillion By 2021*, *Cybersecurity Ventures*. Available at: https://cybersecurityventures.com/annual-cybercrime-report-2017/ (Accessed: 9 September 2023).

Ring, M. *et al.* 2019. 'A survey of network-based intrusion detection data sets', *Computers and Security*, 86, pp. 147–167. Available at: https://doi.org/10.1016/j.cose.2019.06.005.

Romanosky, S. 2016. 'Examining the costs and causes of cyber incidents', *Journal of Cybersecurity*, p. tyw001. Available at: https://doi.org/10.1093/cybsec/tyw001.

Saridakis, G. *et al.* 2016. 'Individual information security, user behaviour and cyber victimisation: An empirical study of social networking users', *Technological Forecasting and Social Change*, 102, pp. 320–330. Available at: https://doi.org/10.1016/j.techfore.2015.08.012.

Schneier, B. 2016. *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. W. W. Norton & Company.

Stallings, W. and Brown, L. 2018. *Computer Security: Principles and Practice*. 4th edn. Pearson.

Zeltser, L. *et al.* 2002. *Inside Network Perimeter Security: The Definitive Guide to Firewalls, Vpns, Routers, and Intrusion Detection Systems*. Sams.

Zwicky, E.D., Cooper, S. and Chapman, D.B. 2000. *Building Internet Firewalls*. 2nd edn. O'Reilly Media, Inc.

BAB 7
IP ADDRESS DAN SUBNETTING

Oleh Johni S Pasaribu

7.1 Pendahuluan

Pada lapisan network, diperlukan identifikasi setiap perangkat pada Internet sehingga dimungkinkan komunikasi global antar semua perangkat. Hal ini analog dengan sistem telekomunikasi telepon, dimana setiap perangkat telepon memiliki nomor teleponnya masing-masing disamping kode area dan kode negara. Pengidentifikasian dalam lapisan network pada protokol TCP/IP untuk mengidentifikasi setiap perangkat yang terhubung ke Internet adalah disebut dengan Internet address atau IP address. Suatu IP address adalah alamat 32-bit yang unik dan universal yang merupakan koneksi host atau router ke Internet. IP address adalah unik. Unik dalam arti bahwa setiap alamat hanya satu yang terhubung ke Internet dimana tidak pernah mempunyai alamat yang sama pada dua perangkat pada Internet. Akan tetapi, bila terdapat sebuah perangkat mempunyai dua koneksi ke Internet melalui dua jaringan maka tentunya akan terdapat dua alamat. IP address adalah universal yang artinya sistem pengalamatan haruslah dapat diterima oleh setiap host yang ingin koneksi ke Internet (Forouzan, 2007).

Internet Protocol versi 4 menggunakan alamat logis 32-bit. *Internet Protocol version* 4 (IPv4) adalah versi keempat dari *Internet Protocol* (IP). Ini adalah salah satu protokol inti dari metode internetworking berbasis standar di Internet, dan merupakan versi pertama yang digunakan untuk produksi di ARPANET pada tahun 1983. Protokol ini merutekan sebagian besar lalu lintas Internet hingga pada saat ini, meskipun penerapan

protokol penggantinya sedang berlangsung, IPv6. IPv4 menggunakan alamat 32-bit (empat byte), yang membatasi ruang alamat menjadi 4.294.967.296 (2^{32}) atau lebih dari 4 milyar alamat. Pesatnya ledakan internet dan keberadaan jaringan nirkabel dan broadband berkecepatan tinggi telah berkontribusi terhadap menipisnya IPv4. Protokol IPv4 yang dibuat lebih dari tiga dekade lalu dengan ruang alamat sekitar 4 miliar tidak dapat memenuhi kebutuhan internet modern. IANA (*Internet Assigned Numbers Authority)* mengalokasikan potongan terakhir alamat IPv4 pada tanggal 3 Februari 2011 ke Regional Internet Registries yang mengumumkan akhir dari alamat IPv4 (Rajesh Kumar, 2016). Internet Protocol versi 6 juga dikenal sebagai IPng (IP generasi berikutnya) adalah versi terbaru dari IP untuk Internet. IPv6 hadir dengan skema alamat 128 bit, cukup untuk mencakup hampir setiap perangkat yang terhubung di bumi dengan alamat unik global (Dunn, 2002). IPv6 menggunakan alamat 128 bit dengan ruang alamat 2^{128} (kira-kira $3{,}4\times10^{38}$) alamat. Ruang alamat yang begitu besar memungkinkan setiap perangkat dan pengguna di dunia dapat terhubung ke internet (Rajesh Kumar, 2016).

Apa sebenarnya subnetting itu? Subnetting adalah mengambil jaringan IP dan membaginya menjadi jaringan IP yang lebih kecil yang disebut subnetwork, atau subnet. Setiap jaringan IP atau subnet, adalah domain broadcast. Domain broadcast adalah kumpulan perangkat yang dapat menerima lalu lintas broadcast satu sama lain. Lalu lintas broadcast adalah lalu lintas yang dikirimkan ke setiap perangkat di jaringan. Setiap kelas IP dilengkapi dengan subnet mask defaultnya sendiri yang membatasi kelas IP tersebut untuk memiliki Net ID dan Host ID. Classful IP addressing tidak memberikan fleksibilitas untuk memiliki lebih sedikit jumlah Host per jaringan atau lebih banyak jaringan per kelas IP. CIDR atau Classless Inter Domain Routing memberikan fleksibilitas peminjaman bit bagian Host dari alamat IP dan menggunakannya sebagai jaringan dalam jaringan, yang disebut

Subnet. Dengan menggunakan subnet, satu alamat IP Kelas A dapat digunakan untuk memiliki sub-jaringan yang lebih kecil sehingga memberikan kemampuan manajemen jaringan yang lebih baik (Rajesh Kumar, 2016).

7.2 Format IP Address

Pada tahun 1970-an, Departemen Pertahanan AS mengembangkan *Transmission Control Protocol* (TCP), untuk menyediakan fungsi-fungsi lapisan Network dan Transportasi. Ketika hal ini terbukti menjadi solusi yang tidak fleksibel, fungsi-fungsi tersebut dipisahkan - dengan *Internet Protocol* (IP) yang menyediakan layanan lapisan Network, dan TCP menyediakan layanan lapisan Transport.

Bersama-sama, TCP dan IP menyediakan fungsionalitas inti untuk TCP/IP atau rangkaian protokol Internet. IP menyediakan dua layanan lapisan Jaringan dasar (Forouzan, 2007):

1. Pengalamatan logis (*Logical Addressing*) – memberikan alamat unik yang mengidentifikasi host dan jaringan tempat host berada.
2. Perutean (*Routing*) – menentukan jalur terbaik ke jaringan tujuan tertentu, dan kemudian merutekan data sesuai dengan itu.

IP awalnya didefinisikan dalam RFC 760, dan telah direvisi beberapa kali. IP Versi 4 (IPv4) adalah versi pertama yang mengalami penerapan secara luas, dan didefinisikan dalam RFC 791. IPv4 akan menjadi fokus panduan ini. IPv4 menggunakan alamat 32-bit, yang membatasi jumlah kemungkinan alamat menjadi 4,294,967,296. IPv4 pada akhirnya akan digantikan oleh IP Versi 6 (IPv6), karena kurangnya alamat IPv4 yang tersedia.

Fungsi inti dari IP adalah untuk menyediakan pengalamatan logis untuk host. **IP Address** menyediakan struktur hierarki menemukan host secara unik serta pada jaringan mana

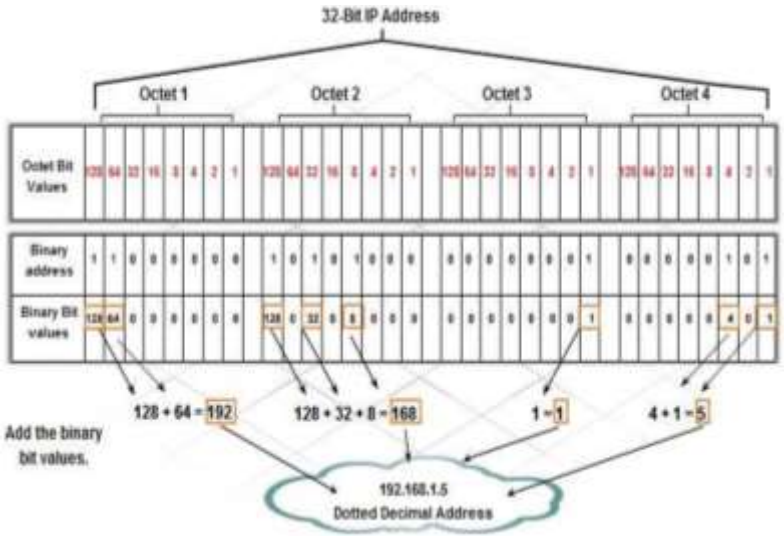
host tersebut berada. Ada dua notasi yang biasa dipakai untuk menunjukkan IP address: biner dan desimal bertitik. Pada notasi biner, IP address dinyatakan dalam 32 bit. Agar alamatnya dapat dibaca, satu atau lebih spasi dibuat antar setiap oktet (8 bit). Setiap oktet sering disebut sebagai byte. Jadi biasanya mendengar IP address sebagai 32-bit address, 4-oktet address, atau 4-byte address. Alamat IP paling sering direpresentasikan dalam **desimal**, dalam format berikut: 158.80.164.3. Alamat IP terdiri dari empat oktet, dipisahkan oleh titik:

First Octet	Second Octet	Third Octet	Fourth Octet
158	80	164	3

Setiap oktet adalah angka 8-bit (byte), sehingga menghasilkan alamat IP 32-bit. Nilai terkecil yang mungkin dari sebuah oktet adalah 0, atau 00000000 dalam biner. Nilai terbesar yang mungkin dari sebuah oktet adalah 255, atau 11111111 dalam biner. Alamat IP di atas yang direpresentasikan dalam biner akan terlihat sebagai berikut:

First Octet	Second Octet	Third Octet	Fourth Octet
10011110	01010000	10100100	00000011

Skema IP Addressing:



Gambar 7.1. Skema IP Addressing

7.3 Konversi Desimal ke Biner

Metode paling sederhana untuk mengkonversi antara desimal dan biner adalah dengan mengingat tabel berikut:

128 64 32 16 8 4 2 1

Untuk mengubah bilangan desimal 172 ke biner, mulailah dari kolom paling kiri. Karena 172 lebih besar dari 128, bit biner tersebut akan disetel ke 1. Selanjutnya, tambahkan nilai kolom berikutnya (128 + 64 = 192). Karena 172 kurang dari 192, bit biner tersebut akan disetel ke 0.

Sekali lagi, tambahkan nilai kolom berikutnya (128 + 32 = 160). Karena 172 lebih besar dari 160, bit biner tersebut akan disetel ke 1. Lanjutkan proses ini hingga kolom dengan bit biner yang disetel ke 1 berjumlah 172:

Decimal	128	64	32	16	8	4	2	1
Binary	1	0	1	0	1	1	0	0

7.4 Konversi Biner ke Desimal

Internet address biasanya dituliskan dalam bentuk desimal agar membuat IP address lebih kompak dan mudah dibaca. Berikut ini menunjukkan IP address dalam notasi desimal bertitik yaitu dengan sebuah titik untuk memisahkan byte-byte(oktet-oktet). Perhatikan bahwa karena setiap byte (oktet) hanya 8 bit, jadi setiap angka dalam notasi desimal bertitik antara 0-255.

Mengonversi dari biner kembali ke desimal bahkan lebih sederhana. Terapkan bilangan biner ke tabel konversi, lalu jumlahkan kolom mana pun dengan bit biner yang disetel ke 1. Misalnya, perhatikan bilangan biner 11110001:

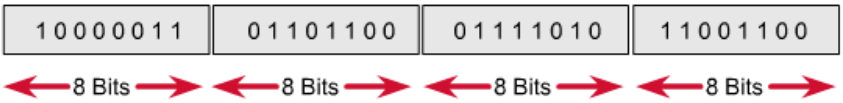
Decimal	128	64	32	16	8	4	2	1
Binary	1	1	1	1	0	0	0	1

Dengan menjumlahkan 128 + 64 + 32 + 16+ 1 maka dapat ditentukan 11110001 sama dengan 241.

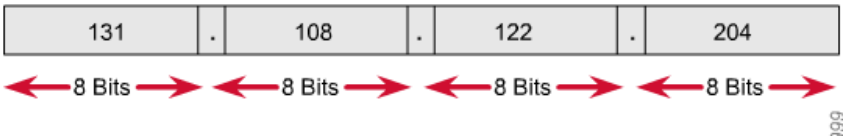
Misalkan diberikan IP Address dalam notasi biner berikut: 10011110.01010000.10100100.00000011 maka dalam notasi desimal: 128.11.3.31.

IP Address terdiri dari 32 bits.

Terbagi menjadi dua bagian: networkID & HostID. 32 bit tersebut dibagi menjadi 4 bagian, setiap bagian terdiri dari 8 bit.



Untuk kemudahan dikonversi menjadi desimal.



Latihan

1. Ubahlah IP address berikut menjadi notasi desimal bertitik:
   a. 10000001 00001011 00001011 11101111
   b. 11000001 10000011 00011011 11111111
   c. 11100111 11011011 10001011 01101111
   d. 11111001 10011011 11111011 00001111

2. Ubahlah IP address berikut menjadi notasi biner:
   a. 111.56.45.78
   b. 221.34.7.82
   c. 241.8.56.12
   d. 75.45.34.78

3. Dari setiap IP address berikut, carilah kesalahan yang ada:
   a. 111.56.045.78
   b. 221.34.7.8.20
   c. 75.45.301.14
   d. 11100010.23.14.67

Kadang-kadang IP adress dalam notasi heksadesimal dimana sering digunakan dalam pemrograman jaringan. Setiap

digit heksadesimal ekivalen dengan empat bit. Ini berarti alamat 32-bit mempunyai digit 8 heksadesimal.

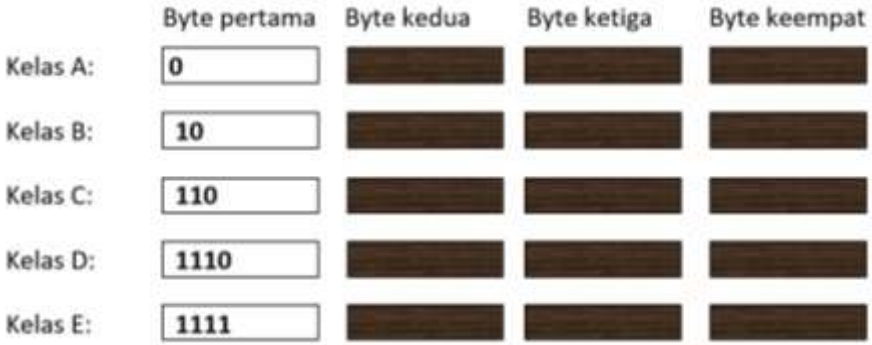
4. Ubahlah IP address berikut menjadi notasi heksadesimal:
   a. 10000001 00001011 00001011 11101111
   b. 11000001 10000011 00011011 11111111

7.5 Classful Addressing

Pada waktu dimulai beberapa puluh tahun yang lalu, IP address menggunakan konsep kelas-kelas dimana disebut dengan classful addressing. Pada pertengahan tahun 1990an, arsitektur baru yaitu classless addressing diperkenalkan untuk menggantikan arsitektur semula. Akan tetapi, sebagian besar Internet masih menggunakan classful addressing karena migrasi cukup lambat. Pada bagian ini, hanya dibahas classful addressing, dimana ruang IP address dibagi menjadi lima kelas: kelas A, kelas B, kelas C, kelas D dan kelas E .

7.5.1 Menggunakan notasi biner

Dalam notasi biner, beberapa bit pertama menunjukkan kelas IP address tersebut seperti pada gambar berikut (Forouzan, 2007):



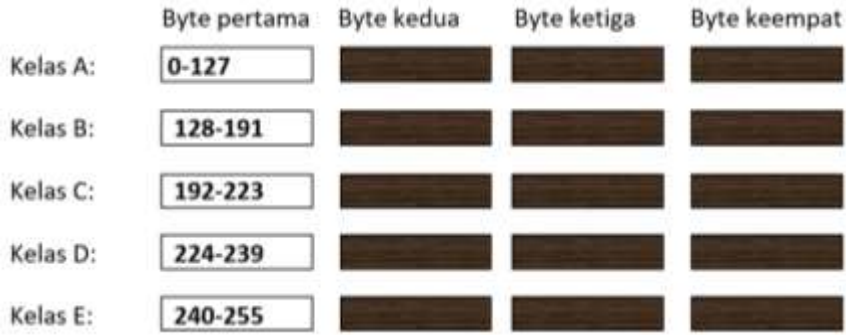
Gambar 7.2. Menemukan kelas dalam notasi biner

Latihan

1. Buktikan bahwa terdapat 2.147.483.648 alamat dalam kelas A?
2. Carilah kelas address berikut:
   a. **0**0000001 00001011 00001011 11101111
   b. **110**00001 10000011 00011011 11111111
   c. **10**100111 11011011 10001011 01101111
   d. **1111**1001 10011011 11111011 00001111

7.5.2 Menggunakan notasi desimal bertitik

Jika alamat diberikan dalam notasi desimal bertitik, kita hanya perlu melihat angka pada byte pertama untuk menentukan kelas alamat tersebut. Setiap kelas mempunyai range alamat yang spesifik. Gambar berikut menunjukkan kelas dalam notasi desimal (Forouzan, 2007).



Gambar 7.3. Menemukan kelas dalam notasi desimal

Hal ini berarti bahwa jika byte pertama (dalam desimal) antara 0-127, maka kelas A. Jika byte pertama antara 128-191, maka kelas B. Dan seterusnya.

1. Carilah kelas untuk address berikut:
   a. **227**.12.14.87
   b. **193**.14.56.22

c. **14**.23.120.8
d. **252**.5.15.111
e. **134**.11.78.56

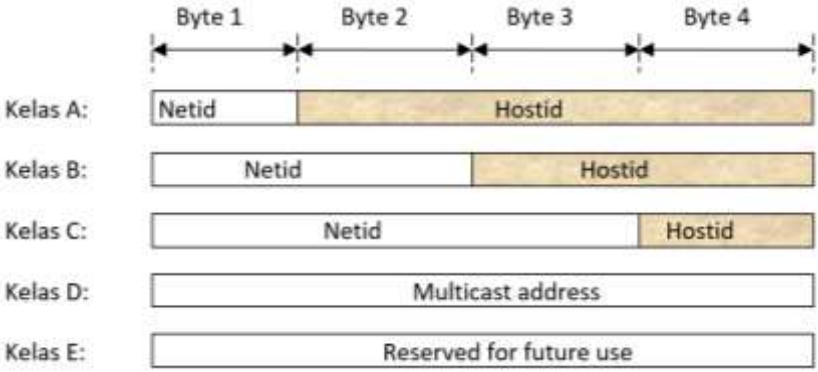
7.5.3 Unicast, Multicast dan Reserved Addresses

Alamat di kelas A, B, dan C ditujukan untuk komunikasi unicast, dari satu sumber ke satu tujuan. Sebuah host harus memiliki setidaknya satu alamat unicast untuk dapat mengirim atau menerima paket. Alamat di kelas D ditujukan untuk komunikasi multicast, dari satu sumber ke sekelompok tujuan. Jika sebuah host termasuk dalam suatu grup atau beberapa grup, host tersebut mungkin memiliki satu atau lebih alamat multicast. Alamat multicast hanya dapat digunakan sebagai alamat tujuan, namun tidak pernah digunakan sebagai alamat sumber. Alamat di kelas E dicadangkan. Ide awalnya adalah menggunakannya untuk tujuan khusus. Mereka hanya digunakan dalam beberapa kasus.
Ada tiga jenis paket IP:

1. Unicast adalah paket yang dikirim dari satu host ke satu host lainnya
2. Multicast adalah paket yang dikirim dari satu host ke sekelompok host
3. Broadcast adalah paket yang dikirim dari satu host ke semua host lain di jaringan lokal

7.5.4 Netid dan Hostid

Pada classful addressing, suatu IP address dalam kelas-kelas A, B dan C terbagi dalam netid dan hostid. Bagian-bagian ini panjangnya berubah sesuai dengan kelasnya. Gambar berikut menunjukkan byte-byte netid dan hostid. Perhatikan bahwa kelas-kelas D dan E tidak terbagi dalam netid dan hostid.



Gambar 7.4. Netid dan hostid

Pada kelas A: berisikan netid (1 byte) dan berisikan hosted (3 byte). Pada kelas B: berisikan netid (2 byte) dan berisikan hosted (2 byte). Pada kelas C: berisikan netid (3 byte) dan berisikan hosted (1 byte).

7.5.5 Network Addresses

Alamat-alamat jaringan (*network addresses*) berperan penting dalam classful addressing. Sebuah network address mempunyai sifat-sifat berikut:

1. Network address adalah alamat pertama dalam blok.
2. Network address menghubungkan jaringan ke Internet. Pada bagian selanjutnya, kita akan mempelajari bahwa router mengarahkan paket berdasarkan alamat jaringan.
3. Dengan network address, kita dapat mengetahui kelas alamat tersebut, blok, dan range alamat-alamat dalam blok.

Latihan

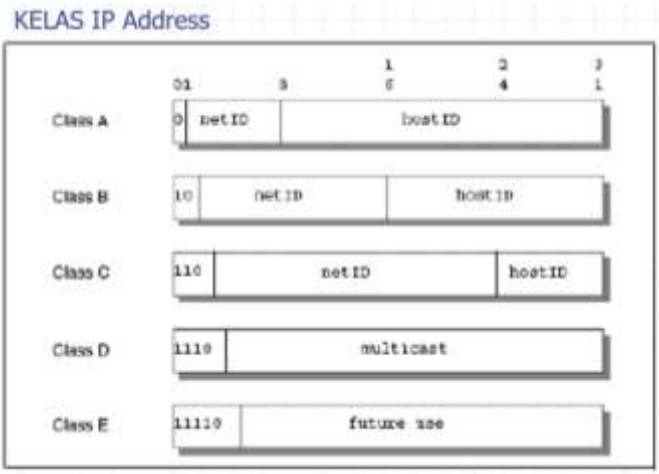
1. Diberikan network address 17.0.0.0, carilah kelas, blok dan range alamat-alamat.
2. Diberikan network address 132.21.0.0, carilah kelas, blok dan range alamat-alamat.

3. Diberikan network address 222.34.76.0, carilah kelas, blok dan range alamat-alamat.

7.5.6 Kelas IP Address

Pembagian kelas berdasarkan 2 hal:

1. Network ID (identitas jaringan)
2. Host ID (identitas hosts: komputer, router, dll.)



Gambar 7.5. Kelas IP Address

Kelas IP Address A (Kelas A):

1. Format: 0nnnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh
2. Net ID: Bit pertama 0, dan 7 bit alamat network (0 – 127)
   Jumlah: 126 Kelas A (0 dan 127 dicadangkan)
   Range IP: 1.xxx.xxx.xxx s/d 126.xxx.xxx.xxx
3. Host ID: 24 bit untuk alamat host.
4. Jumlah Host: 16.777.214
5. Jadi bila IP: 115.23.5.123 berarti Net Id = 115, Host Id= 23.15.123

Kelas IP Address B (Kelas B):

1. Format: 10nnnnnn.nnnnnnnn.hhhhhhhh.hhhhhhhh
2. Net ID: 2 Bit pertama 10, dan 14 bit alamat network
   Jumlah: 16382 (64*256-2) Kelas B
   Range IP: 128.nnn.xxx.xxx s/d 191.nnn.xxx.xxx
3. Host ID: 16 bit untuk alamat host
4. Jumlah Host: 65.532
5. Jadi bila IP: 159.23.15.123 berarti Net Id = 159.23, Host Id= 15.123

Kelas IP Address C (Kelas C):

1. Format: 110nnnnn.nnnnnnnn.nnnnnnnn.hhhhhhhh
2. Net ID: 3 Bit pertama 110, plus 21 bit berikutnya
   Jumlah: 2.097.152 Kelas C
   Range IP: 192.nnn.nnn.xxx s/d 223.nnn.nnn.xxx
3. Host ID: 8 bit untuk alamat host
4. Jumlah Host: 254
5. Jadi bila IP: 198.23.5.123 berarti Net Id = 198.23.5, Host Id= 123

Kelas IP Address D (Kelas D):

Ruang alamat multicast (RFC 1112). Tidak dikenal network bit dan host bit.

1. Format:
   1110mmmm.mmmmmmmm.mmmmmmmm.mmmmmmmm
2. 4 Bit pertama: 1110 (Byte awal: 224 – 247)
   Bit Multicast: 28 bit

Kelas IP Address E (Kelas E):
Dicadangkan untuk keperluan experimental (tidak untuk umum).

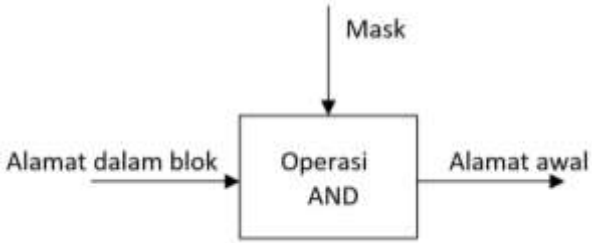
1. Format:
   1111mmmm.mmmmmmmm.mmmmmmmm.mmmmmmmm
2. 4 Bit pertama: 1111 (Byte awal: 248 – 255)
   Bit Multicast: 28 bit

7.5.7 Mask

Pada bagian sebelumnya dikatakan bahwa jika network address diberikan, akan ditemukan blok dan range alamat dalam blok tersebut. Bagaimana sebaliknya? Jika suatu alamat diberikan, dapatkah diperoleh alamat jaringan (alamat pertama dalam blok)? Hal ini penting karena untuk mengarahkan paket ke jaringan yang benar, router perlu memisahkan network address dari alamat tujuan (alamat host) pada packet header.

Satu cara menemukan alamat jaringan adalah pertama-tama memperoleh kelas IP address dan netid. Kemudian kita men-set hostid nol untuk memperoleh alamat jaringan. Misalnya, jika diberikan alamat 134.45.78.2, kita dapat memastikan bahwa alamat tersebut adalah kelas B. Netid adalah 134.45 (2 byte) dan network address adalah 134.45.0.0. Prosedur umum yang digunakan dengan mask untuk memperoleh network address dari alamat yang diberikan.

Mask adalah suatu bilangan biner 4 byte (32-bit) yang memberikan alamat pertama dalam blok (network address) jika bit-bit pada mask dilakukan operasi AND dengan alamat pada blok. Berikut diberikan konsep masking:



Gambar 7.6. Konsep masking

7.5.8 Default Mask

Pada classful addressing, ada tiga mask, masing-masing satu untuk setiap kelas. Tabel berikut menunjukkan mask untuk setiap kelas. Pada kelas A, mask adalah delapan angka 1 dan dua puluh empat angka 0. Pada kelas B, mask adalah enam belas angka 1 dan enam belas angka 0. Pada kelas C, mask adalah dua puluh empat angka 1 dan delapan angka 0. Angka 1 menunjukkan netid; angka 0 menentukan hostid. Ingat bahwa network address dalam setiap kelas adalah netid dengan hostid semuanya 0. Berikut diberikan default mask untuk setiap kelas.

Tabel 7.1. Default mask

Class	*Mask dalam biner*				*Mask dalam desimal bertitik*	*Menggunakan Slash*
A	**11111111**	00000000	00000000	00000000	**255**.0.0.0	**/8**
B	**11111111**	11111111	00000000	00000000	**255.255**.0.0	**/16**
C	**11111111**	11111111	11111111	00000000	**255.255.255**.0	**/24**

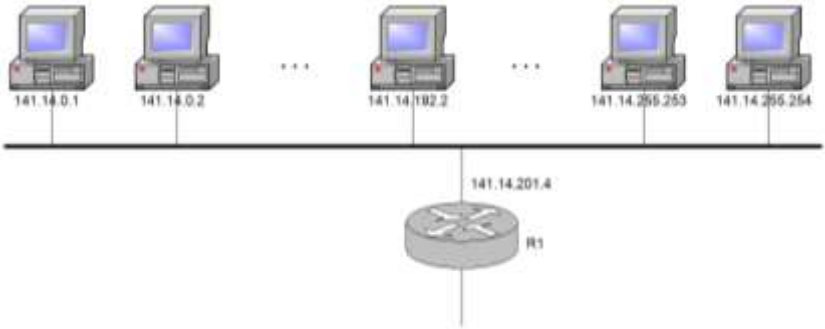
Perhatikan bahwa banyaknya angka 0 sesuai dengan banyaknya 0 pada hostid dan banyaknya angka 1 dalam setiap kelas sesuai dengan banyaknya bit pada netid. Dengan kata lain, bila suatu mask dilakukan operasi AND dengan suatu alamat, netid akan muncul dan hostid diset 0.

Latihan

1. Diberikan alamat 23.56.7.91 dan default mask kelas A, carilah alamat awal (network address).
2. Diberikan alamat 132.6.17.85 dan default mask kelas B, carilah alamat awal (network address).
3. Diberikan alamat 201.180.56.5 dan default mask kelas C, carilah alamat awal (network address).

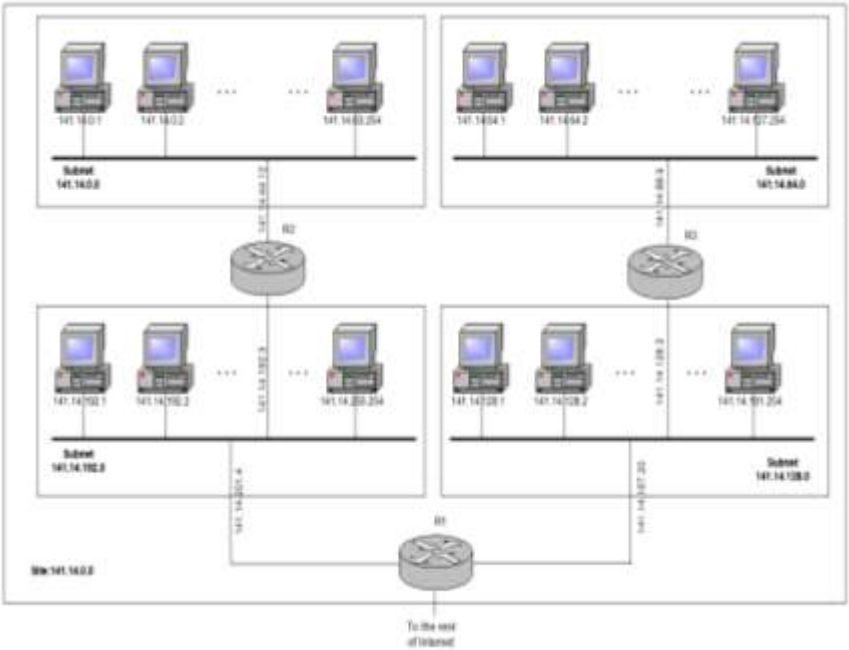
7.6 Subnetting

Pada subnetting, satu jaringan dibagi menjadi beberapa sub-sub jaringan yang lebih kecil dengan setiap subjaringan (subnet) mempunyai alamat subnet sendiri. Seperti yang telah dipelajari sebelumnya, sebuah IP address panjangnya 32 bit. Satu bagian dari alamat itu menunjukkan network (netid), dan satu bagian lagi menunjukkan host (hostid) pada jaringan. Ini berarti terdapat hirarkhi dalam pengalamatan IP address. Pertama-tama harus mendapatkan jaringan dulu dengan menggunakan bagian pertama dari alamat (netid) dalam mencapai suatu host pada Internet. Setelah itu baru mencapai host untuk bagian kedua (hostid). Dengan kata lain, IP address didisain berdasarkan dua tingkat hirarkhi. Akan tetapi, dalam banyak hal, dua tingkat hirarkhi ini tidak cukup. Misalkan suatu perusahaan dengan alamat jaringan 141.14.0.0 (blok kelas B). Perusahaan mempunyai dua tingkat hirarkhi pengalamatan, tetapi seperti pada gambar berikut, tidak dapat mempunyai lebih dari satu jaringan fisik.



Gambar 7.7. Jaringan dengan dua tingkat hierarki

Default mask kelas B ini adalah 255.255.0.0 yang berarti bahwa terdapat semua alamat mempunyai 16 bit yang sama (net id). Bit-bit lainnya menunjukkan alamat-alamat yang berbeda pada jaringan (host id). Jadi alamat jaringan (*network address*) adalah alamat pertama dalam blok; hostid adalah semua bernilai 0 pada alamat jaringan. Dengan cara ini, perusahaan tersebut dibatasi dengan dua tingkat hirarkhi. Host-host tidak dapat dibagi menjadi beberapa kelompok; semua host berada pada tingkat yang sama. Perusahaan tersebut mempunyai satu jaringan dengan banyak host. Solusi untuk masalah ini adalah subnetting, membagi satu jaringan menjadi jaringan-jaringan lebih kecil yang disebut dengan subnetwork (subnet). Misalkan, gambar berikut menunjukkan jaringan dari gambar sebelumnya yang dibagi menjadi empat subnet, seperti ditunjukkan pada gambar berikut.



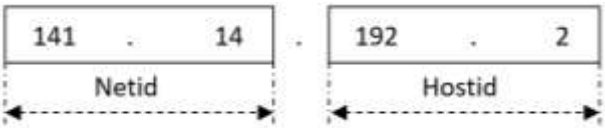
Gambar 7.8. Jaringan dengan tiga tingkat hierarki (subnetting)

Subnet-subnet terlihat sebagai sebuah jaringan tunggal kepada jaringan Internet. Paket yang ditujukan untuk host 141.14.192.2 melalui router R1. Router R1 tahu bahwa jaringan 141.14 terbagi menjadi subnet-subnet. Router R1 tahu bahwa paket harus diberikan ke subnet 141.14.192.0.

7.6.1 Tiga tingkat Hierarki

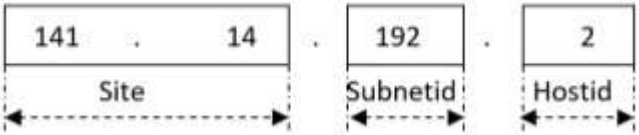
Menambahkan subnet-subnet membentuk tingkat intermediate dari hirarkhi pada sistem IP addressing. Sehingga diperoleh tiga tingkat: site, subnet, dan host. Site adalah tingkat pertama. Tingkat kedua adalah subnet. Host adalah tingkat ketiga; hal ini menunjukkan koneksi host ke subnet. Lebih jelasnya lihat gambar berikut.

Pengalamatan dalam sebuah jaringan tanpa subnetting:



Gambar 7.9. Alamat dalam jaringan tanpa subnetting

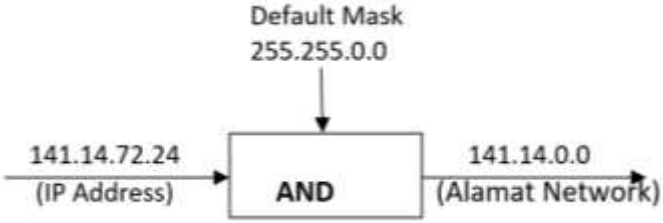
Pengalamatan dalam sebuah jaringan dengan subnetting:



Gambar 7.10. Alamat dalam jaringan dengan subnetting

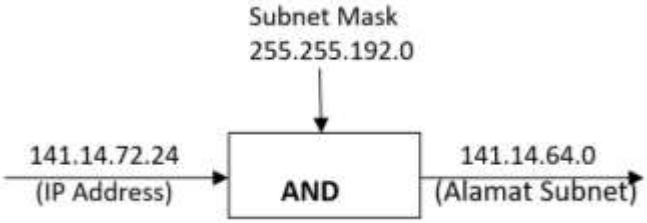
7.6.2 Subnet Mask

Kita telah mendiskusikan network mask (*default mask*) pada bagian sebelumnya. Network mask digunakan bila sebuah jaringan tidak dibagi. Network mask digunakan untuk menemukan alamat pertama di dalam blok atau alamat jaringan. Namun, bila suatu mask dibagi, situasinya berbeda. Disini harus ada subnet mask. Subnet mask mempunyai lebih banyak angka 1 dibandingkan dengan netmask (*default mask*). Gambar berikut menunjukkan situasi tanpa subnetting dan dengan subnetting.
Tanpa subnetting:



Gambar 7.11. Mencari alamat network

Dengan subnetting:



Gambar 7.12. Mencari alamat subnet

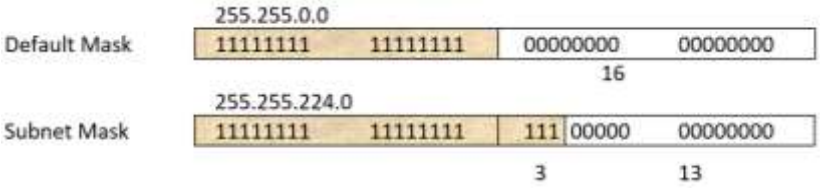
Diberikan IP address, kita dapat menemukan alamat subnet sama seperti kita memperoleh alamat jaringan pada bagian sebelumnya. Disini mask dihubungkan dengan address.

Latihan

1. Bila alamat tujuan (IP Address) adalah 200.45.34.56 dan subnet mask adalah 255.255.255.240, tentukan berapa alamat subnet?
2. Jika alamat tujuan (IP Address) adalah 19.30.84.5 dan subnet mask adalah 255.255.192.0, tentukan berapakah alamat subnet?

Banyaknya angka 1 dalam suatu default mask sudah ditentukan (8, 16, atau 24). Pada subnet mask banyaknya angka 1 lebih banyak dari banyaknya angka 1 pada default mask. Dengan kata lain, untuk sebuah subnet mask, kita mengubah beberapa angka 0 pada bagian kiri default mask menjadi angka-angka 1 sehingga menjadi sebuah subnet mask. Gambar berikut menunjukkan perbedaan antara default mask kelas B dan sebuah subnet mask untuk blok yang sama.

Perbandingan antara sebuah default mask dan sebuah subnet mask:



Gambar 7.13. Subnet mask

7.6.3 Mendisain Subnet-subnet

Banyaknya subnet dapat diperoleh dengan menghitung tambahan angka 1 kepada default mask untuk membuat subnet mask. Misalnya, banyaknya tambahan angka 1 pada gambar di atas adalah 3, sehingga banyaknya subnet adalah 2^3 atau 8.

Banyaknya alamat per subnet dapat diperoleh dengan menghitung banyaknya angka 0 dalam subnet mask. Misalnya, pada gambar di atas banyaknya angka 0 adalah 13, karena itu banyaknya alamat dalam setiap subnet adalah $2^{13} = 8192$.

Untuk lebih baik memahami subnetting, berikut ditunjukkan contoh bagaimana seorang manajer jaringan mendisain subnet-subnet untuk perusahaannya. Hal ini memerlukan beberapa langkah:

1. Menentukan Banyaknya Subnet-subnet
   Langkah pertama dalam mendisain adalah menentukan banyaknya subnet yang diperlukan untuk suatu perusahaan. Keputusan ini bergantung pada beberapa faktor: lokasi fisik (banyaknya lantai), banyaknya departemen, banyaknya host yang diperlukan untuk setiap subnet, dan seterusnya. Agar operasi masking yang lebih tepat, direkomendasikan banyaknya subnet adalah pangkat 2 (0, 2, 4, 8, 16, 32, dst). Perhatikan bahwa pilihan angka 0 berarti tidak ada subnetting.
2. Menentukan Subnet Mask
   Langkah kedua adalah menentukan subnet mask. Aturan-aturan berikut dapat membantu kita dalam menentukan subnet mask dengan mudah:

a. Tentukan banyaknya angka 1 dalam default mask
b. Tentukan banyaknya angka 1 yang menunjukkan subnet-subnet
c. Tambahkan banyaknya angka 1 pada langkah nomor 2 ke langkah nomor 1
d. Cari banyaknya angka 0 dengan mengurangi banyaknya angka 1 dalam langkah no 3 dengan 32

3. Menentukan Range Address dalam Setiap Subnet
   Setelah menentukan subnet mask, network administrator dapat mencari range address untuk setiap subnet. Dua metode digunakan untuk mendapatkan alamat pertama dan alamat terakhir dalam setiap subnet. Pada metode pertama, kita mulai dengan subnet pertama. Alamat pertama dalam subnet pertama adalah alamat pertama dalam blok. Kemudian kita menambahkan banyaknya alamat-alamat dalam setiap subnet untuk mendapatkan alamat terakhir. Kemudian kita tambahkan satu pada address untuk memperoleh alamat pertama dalam subnet berikutnya. Kemudian prosedur tadi diulangi untuk subnet ini, demikian seterusnya. Pada metode kedua, dimulai dengan subnet terakhir. Alamat terakhir dalam subnet terakhir adalah alamat terakhir dalam blok. Kemudian dengan menggunakan mask untuk memperoleh alamat pertama dalam subnet ini. Kemudian kita mengurangi satu dari alamat ini untuk mendapatkan alamat terakhir subnet terakhir yang kedua. Kemudian prosedur tadi diulangi untuk subnet ini, demikian seterusnya.

Latihan

1. Sebuah perusahaan diberikan site address 201.70.64.0 (kelas C). Perusahaan membutuhkan enam subnet. Coba disain subnet-subnetnya.
2. Sebuah perusahaan diberikan site address 181.56.0.0 (kelas B). Perusahaan membutuhkan 1000 subnet. Coba disain subnet-subnetnya.

DAFTAR PUSTAKA

Dunn, T. 2002. 'The IPv6 Transition', *IEEE Internet Computing*, 6(3), pp. 11–13.

Forouzan, B. A. 2007. *Data Communications and Networking*. 4th Editio. McGraw-Hill Companies, Inc.

Rajesh Kumar, P. R. S. 2016. 'Computer Network - IP Address & Subnetting', *International Journal of Engineering and Advanced Technology (IJEAT)*, 5(4).

BAB 8
LAN DAN WAN

Oleh Rudi Sutomo

8.1 Pendahuluan

Lokal Area Network (LAN) dan *Wide Area Network* (WAN) adalah dua jenis jaringan komputer yang sangat penting untuk komunikasi kontemporer. Kami akan menjelaskan perbedaan antara keduanya, karakteristik utama, komponen, dan manajemen yang terlibat. Memahami LAN dan WAN adalah penting dalam mengelola infrastruktur jaringan yang efisien dan aman.

8.2 LAN (*Local Area Network*)

8.2.1 Pengertian LAN

Jaringan komputer lokal, juga disebut LAN, mencakup area terbatas, seperti kampus, bangunan, atau lokasi fisik lainnya. LAN memungkinkan perangkat-perangkat seperti komputer, printer, dan server untuk berkomunikasi dan berbagi sumber daya secara efisien dalam jarak yang dekat. Salah satu konsep kunci dalam LAN adalah topologi, yang menggambarkan cara perangkat dalam jaringan terhubung satu sama lain.

Jaringan komputer lokal, juga dikenal sebagai LAN, adalah jaringan komputer yang mencakup area yang lebih kecil, seperti gedung, kantor, kampus, rumah, sekolah, atau tempat lain. Kebanyakan LAN saat ini menggunakan perangkat switch yang berbasis pada teknologi IEEE 802.3 Ethernet dan memiliki kecepatan transfer data 10, 100, atau 1000 Mbit/s selain teknologi Ethernet dan 802.11b. (juga dikenal sebagai Wi-fi) juga sering digunakan untuk membentuk LAN. Hotspot adalah tempat-tempat yang terhubung ke teknologi Wi-Fi. Pada sebuah LAN, setiap node

atau komputer memiliki kapasitas komputasi yang berbeda dari konsep dump terminal. Selain itu, setiap komputer memiliki kemampuan untuk mengakses sumber daya LAN yang diatur.Perangkat seperti printer atau data dapat menjadi sumber daya.

Seorang pengguna pada LAN juga dapat berbicara dengan orang lain dengan aplikasi yang sesuai. Sebuah network atau jaringan adalah kumpulan sistem komputer yang terletak di dalam satu gedung, kompleks gedung, atau kampus. Mereka tidak menggunakan media komunikasi umum seperti telepon, tetapi pemilik LAN yang mengatur dan menggunakan media tersebut. Menurut definisi sebelumnya, sebuah LAN dibatasi secara fisik. Semua komputer yang terhubung ke jaringan, juga dikenal sebagai LAN, memiliki kemampuan untuk berkomunikasi atau bertukar data satu sama lain. Kerjasama ini semakin berkembang dari hanya berbagi data hingga penggunaan peralatan bersama. LAN yang sering menggunakan hub/switch akan mengikuti prinsipnya. Hub hanya memiliki satu domain collision dalam hal ini, sehingga penyampaian data dikirim secara broadcast. Selain itu, jika salah satu port sibuk, port-port lain harus menunggu karena hub tidak tahu alamat tujuan (Tanenbaum & Wetherall, 2014).

8.2.2 Tipe Jaringan LAN

Topologi LAN mengacu pada pola fisik koneksi antar perangkat dalam jaringan. Beberapa topologi umum termasuk topologi bus, star, ring, dan mesh. Topologi ini memiliki karakteristik, kelebihan, dan kekurangan masing-masing. Ada banyak jenis LAN dalam jaringan, beberapa di antaranya adalah sebagai berikut. (Komputasi & Jaringan, 2018):

1. **ARCNet (*Attached Resource Computer Network*)**

   ARCNet menggunakan protokol yang dibuat sendiri oleh perusahaan datapoint; itu tidak menggunakan protokol IEEE yang biasa digunakan pada jaringan. Menurut kartu jaringan

yang digunakan, ARCNet berimpedansi rendah (low impedance) dan ARCNet berimpedansi tinggi (high impedance). Jika media transmisi data adalah kabel koaksial RG-62 atau kabel UTP, jaringan ARCNet dapat mencapai kecepatan maksimum 2,5 Mbps. Jaringan ARCNet juga menggunakan metode akses pelewatan token, juga dikenal sebagai token passing. Bit tanda berputar, yang merupakan token, bergerak melalui stasiun jaringan. Setiap workstation harus menunggu sampai workstation lain mendapat giliran untuk memperoleh token.

2. Token Ring

IBM (*Institute Business Machines*) adalah pencipta pertama jaringan token ring. Semua workstation terhubung melalui kabel berbentuk cincin. Setiap node harus terhubung ke konsentrator atau hub yang disebut MAU atau MSAU (*Multi Station Access Unit*). Dalam jaringan token ring, pelewatan token adalah metode akses yang digunakan. Bit tanda yang berputar di sekitar stasiun jaringan disebut token. Setiap workstation memiliki hak untuk mengirim data jika mereka menerima token. Jika tidak, workstation lain harus menunggu sampai mereka mendapat giliran untuk mendapatkan token. IBM membuat kabel untuk jaringan token ring. Kartu jaringan 4 Mbps dan 16 Mbps berbeda. Kartu jaringan 4 Mbps hanya dapat bekerja pada kecepatan 4 Mbps, sementara kartu jaringan 16 Mbps dapat bekerja pada kecepatan 4 Mbps dan 16 Mbps.

3. FDDI (*Fiber Distributed Data Interface*)

FDDI adalah jenis jaringan yang biasanya digunakan untuk menghubungkan dua atau lebih LAN melalui jaringan serat berkecepatan tinggi (SDH). Metode akses dalam jaringan ini adalah pelewatan token. Kecepatan tinggi jaringan FDDI adalah salah satu keuntungan utamanya. Ini dapat dicapai dengan kecepatan 100 Mbps dengan kabel serat optik.

4. **ATM (*Asynchronous Transfer Mode*)**

ATM adalah jaringan yang dapat mengirimkan data dalam bentuk paket kecil. Ini berbeda dengan jaringan lain yang dapat mengirimkan data dalam bentuk paket yang panjang. Kecepatan maksimal adalah 155 Mbps jika Anda menggunakan jaringan ATM (singkatan dari Asynchronous Transfer Mode). ATM biasanya digunakan untuk menghubungkan dua atau lebih LAN, dan ISP (*Internet Service Provider*) sering menggunakan ATM untuk mendukung kecepatan akses internet yang tinggi untuk penggunanya. ATM dapat menggunakan kabel serat optik atau kabel UTP sebagai media transmisi.

5. **Local Talk**

Local Talk adalah jaringan pertama untuk komputer Macintosh yang dikembangkan oleh Apple Computer Inc., yang menggunakan metode CSMA/CA (*Carier Sense Multiple Access with Collision Avoidance*). Jaringan ini menggunakan adapter Local Talk dan kabel TP khusus, yang memungkinkan berbagai komputer terhubung melalui port serial. Kecepatan transmisi data hanya 230 Kbps adalah kelemahan jaringan Local Talk.

6. **Ethernet**

Jaringan Ethernet menjadi populer karena lebih cepat, murah, dan mudah diinstal. Standar IEEE 802.3 untuk jaringan Ethernet dibuat oleh IEEE dan mengatur cara komponen berinteraksi satu sama lain dan mengkonfigurasi jaringan. Jenis jaringan Ethernet termasuk yang berikut: 10Base-5 menggunakan kabel koaksial tebal (RG-8); 10Base-2 menggunakan kabel koaksial tipis (RG-58); 10Broad-36 menggunakan kabel broadband; 10Base-T menggunakan kabel UTP kategori 3; dan 10Base-F menggunakan kabel serat optik.

Standar Fast Ethernet IEEE 802.3u dirancang untuk jaringan Ethernet yang membutuhkan kecepatan transmisi

yang lebih tinggi. Standar ini mengembangkan standar jaringan Ethernet 802.3 dan mengubah struktur kabel untuk meningkatkan kecepatan jaringan Ethernet dari 10 Mbps menjadi 100 Mbps. Jaringan 100Base-TX menggunakan kabel UTP kategori 5, jaringan 100Base-FX menggunakan kabel serat optik, dan jaringan 100Base-T4 menggunakan dua kabel UTP kategori 5.

Standar 100Base-TX kompatibel dengan 10Base-T Gigabit Ethernet, yang menggunakan standar IEEE sumber 802.3z, yang merupakan evolusi berikutnya dalam jaringan Ethernet. Sistem jaringan ini memiliki kecepatan transmisi data hingga 1000 Mbps. Dua jenis jaringan ini adalah 1000Base-X, yang menggunakan kabel serat optik dan twinax, dan 1000Base-T, yang menggunakan kabel UTP kategori 5e. Jaringan Ethernet saat ini baru dikembangkan dan memiliki kecepatan transmisi data hingga 10.000 Mbps. Untuk jaringan ini, Intel telah membuat kartu jaringan.

7. WLAN (Wireless LAN)

Jaringan WLAN adalah jaringan LAN yang menggunakan gelombang elektromagnetik untuk mengirim data daripada kabel. Pada awalnya, jaringan WLAN hanya dapat mengirim data pada kecepatan hingga 2 Mbps, tetapi kemudian diperbaiki sehingga dapat mengirim data pada kecepatan hingga 11 Mbps. Telah mengalami perubahan waktu, jaringan WLAN telah diperbaiki lagi sehingga mampu mengirim data pada kecepatan hingga 11 Mbps.

Perkembangan terbaru memungkinkan jaringan WLAN mengirimkan data dengan kecepatan hingga 180 Mbps. Jaringan ini membutuhkan peraltan NIC khusus dipasang di slot PCI, USB, atau PCMCIA. Antena menggantikan port kabel pada NIC. Semua peralatan yang terhubung ke jaringan WAN memiliki kemampuan untuk berhubungan satu sama lain

secara mandiri atau melalui Point Access Wireless, atau WAP, yang berfungsi sebagai hub atau konsentrator

Jaringan nirkabel, juga dikenal sebagai jaringan nirkabel, mendistribusikan informasi melalui gelombang radio sebagai media transisi yang diatur untuk bekerja pada frekuensi tertentu secara standar. Jaringan nirkabel bergantung pada kenyamanan pengguna dan mobilitas mereka untuk tetap terkoneksi ke jaringan (Maulana & Fauzi, 2018).

IEEE Standard	Maximum Speed	Frequency	Backwards Compatible
802.11	2 Mb/s	2.4 GHz	—
802.11a	54 Mb/s	5 GHz	—
802.11b	11 Mb/s	2.4 GHz	—
802.11g	54 Mb/s	2.4 GHz	802.11b
802.11n	600 Mb/s	2.4 GHz and 5 GHz	802.11a/b/g
802.11ac	1.3 Gb/s (1300 Mb/s)	5 GHz	802.11a/n
802.11ad	7 Gb/s (7000 Mb/s)	2.4 GHz, 5 GHz, and 60 GHz	802.11a/b/g/n/ac

Gambar 8.1. Standarisasi IEEE 802.11
(sumber : https://multimedia-howto.blogspot.com/2020/04/wifi-standar-80211-dan-wifi-spectrum.html)

Jaringan nirkabel, juga dikenal sebagai jaringan nirkabel, mengirimkan informasi melalui gelombang radio sebagai media transisi yang diatur untuk bekerja pada frekuensi tertentu secara standar. Jaringan nirkabel bergantung pada seberapa mudah pengguna terhubung ke jaringan dan seberapa mudah mereka dapat mengaksesnya (Maulana & Fauzi, 2018).

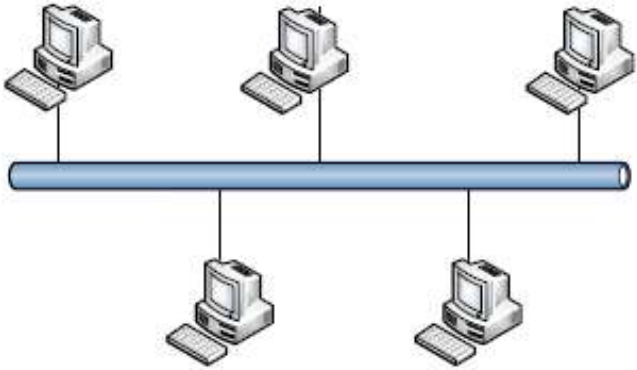
8.2.3 Topologi LAN

Perangkat keras seperti komputer, switch, router, kabel jaringan, dan perangkat lainnya merupakan komponen utama jaringan lokal (LAN). Setiap bagian memiliki fungsi khusus untuk menjaga konektivitas yang stabil dan pengiriman data yang efektif.

Jenis koneksi fisik yang menghubungkan setiap node dalam sebuah jaringan disebut topologi. Tiga topologi utama yang digunakan dalam sistem LAN adalah topologi bus, ring, dan bintang. Topologi jaringan ini kemudian berkembang menjadi topologi pohon, mesh, dan nirkabel. (Suprapto, 2020).

1. Topologi Bus

Topologi bus, juga disebut topologi backbone, adalah ketika sebuah kabel coaxial dibentangkan dan beberapa komputer disambungkan padanya. Secara sederhana, topologi bus terdiri dari satu kabel media transmisi dari satu ujung ke ujung lain, dan kedua ujungnya ditutup dengan resistor atau terminator yang tahan listrik lebih dari 60 ohm.



Gambar 8.2 Topologi BUS
(sumber:
https://www.kompas.com/skola/read/2023/01/28/170000469/topologi-bus--pengertian-kelebihan-dan-kekurangannya)

Topologi Bus adalah salah satu jenis topologi jaringan komputer yang memiliki ciri-ciri sebagai berikut:

a. Sambungan/Tap pada Titik Tertentu: Dalam topologi bus, ada satu jalur kabel utama yang menghubungkan

semua terminal atau perangkat. Pada titik-titik tertentu di jalur ini, sambungan atau tap digunakan untuk menghubungkan setiap terminal ke jaringan.

b. Transmisi Data Full Duplex dan Broadcast: Transmisi data dalam topologi bus bersifat full duplex, yang berarti data dapat dikirim dan diterima secara bersamaan. Selain itu, topologi bus mendukung mode broadcast, di mana semua terminal dalam jaringan dapat menerima transmisi data yang dikirimkan.
c. Protokol Ethernet atau CSMA/CD: Protokol Ethernet atau *Carrier Sense Multiple Access with Collision Detection* (CSMA/CD) adalah dua protokol yang paling umum digunakan dalam topologi bus. Protokol ini mengatur penyebaran dan penerimaan data di jaringan.
d. Penggunaan Kabel Coax (10Base5 dan 10Base2): Kabel koaksial, seperti 10Base5 dan 10Base2, dapat digunakan untuk menerapkan topologi bus. IEEE8023 mengisolasi standar ini.

Kelebihan Topologi Bus:

a. Instalasi Lebih Mudah: Instalasi topologi bus relatif mudah karena hanya memerlukan satu jalur kabel utama yang dihubungkan ke setiap terminal.
b. Kerusakan Isolasi: Komunikasi antar klien tidak akan terpengaruh oleh kerusakan atau gangguan pada komputer klien lainnya. Jalur kabel utama tetap terhubung ke masing-masing terminal.
c. Biaya Relatif Lebih Murah: Karena penggunaan kabel yang lebih sedikit, penerapan topologi bus cenderung lebih hemat biaya dibandingkan dengan metode lain.

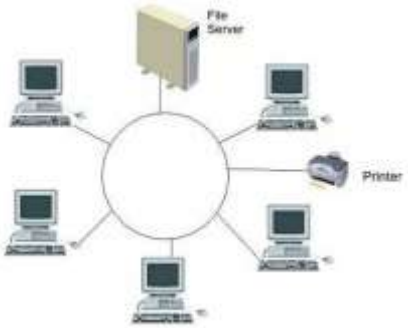
Kelemahan Topologi Bus:

a. Kesalahan pada Jalur Utama: Jika kabel utama atau backbone mengalami kerusakan atau terputus, maka komunikasi dalam jaringan bisa gagal sepenuhnya.
b. Pencarian Gangguan Sulit: Pencarian gangguan atau titik masalah pada jalur kabel utama yang panjang bisa menjadi tugas yang sulit dan memakan waktu.
c. Tabrakan Data (*Collision*): Jika banyak client mengirim pesan secara bersamaan, dapat terjadi tabrakan data (*collision*) yang memperlambat kecepatan komunikasi dalam jaringan.

Perlu diingat bahwa topologi bus adalah salah satu dari beberapa topologi yang digunakan dalam jaringan komputer, dan pilihan topologi harus dipertimbangkan berdasarkan kebutuhan dan batasan tertentu dari suatu jaringan.

2. Topologi Ring

Karena bentuknya yang menyerupai cincin yang melingkar yang berfungsi hampir mirip dengan konsentrator pada topologi bintang, akan menghubungkan semua komputer dalam jaringan.



Gambar 8.3. Topologi Ring
(sumber: https://lamanit.com/topologi-ring/)

Penjelasan Fungsi-fungsi dalam Topologi Cincin:

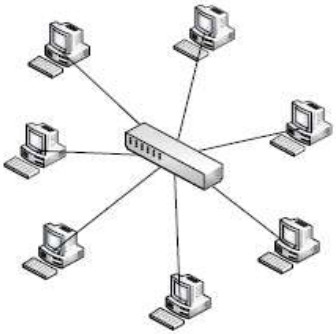
a. **Penyelipan Data:**
   Penyelipan data adalah langkah awal dalam proses pengiriman data dalam topologi cincin. Terminal pengirim menyelipkan data ke dalam saluran transmisi. Sebelum data dimasukkan ke dalam saluran, data tersebut biasanya diberi alamat tujuan yang sesuai dan bit-bit tambahan yang diperlukan sesuai dengan protokol yang digunakan.

b. **Penerimaan Data:**
   Penerimaan data terjadi ketika terminal yang menjadi tujuan atau penerima telah mengambil data dari saluran transmisi. Proses ini melibatkan perbandingan alamat pada paket data dengan alamat terminal itu tersebut. Jika alamat pada paket data sesuai dengan alamat terminal tersebut, data kiriman akan disalin atau diterima oleh terminal penerima.

c. **Pemindahan Data:**
   Pemindahan data adalah langkah akhir dalam proses pengiriman data dalam topologi cincin. Ini terjadi ketika kiriman data tidak diterima oleh terminal yang dituju atau mungkin akibat kesalahan alamat. Dalam situasi ini, data yang dikirim akan terus bergerak dalam cincin hingga mencapai terminal pengirim awal. Terminal pengirim akan mengambil kembali data tersebut karena tidak ada terminal yang menerimanya. Data mengalir dalam satu arah sepanjang cincin, dan setiap terminal berfungsi sebagai penerima dan pengirim data secara bergantian. Kelebihan dari topologi cincin adalah bahwa tidak ada tabrakan data (collision) seperti pada topologi bus, tetapi kekurangannya adalah jika satu terminal rusak, itu dapat memengaruhi seluruh cincin. Fungsi-fungsi di atas menjelaskan bagaimana data dikirim dan diterima dalam topologi cincin untuk memastikan data mencapai tujuan yang benar.

3. Topologi Star

Sebuah alat yang disebut concentrator, juga dikenal sebagai "topologi bintang", berfungsi sebagai hub atau switch terpusat di mana semua komputer dalam jaringan dihubungkan.



Gambar 8.4. Topologi Star
(sumber:
https://blog.unnes.ac.id/srirahayu/2016/02/22/pengertian-karakteristik-kelebihan-kekurangan-topologi-star/)

Kelebihan Topologi Star:

a. Pengelolaan yang Mudah: Topologi star membuat pengelolaan jaringan menjadi lebih mudah karena semua koneksi dan aktivitas dapat dipantau dan dikelola melalui terminal pusat. Ini memungkinkan administrator untuk dengan mudah mendeteksi masalah dan melakukan perawatan.
b. Kegagalan Isolasi: Kegagalan pada satu komponen atau terminal tidak akan mempengaruhi komunikasi terminal lainnya. Dengan kata lain, jika salah satu terminal mengalami masalah atau harus dinonaktifkan, jaringan tetap berfungsi dengan baik kecuali gangguan pada terminal pusat.

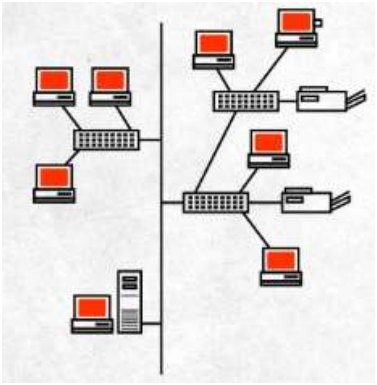
Kelemahan Topologi Star:

a. Kegagalan Pusat Pengendalian : Jika terminal pusat mengalami kegagalan, seluruh komunikasi dalam jaringan akan terganggu. Tanpa terminal pusat, terminal lainnya tidak dapat berkomunikasi satu sama lain.
b. Ketergantungan pada Pusat Kontrol: Semua komunikasi dalam topologi star tergantung pada kinerja dan ketersediaan terminal pusat. Jika terminal pusat mengalami overloading, maka kecepatan komunikasi dapat berkurang sesuai dengan jumlah komputer yang terhubung.
c. Biaya: Menggunakan perangkat keras tambahan seperti HUB atau MAU sebagai terminal pusat dapat meningkatkan biaya awal implementasi jaringan.

Penting untuk memahami kelebihan dan kelemahan topologi star serta mempertimbangkan kebutuhan dan kendala khusus dari suatu jaringan sebelum memilih jenis topologi yang sesuai. Topologi star cocok untuk jaringan yang memerlukan pengelolaan yang mudah dan isolasi kegagalan, tetapi perlu memperhatikan kerentanannya terhadap kegagalan terminal pusat.

4. Topologi Tree

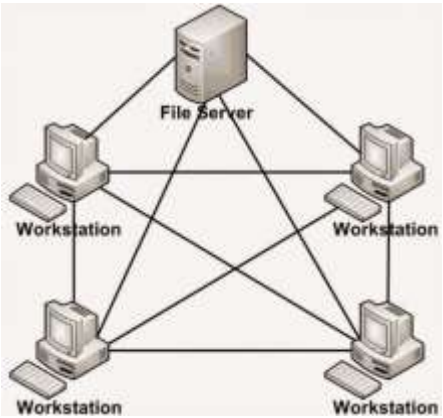
Pengembangan topologi bus, juga dikenal sebagai topologi pohon, melibatkan media transmisi yang terdiri dari satu kabel yang bercabang, tetapi loop tidak tertutup.



Gambar 8.5. Topologi Tree
(sumber: https://qwords.com/blog/pengertian-topologi-tree-serta-kelebihan-dan-kekurangannya/)

5. Topologi Mesh

Jika tidak ada perencanaan awal ketika membangun jaringan, topologi mesh biasanya muncul tanpa aturan koneksi.



Gambar 8.6. Topologi Mesh
(sumber: https://www.dosenpendidikan.co.id/wp-content/uploads/2019/12/Topologi-Mesh.png)

6. Topologi Wireless

Karena kemampuan mereka untuk mengurangi biaya pemasangan kabel serta mengurangi beban yang terkait dengan relokasi kabel apabila arsitektur bangunan berubah, jaringan nirkabel menjadi populer sebagai alternatif dari jaringan kabel, terutama untuk pengembangan LAN tradisional. WLAN, WaveLAN, HotSpot adalah beberapa nama topologi ini.

Gambar 8.7. Topologi Wireless
(sumber: https://www.skomnet.com/2018/11/jaringan-wifi.html)

Penjelasan tentang Jaringan WiFi:

Jaringan WiFi, atau jaringan lokal nirkabel, adalah teknologi jaringan yang menghubungkan perangkat dalam jaringan tanpa menggunakan kabel fisik. Jaringan WiFi menggunakan teknologi komunikasi radio untuk mengirimkan data antar perangkat. Ini memiliki berbagai keunggulan dan kelemahan:

Keunggulan Jaringan WiFi:

1. Biaya Pemeliharaan Murah: Setelah infrastruktur WiFi terpasang, biaya pemeliharaan cenderung rendah karena tidak perlu memasang atau mengganti kabel fisik.

2. Infrastruktur Berdimensi Kecil: WiFi tidak memerlukan infrastruktur kabel yang besar, sehingga cocok untuk bangunan dengan ruang terbatas atau bangunan yang berdekatan.
3. Pembangunan Cepat: Menginstal jaringan WiFi bisa cepat dan lebih sederhana dibandingkan dengan pemasangan kabel.
4. Mudah dan Murah untuk Direlokasi: Jaringan WiFi mudah untuk direlokasi atau diubah konfigurasinya jika dibandingkan dengan jaringan kabel yang memerlukan perubahan fisik yang lebih besar.
5. Mendukung Portabilitas: Perangkat yang terhubung ke jaringan WiFi bisa berpindah-pindah dengan mudah tanpa perlu mengganti infrastruktur kabel.

Kelemahan Jaringan WiFi:

1. Biaya Peralatan Mahal: Peralatan untuk jaringan WiFi seperti router dan akses poin dapat menjadi mahal, terutama jika diperlukan perangkat khusus dengan fitur tambahan.
2. Delay yang Sangat Besar: Jaringan WiFi bisa mengalami latency yang tinggi atau delay, terutama dalam lingkungan dengan banyak perangkat yang bersaing untuk akses ke saluran radio yang terbatas.
3. Kesulitan karena Masalah Propagasi Radio: Kinerja jaringan WiFi dipengaruhi oleh kondisi propagasi radio seperti interferensi, redaman sinyal, dan refleksi, yang dapat membuat koneksi menjadi tidak stabil.
4. Mudah untuk Terinterferensi: Jaringan WiFi dapat terganggu oleh perangkat lain yang menggunakan spektrum radio yang sama, seperti microwave oven atau perangkat Bluetooth.
5. Kapasitas Jaringan Terbatas: Kapasitas jaringan WiFi terbatas oleh spektrum frekuensi yang terbatas, yang dapat

mengakibatkan kinerja yang buruk jika terlalu banyak perangkat yang terhubung secara bersamaan.
6. Keamanan/Kerahasiaan Data Kurang Terjamin: Jaringan WiFi rentan terhadap serangan keamanan jika tidak diatur dengan baik. Untuk menjaga keamanan data, perlu diimplementasikan protokol keamanan yang kuat seperti WPA2 atau WPA3.

Jaringan WiFi adalah solusi yang populer untuk menghubungkan perangkat dalam lingkungan rumah, kantor, atau umum. Namun, penting untuk mempertimbangkan keunggulan dan kelemahan ini saat merencanakan, menginstal, dan mengelola jaringan WiFi.

8.3 WAN (*Wide Area Network*)

8.3.1 Pengertian WAN

Wide Area Network (WAN) adalah jaringan komputer yang mencakup area geografis yang sangat luas, seperti kota, negara, atau bahkan benua. WAN berfungsi sebagai tulang punggung komunikasi global, menghubungkan lokasi yang berjauhan secara efektif. Jika WAN mencakup area intercontinental, maka WAN disebut sebagai jaringan informasi global atau internet. Dua metode pengiriman paket data ada dalam jaringan IP: datagram, yang digunakan di internet, dan connection-oriented, di mana setup koneksi logika dilakukan sebelum pengiriman paket. Mode koneksi ini dikenal sebagai virtual circuit, dan memungkinkan penggunaan sumber daya jaringan secara bersamaan. Dengan cara ini, urutan paket dapat dijamin. Namun, tingkat kontinuitas real-time tidak selalu dapat dijamin dan sangat bergantung pada kapasitas jaringan dan tingkat kepadatan lalu lintas. Mode virtual circuit ini juga memungkinkan organisasi untuk memiliki jaringan privat virtual (VPN) yang meluas secara logis, mencakup area nasional bahkan internasional, tanpa harus memiliki infrastruktur

fisik yang luas. WAN melibatkan sejumlah perangkat seperti router, modem, dan protokol seperti HDLC, PPP, Frame Relay, dan lainnya. Ini memungkinkan organisasi untuk berkomunikasi dan mentransfer data secara efisien di seluruh dunia, tetapi juga membutuhkan manajemen yang cermat dan pemilihan teknologi yang sesuai.("Computer Networks and Internets," 1997).

Dengan mode virtual circuit ini, sebuah kelompok bisnis atau organisasi dapat memiliki jaringan privat virtual (seperti *Virtual Private Network* atau IP VPN) atau jaringan PBX (*Private Branch Exchange*). Karena jaringan IP VPN dibangun secara logika dan dibuat hanya saat diperlukan, jaringan IP VPN tidak memiliki ruang area terbatas seperti PABX. Akibatnya, jaringan pribadi IP VPN dapat mencakup area yang lebih besar daripada PABX. Jaringan WAN adalah jenis jaringan komputer yang dapat menghubungkan banyak lokasi, seperti kota, negara, atau bahkan benua. Struktur jaringan WAN terdiri dari berbagai jaringan yang berbeda namun saling terhubung, yang mengharuskan penggunaan intermediate device, seperti router, untuk mengelola dan mengarahkan lalu lintas data antar lokasi. Jaringan WAN terdiri dari banyak perangkat lain selain router. Ini termasuk modem, CSU/DSU (Unit Layanan Channel/Unit Layanan Data), *Access Server, Communication Server*, Switch WAN, dan Core Router.

Berbagai protokol dapat digunakan dalam jaringan WAN, tergantung pada infrastruktur dan kebutuhan jaringan. Protokol-protokol ini termasuk HDLC (*High-Level Data Link Protocol*), PPP (*Point-to-Point Protocol*), X.25 Protocol, Frame Relay, dan ISDN. Media komunikasi yang digunakan dalam jaringan WAN umumnya berupa saluran komunikasi publik, seperti kabel serat optik, kabel tembaga, satelit, gelombang radio, dan sebagainya. Pemanfaatan media publik ini memungkinkan jaringan WAN untuk mencakup area yang sangat luas dan memfasilitasi komunikasi antarlokasi yang jauh. Berikutnya, gambaran visual dari jaringan WAN akan

memberikan ilustrasi tentang bagaimana berbagai lokasi yang berjauhan dapat terhubung melalui infrastruktur WAN. Jaringan WAN memainkan peran penting dalam mendukung komunikasi dan pertukaran data yang efisien di tingkat global, membantu organisasi dan individu untuk berinteraksi di seluruh dunia dengan cepat dan efektif (Anwar, 2018).

8.3.2 Teknologi WAN

Teknologi WAN adalah kerangka kerja yang mencakup berbagai metode komunikasi yang penting dalam dunia jaringan komputer, seperti *circuit-switching*, *packet-switching*, dan teknologi *Virtual Private Network* (VPN). Setiap metode ini memiliki karakteristik dan kegunaan yang unik.

Dalam membangun jaringan WAN, berbagai media transmisi dapat digunakan, termasuk kabel serat optik (*fiber optic*), kabel telepon, dan bahkan satelit. Karena cakupannya yang sangat luas, pembangunan jaringan WAN seringkali memerlukan investasi biaya yang substansial. Namun, hal ini memungkinkan jaringan ini untuk menghubungkan berbagai lokasi yang terpisah jauh, mendukung komunikasi antar wilayah yang luas.

Jaringan WAN memiliki karakteristik yang khas yang menjadikannya unik di antara jenis-jenis jaringan komputer lainnya:

1. **Menghubungkan Perangkat yang Tidak Bisa Diakses oleh Jaringan Lain:** Dengan menggunakan WAN, perangkat atau lokasi yang tidak dapat dijangkau oleh jaringan lokal (LAN) atau jaringan metropolitan (MAN) dapat dihubungkan.
2. **Koneksi pada Jarak yang Berjauhan:** Salah satu fitur utama WAN adalah kemampuannya untuk menghubungkan lokasi yang berjauhan, termasuk antar kota, negara, dan benua.

3. **Mengirimkan Paket Data Antar Perangkat:** WAN memungkinkan pengiriman paket data antar perangkat seperti switch dan router, bahkan antar jaringan yang telah dibangun.
4. **Akses Bandwidth Jarak Jauh:** Untuk mengakses bandwidth pada jarak jauh, WAN memerlukan koneksi serial yang mendukung berbagai jenis media transmisi.
5. **Lapisan OSI Layer:** Lapisan fisik dan lapisan data link adalah beberapa lapisan Open Systems Interconnection (OSI) di mana WAN beroperasi.

Jaringan WAN memainkan peran penting dalam menghubungkan dunia dan mendukung berbagai bentuk komunikasi di seluruh dunia. Dengan cakupan yang sangat luas dan teknologi yang unik, WAN memfasilitasi pertukaran data dan informasi yang vital dalam berbagai konteks, dari bisnis hingga pendidikan dan pemerintahan.

8.3.3 Komponen WAN

Komponen jaringan WAN melibatkan sejumlah perangkat keras penting yang memainkan peran utama dalam memastikan konektivitas yang handal dalam skala geografis yang luas. Untuk memahami lebih lanjut, berikut adalah penjelasan mengenai beberapa perangkat jaringan WAN yang esensial:

1. **Router:**

   Router adalah perangkat yang memiliki peran penting dalam jaringan WAN. Tugas utamanya adalah mengatur dan mengarahkan lalu lintas data antara berbagai perangkat dan jaringan. Router tidak hanya mengirimkan paket data dari internet ke perangkat lain, tetapi juga mendukung konektivitas secara keseluruhan. Ini mencakup pengaturan koneksi, fleksibilitas, manajemen lalu lintas, dan banyak lagi.

2. **Modem:**

   Perangkat elektronik yang disebut modem, atau modulator demodulator, digunakan untuk menghubungkan perangkat seperti komputer, laptop, atau ponsel ke internet. Tugas modem adalah mengubah sinyal digital dari perangkat menjadi sinyal analog yang dapat dikirim melalui jalur telepon atau jaringan lainnya. Selain itu, modem juga berfungsi sebagai pengirim data melalui proses modulasi dan demodulasi sinyal.

3. **Antena:**

   Meskipun bukan bagian utama dari infrastruktur jaringan WAN, antena memainkan peran penting dalam memperkuat sinyal komunikasi. Antena digunakan untuk menangkap sinyal dari berbagai sumber, seperti satelit atau pemancar lainnya, dan mengoptimalkan kualitas sinyal. Ini dapat membuat sinyal menjadi lebih stabil dan memperluas jangkauannya.

   Perangkat-perangkat ini berperan kunci dalam menjaga konektivitas dan kinerja jaringan WAN. Mereka bekerja bersama untuk memungkinkan komunikasi yang andal di seluruh area geografis yang luas, baik itu untuk tujuan bisnis, pendidikan, atau penggunaan pribadi.

8.3.4 Protokol WAN

Protokol WAN seperti TCP/IP dan MPLS berperan sebagai bahasa komunikasi yang digunakan oleh perangkat jaringan untuk berinteraksi melintasi jaringan WAN. Memahami protokol WAN adalah kunci dalam mengelola dan memelihara jaringan yang efisien. Dalam praktiknya, jaringan WAN menggunakan dua komponen teknologi komunikasi utama, yaitu kabel transmisi dan komponen switching.

Kabel transmisi adalah alat fisik yang mengangkut bit data dari satu komputer ke komputer lain dalam jaringan WAN. Sementara itu, komponen switching adalah komponen komputer khusus yang menghubungkan dua atau lebih kabel transmisi. Ini

berfungsi sebagai perute data yang mengarahkan lalu lintas data ke tujuannya yang benar dalam jaringan. Selain itu, jaringan WAN juga bisa beroperasi dalam mode nirkabel. Jaringan nirkabel, atau jaringan wireless, mengandalkan gelombang radio sebagai media transmisi untuk mendistribusikan informasi. Jaringan ini sering digunakan karena kenyamanan dan mobilitas pengguna dalam menjaga koneksi ke jaringan.

Untuk memberikan pemahaman tentang bagaimana jaringan WAN bekerja dalam sebuah contoh kasus:

1. Sebuah perusahaan memutuskan untuk menempatkan satu komputer server khusus untuk mengelola akses ke basis data yang dimilikinya.
2. Komputer server ini bertugas mengirimkan informasi dari basis data serta paket data ke seluruh jaringan WAN sesuai dengan topologi yang telah diimplementasikan.
3. Dengan topologi jaringan yang telah dibangun, komputer klien atau pengguna dapat mengakses informasi yang terdapat di komputer server, bahkan jika mereka berada di lokasi yang berbeda, baik di luar pulau maupun antar negara.

Dengan cara ini, jaringan WAN memungkinkan berbagai lokasi yang terpisah secara geografis untuk tetap terhubung dan berkomunikasi dengan efisien, memfasilitasi pertukaran data dan informasi di tingkat global.

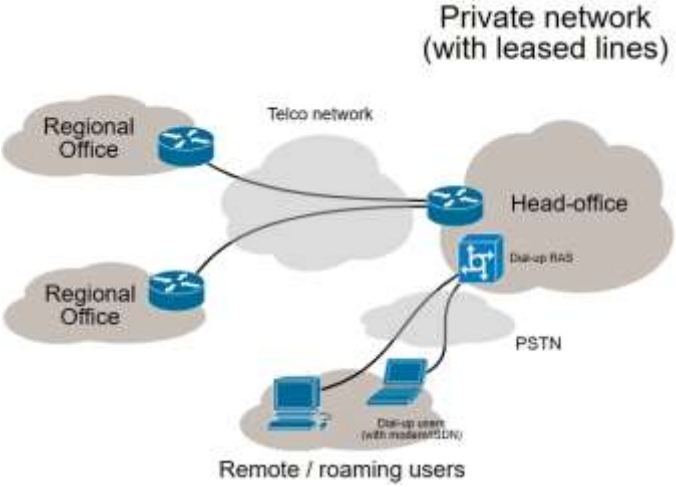
Koneksi digunakan pada jaringan WAN terdiri dari:

1. Leased line

Salah satu jenis koneksi jaringan yang dikenal sebagai jalur sewa yang digunakan untuk menghubungkan dua lokasi secara langsung dan eksklusif. Salah satu perbedaan utama antara koneksi jaringan yang dikontrak dengan jaringan yang dikontrak adalah bahwa jaringan yang dikontrak tidak

memerlukan proses pengaturan panggilan untuk memulai pengiriman data. Dalam leased line, koneksi antara dua titik (misalnya, dua kantor cabang perusahaan) selalu aktif dan tersedia untuk pengiriman data sepanjang waktu. Ini berbeda dengan koneksi dial-up yang memerlukan inisiasi panggilan setiap kali Anda ingin terhubung ke jaringan.

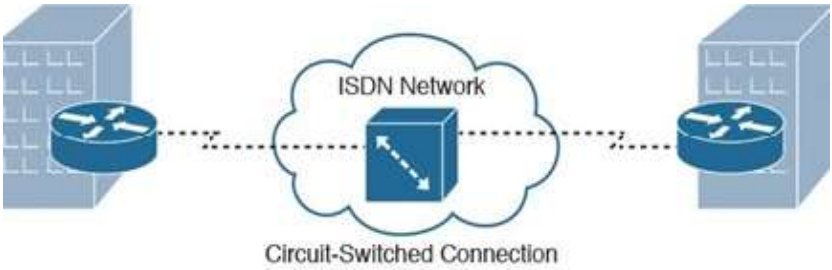
Koneksi *leased line* sering menggunakan metode pengiriman data yang disebut *Synchronous Serial*. Ini berarti data dikirim secara terus menerus dan sinkron, tanpa memerlukan proses pengiriman yang kompleks seperti pada koneksi dial-up yang asinkron. Koneksi leased line umum digunakan dalam aplikasi yang memerlukan koneksi yang sangat andal dan selalu aktif, seperti untuk koneksi internet bisnis, VoIP (*Voice over* IP), atau koneksi antara pusat data dan cabang perusahaan. Meskipun biayanya lebih tinggi daripada beberapa opsi lainnya, leased line menawarkan keandalan dan kinerja yang konsisten(Chwan-Hwa (John) Wu; J. David Irwin, 2013).



Gambar 8.8. Leased line
(sumber: https://en.wikipedia.org/wiki/Leased_line)

2. Circuit-switch

Untuk memulai pengiriman data, pengaturan panggilan dilakukan pada koneksi switching sirkuit. PTSN dan ISDN adalah protokol pada WAN yang menggunakan koneksi *switching* sirkuit pada jaringan publik.



Gambar 8.9. Circuit-switch
(sumber: https://en.wikipedia.org/wiki/Leased_line)

Dua protokol WAN yang menggunakan koneksi circuit switching di jaringan publik adalah *Public Switched Telephone Network* (PSTN) dan *Integrated Services Digital Network* (ISDN):

a. PSTN (*Public Switched Telephone Network*): PSTN adalah jaringan telepon umum yang menggunakan koneksi circuit switching untuk menyediakan layanan telepon tradisional. Ketika seseorang melakukan panggilan telepon, PSTN akan mengalokasikan jalur komunikasi fisik eksklusif dari pengirim ke penerima selama panggilan tersebut. Ini memastikan kualitas suara yang baik, tetapi juga membuatnya kurang efisien untuk mentransfer data yang besar atau jenis layanan lainnya selain suara.

b. ISDN (*Integrated Services Digital Network*): ISDN adalah teknologi jaringan yang lebih canggih yang menggunakan koneksi circuit switching untuk

menyediakan layanan suara dan data dalam satu infrastruktur. ISDN memberikan jalur komunikasi digital yang lebih cepat dan lebih andal daripada PSTN. Meskipun sebagian besar layanan ISDN telah digantikan oleh teknologi jaringan yang lebih modern seperti DSL dan fiber optic, ISDN masih digunakan dalam beberapa kasus.

Kedua protokol ini menggunakan circuit switching untuk mengatur panggilan suara dan data di jaringan publik. Namun, dengan perkembangan teknologi jaringan, banyak jaringan WAN saat ini beralih ke metode packet switching seperti IP (*Internet Protocol*) untuk mentransfer data secara lebih efisien dan mendukung berbagai jenis layanan.

3. Packet switching

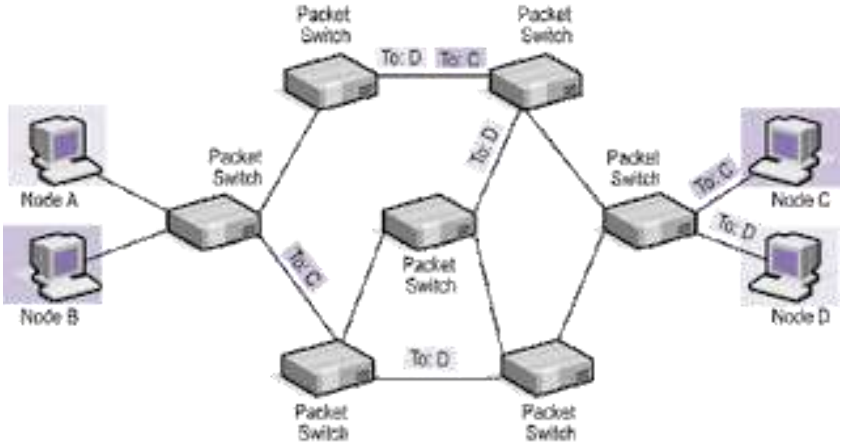
Metode pengiriman data di mana data dibagi menjadi paket-paket kecil sebelum dikirim melalui jaringan. Setiap paket data mengandung informasi pengenal tujuan, yang memungkinkan mereka mengambil rute yang berbeda melalui jaringan sebelum akhirnya diatur ulang dan disusun kembali di tujuan akhir.

Beberapa poin penting tentang packet switching:

a. Pemakaian Bandwidth yang Efisien: Dengan packet *switching, bandwidth* jaringan dapat dibagi di antara berbagai pengguna dan aplikasi. Ini memungkinkan penggunaan yang lebih efisien dari bandwidth yang tersedia karena data hanya dikirim saat diperlukan.
b. Stabilitas Koneksi: Packet switching memungkinkan multipleksing, yaitu berbagi jalur komunikasi antara pengguna yang berbeda. Hal ini dapat meningkatkan stabilitas koneksi, karena ketika satu pengguna tidak aktif, bandwidthnya dapat dialokasikan ke pengguna lain.

c. Pengiriman Data yang Terdistribusi: Pengiriman paket membagi data menjadi paket-paket kecil yang dapat bergerak melalui jaringan dengan cara yang berbeda.. Hal ini memungkinkan pengiriman data yang terdistribusi, yang membuat jaringan lebih tangguh terhadap kegagalan.
d. Pengembangan dari Leased Line: Sebagaimana Anda sebutkan, packet switching adalah pengembangan dari koneksi Leased Line yang lebih tradisional. Leased Line adalah koneksi yang terus terbuka sepanjang waktu, sedangkan packet switching memungkinkan pengiriman data dalam paket-paket yang lebih efisien.
e. Synchronous Serial: Packet switching dapat diimplementasikan menggunakan metode Synchronous Serial, di mana data dikirim secara terus menerus dan sinkron. Ini adalah salah satu cara untuk mengatur pengiriman paket data dalam packet switching.

Packet *switching* adalah dasar dari banyak jaringan modern, termasuk internet. Ini memungkinkan pengiriman data yang efisien dan adaptif, mendukung berbagai aplikasi dan pengguna dalam jaringan yang berbeda-beda.



Gambar 8.10. Packet switching
(sumber:
https://ilhamasterjaringan.blogspot.com/2016/07/switching.html

8.3.5 Manajemen WAN

Manajemen WAN melibatkan pemantauan dan administrasi jaringan yang berada di berbagai lokasi geografis berbeda. Salah satu fokus utama dalam manajemen WAN adalah keamanan, karena melindungi data yang mengalir melalui jaringan WAN dari serangan siber dan ancaman lainnya sangat penting.(Astuti, 2018)
Berikut adalah kelebihan dan kekurangan dari jaringan WAN:

Kelebihan Jaringan WAN:

1. Transmisi File, Data, dan Sumber Daya: Jaringan WAN digunakan untuk mengirim dan menerima file, data, dan sumber daya antara lokasi yang berbeda secara efisien.
2. Informasi Real Time: Jaringan WAN memungkinkan perolehan informasi secara real time, yang penting untuk aplikasi seperti telekomunikasi dan video konferensi.
3. Berbagi Sumber Daya: Jaringan WAN dapat digunakan untuk berbagi sumber daya atau sumber daya antara berbagai lokasi melalui koneksi workstations.

4. Bandwidth Luas: WAN memiliki bandwidth yang besar, yang memungkinkan transfer data yang cepat dan efisien di seluruh jaringan.
5. Skala Global: Jaringan WAN mampu menjangkau negara, benua, bahkan seluruh dunia, yang memungkinkan organisasi untuk terhubung dengan lokasi-lokasi yang sangat jauh secara geografis.

Kekurangan Jaringan WAN:

1. Biaya Tinggi: Biaya pembangunan jaringan WAN, fasilitas, dan perawatan sangat tinggi karena cakupannya yang luas dan infrastruktur yang diperlukan.
2. Kompleksitas: Pengaturan dan konfigurasi jaringan WAN lebih sulit dan rumit dibandingkan dengan jaringan yang lebih kecil. Alat-alat dan perangkat keras yang diperlukan untuk membangun jaringan WAN juga cenderung mahal.
3. Kerentanan terhadap Serangan: Jaringan WAN dengan cakupan global dapat menjadi sasaran serangan siber yang lebih besar. Oleh karena itu, perlindungan yang kuat seperti firewall menjadi penting.
4. Ketergantungan pada Firewall: Untuk menjaga keamanan, jaringan WAN seringkali wajib menggunakan firewall, yang dapat menambah kompleksitas dan biaya tambahan pada pengelolaan jaringan.

Mengelola jaringan WAN memerlukan perhatian khusus terhadap keamanan, skalabilitas, dan efisiensi untuk memastikan bahwa jaringan tersebut beroperasi dengan lancar dan aman di seluruh lokasi geografis yang berbeda.(Sethi, 2013)

DAFTAR PUSTAKA

Anwar, M. C. 2018. *Konsep Jaringan Komputer (Kompilasi terjemahan buku Introduction to Cisco Networking Technologies (INTRO) version 2.1 & Interconnecting Cisco Network Devices, version 2.3)*.

Astuti, I. K. 2018. Fakultas Komputer INDAH KUSUMA ASTUTI Section 01. *Jaringan Komputer*, 8. https://id.scribd.com/document/503304719/jaringan-komputer

Chwan-Hwa (John) Wu; J. David Irwin. 2013. *Introduction to Computer Networks and Cybersecurity - CRC Press Book*. http://www.crcpress.com/product/isbn/9781466572133

Computer networks and Internets. 1997. In *Choice Reviews Online* (Vol. 35, Issue 01). https://doi.org/10.5860/choice.35-0328

Komputasi, L., & Jaringan, D. A. N. 2018. *Buku Petunjuk Praktikum Jaringan Komputer*.

Maulana, A., & Fauzi, A. 2018. Buku-Jaringan--komputer_-FIX. *Repository.Nusamandiri.Ac.Id*, 100.

Sethi, A. K. 2013. Computer Networks and the Internet. In *The Business of Electronics*. https://doi.org/10.1057/9781137323385_8

Tanenbaum, A. S., & Wetherall, D. 2014. *Computer Networks 5th ed*.

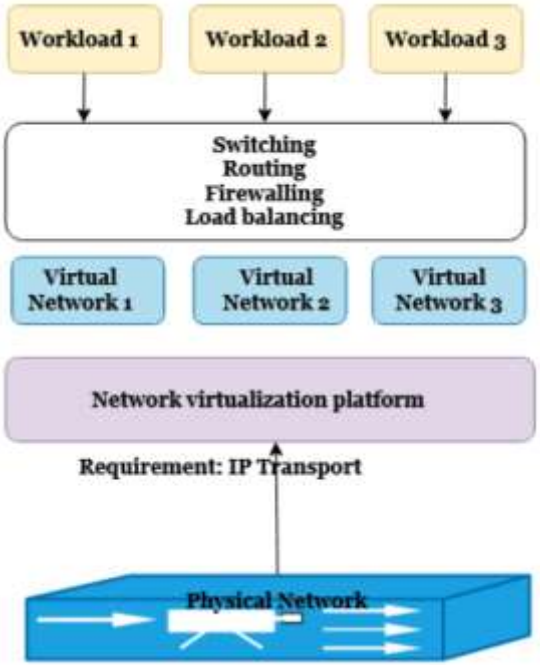
BAB 9
VIRTUALISASI JARINGAN

Oleh Danang Haryo Sulaksono

9.1 Pendahuluan

Sebuah jaringan komputer adalah kumpulan dari komputer dan device terkoneksi pada sebuah channel komunikasi yang memfasilitasi komunikasi setiap user and dapat digunakan oleh user untuk sharing data dan sumber daya. Jaringan komputer sendiri bekerja menggunakan node dan link. Perangkat komunikasi data atau yang disebut juga dengan node, sebagai contoh modem, hub, switch. Sedangkan link dalam jaringan adalah koneksi antara dua atau beberapa node seperti kabel, atau fiber optik. Pada perusahaan besar, keamanan, komunikasi data dan manajemen jaringan merupakan aspek yang sangat penting. Sehingga dibutuhkan sebuah sistem virtualisasi jaringan yang mempunyai skalabilitas, fleksibilitas dan kemudahan manajemen sehingga dapat meningkatkan produktivitas dari sebuah jaringan itu sendiri.
Virtualisasi jaringan adalah sebuah proses untuk menggabungkan sumber daya hardware, software dan fungsi jaringan ke dalam sebuah single management system yaitu virtual network. Virtual networking ini digunakan untuk komunikasi pada beberapa virtual machine (VM) yang berjalan dalam sebuah hypervisor seperti KVM, VirtualBox, XEN, Vsphere, Hyper-V dan lain sebagainya selain itu juga melibatkan platform virtualization dan juga gabungan dari resource virtualization. Virtual network dapat melakukan komunikasi antar device pada beberapa lokasi yang berbeda dengan fungsi dan kemampuan yang sama dengan jaringan komputer tradisional namun lebih efisien dan lebih mudah

dimodifikasi sesuai kebutuhan tanpa harus mengganti atau membeli *physical hardware* yang baru.



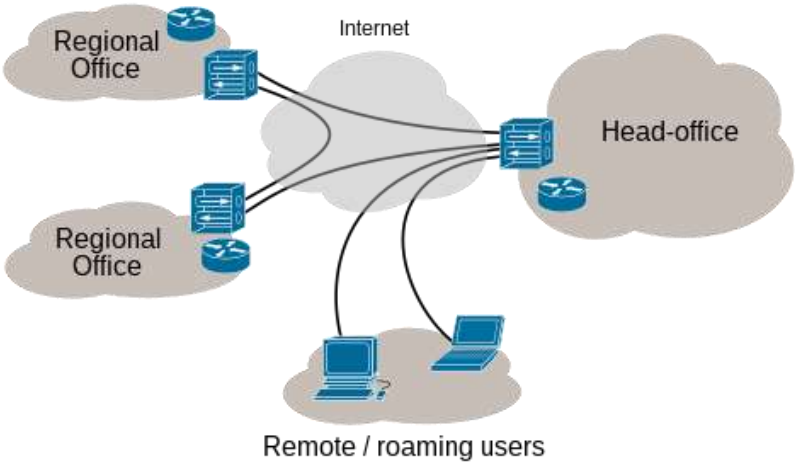
Gambar 9.1. Virtual Network
(sumber: www.parallels.com)

9.2 Kategori Virtual Network

Pada umumnya virtual network terbagi menjadi tiga kategori, yaitu private, internal dan external. Sebuah private virtual network dapat membuat sebuah Vm untuk berkomunikasi hanya dengan VM yang lain dalam host yang sama. External network merupakan sistem yang dapat melakukan komunikasi antara sebuah host dan beberapa jaringan VM. Sedangkan external virtual network dapat mengkoneksikan beberapa VM ke dunia luar.

9.2.1 *Virtual Private Network* (VPN)

VPN adalah sebuah mekanisme untuk membuat sebuah koneksi yang aman antara sebuah komputer atau antara dua jaringan dengan menggunakan sebuah komunikasi yang rentan akan keamanan, contohnya adalah internet. Data tambahan dilampirkan ke paket header, menjelaskan informasi routing yang sesuai dengan ruang alamat yang relevan. Setiap host di ruang tersebut memiliki tabel port-forwarding lokal. Instruksi khusus ini membantu membentuk tunnel alamat, yang hanya dapat dilalui melalui paket header tambahan ini. Dengan cara ini, VPN menghasilkan ruang alamat virtual dan mengenkripsi traffic jaringan menjadi private, dengan cara tabel port-forwarding menghubungkan titik pada setiap alamat. Secara teknis, ini adalah virtualisasi jaringan, meskipun cakupan dan skalanya jauh lebih kecil dibandingkan dengan kategori lainnya.

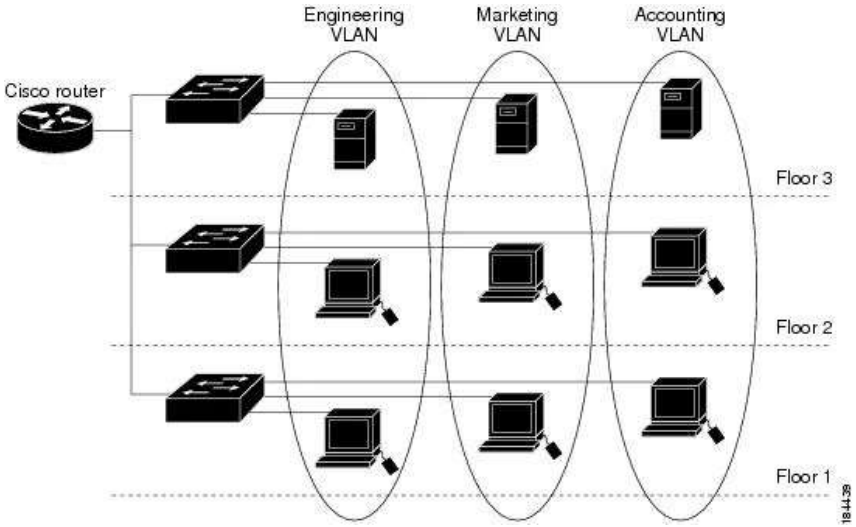


Gambar 9.2. Private Virtual Network (VPN)
(sumber: www.parallels.com)

VPN dapat diklasifikasikan menjadi beberapa kategori, yaitu Remote Access adalah sebuah konfigurasi host-to-network yang mengkoneksikan sebuah komputer kepada local area network, sistem ini dapat memberikan akses kepada sebuah jaringan enterprise, seperti intranet. Kedua adalah site-to-site, sebuah konfigurasi yang mengkoneksikan dua jaringan, konfigurasi ini memperluas jaringan pada lokasi yang berbeda atau mengkoneksikan sebuah grup kantor pada sebuah data center. Kategori ketiga adalah extranet-based site-to-site, adalah sebuah konfigurasi dimana sebuah VPN dapat dimiliki oleh beberapa organisasi.

9.2.2 *Virtual Local Area Network* (VLAN)

VLAN adalah sebuah set logical dari beberapa node yang terdapat dalam sebuah *Local Area Network* (LAN) yang sama. Sebuah VLAN secara logical dapat disegmentasi berdasarkan fungi atau aplikasi, tanpa memperdulikan lokasi dari user. VLAN mempunyai atribut yang sama seperti LAN fisik. Setiap VLAN dianggap sebagai jaringan logical, dan paket yang ditujukan ke stasiun yang bukan milik VLAN harus diteruskan melalui router. Gambar 9.3 menunjukkan VLAN sebagai jaringan logical. Beberapa station di departemen teknik ditugaskan ke satu VLAN, Beberapa station di departemen pemasaran ditugaskan ke VLAN lain, dan Beberapa station di departemen akuntansi ditugaskan ke VLAN lain.



Gambar 9.3. Virtual LAN (VLAN)
(sumber: Cisco.com)

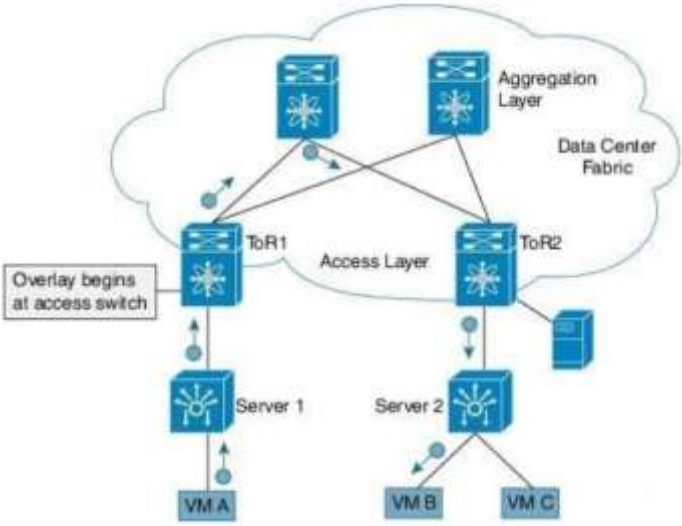
VLAN dapat membuat sebuah extended LAN dipartisi menjadi beberapa LAN yang berbeda. Setiap VLAN diberikan sebuah indentifier, dan paket hanya dapat melakukan perjalanan dari satu segmen ke yang lainnya jika kedua segmen mempunyai identifier yang sama. Hal ini akan membatasi jumlah segmen dalam sebuah extended LAN yang akan menerima paket broadcast. Sebuah fitur tambahan dari VLAN adalah dapat memungkinkan untuk merubah topologi logical tanpa merubah kabel maupun alamat (Peterson, 2011).

9.2.3 *Virtual Extensive Local Area Network* (VXLAN)

VXLAN adalah adalah sebuah protokol enkapsulasi untuk berjalan pada sebuah overlay network pada infrasruktur layer 3. Sebuah overlay network adalah virtual network yang dibangun di atas teknologi jaringan layer 2 dan layer 3 untuk mendukung arsiktektur elastic computing. VXLAN akan memudahkan user

untuk memperluas cloud computing environment sambil melakukan isolation pada aplikasi dan user cloud secara logical (Ruano, 2017).

VXLAN membuat administrator jaringan untuk melakukan migrasi *virtual machine*(VM) dengan jarak yang jauh dan mempunyai peranan yang penting dalam *software-defined networking* (SDN), sebuah arsitektur yang memungkinkan sebuah server atau controller untuk memberikan informasi switch jaringan kemana paket akan dikirimkan. Dalam sebuah jaringan konvensional, setiap switch mempunyai software yang memberitahukan apa yang harus dilakukan. Dalam SDN, pemindahan paket dilakukan secara terpusat dan arus lalul intas jaringan dapat diprogram secara independen dari masing-masing switch dan perlengkapan data center. Untuk mengimplementasikan SDN menggunakan VXLAN, administratir daat menggunakan hardware atau software yang sudah ada, membuat teknologi ini lebih murah secara finansial dibandingkan dengan jaringan komputer konvensional.



Gambar 9.4. VXLAN Overlay
(sumber: Cisco.com)

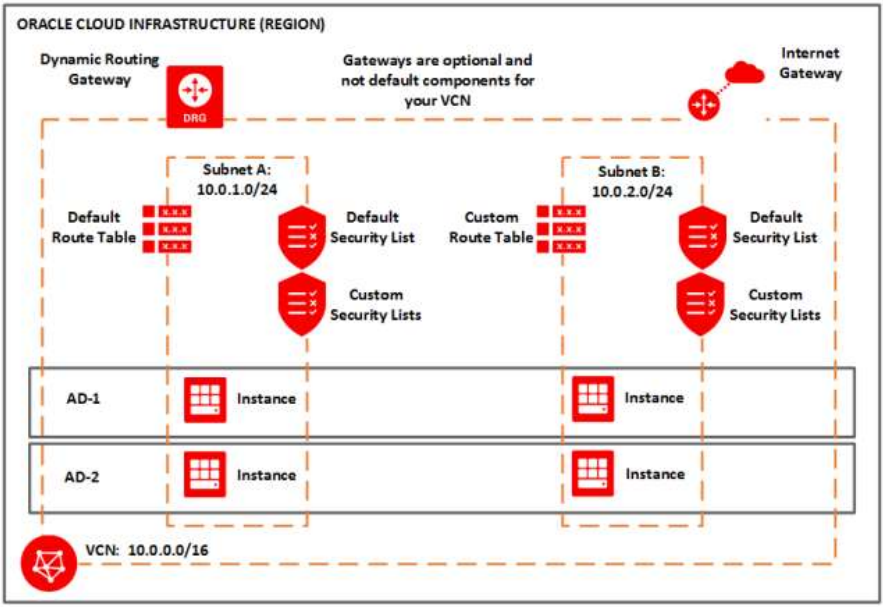
Tujuan utama da VXLAN adalah untuk memperluas ruang alamat VLAN dengan menambahkan sebuah 24 bit segment ID dan menambahkan jumlah ID yang tersedia menjadi 16 juta. Segment ID dari VXLAN pada setiap frame membedakan setiap jaringan logical individu sehingga jutaan jaringan VXLAN layer 2 yang terisolasi dapat berdampingan pada infrastruktur layer 3. Seperti VLAN, hanya virtual machine (VM) dalam jaringan logical yang sama dapat berkomunikasi satu sama lain (George, 2021).

9.3 Virtual Network Provider

Berikut adalah beberapa perusahaan besar penyedia layanan virtual network.

9.3.1 *Oracle Virtual Cloud Network* (VCN)

VCN adalah sebuah virtual, private network yang terhubung dalam Oracle data center. VCN sangata mirip dengan jaringan tradisional, dengan rule pada firewall dan tipe komunikasi spesifik yang dapat dipilih oleh user. Sebuah VCN berada di satu wilayah infrastruktur Oracle Cloud mencangkup satu wilayah block IPV4 *Classless Inter-Domain Routing* (CIDR) yang berdekatan. Jangkauan ukuran VCN yang diperbolehkan antara /16 hingga /30. Contoh: 10.0.0.0/16. Layanan jaringan melakukan reservasi pada dua alamat IP pertama yang terakhir di masing-masing alamat subnet CIDR. Gambar 9.5 adalah sebuah ilustrasi sederhana dari sebuah VCN dengan dua regional subnet. Setiap subnet berisi instance di setiap domain yang tersedia. Subnet A menggunakan default route table, dan subnet B custom route table yang dapat dibuat oleh user.



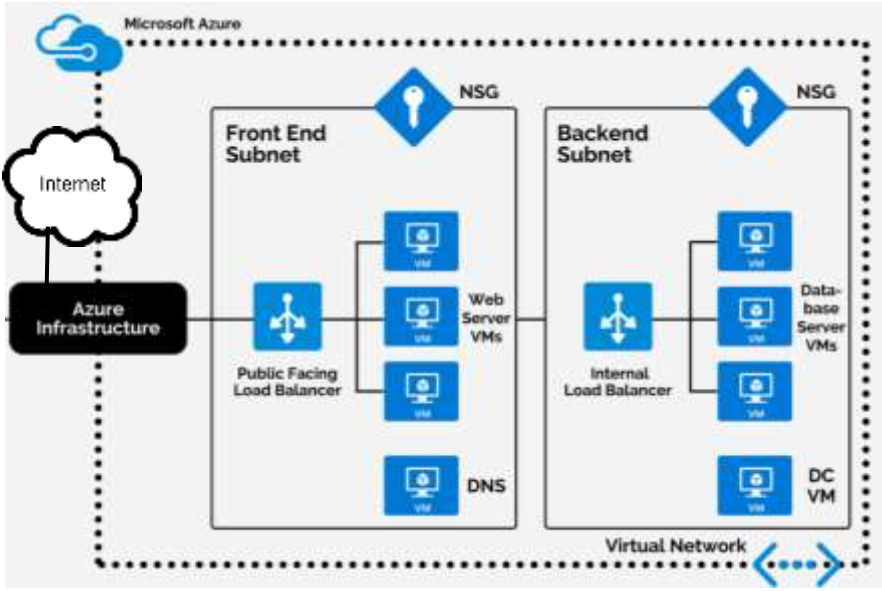
Gambar 9.5. Oracle Cloud Infrastructure
(sumber: Virtual Cloud Network Overview and Deployment Guide)

VCN memberikan dua cara untuk menghubungkan jaringan ke inrastruktur Oracle Cloud, yaitu:

1. VPN connect: memberikan multiple IPSec tunnel antara jaringan dan VCN. Dynamic Routing Gateway (DRG) yang dibuat oleh user dapat ditempelkan kepada VCN
2. Oracle Cloud Infrastructure FastConnect: memberikan sebuah koneksi private antara jaringan yang sudah ada dengan Oracle Cloud Infrastructure.

9.3.2 *Azure Virtual Network* (VNet)

Perusahaan besar Microsoft membuat *Azure Virtual Network*, yaitu sebuah servis yang menyediakan fundamental building block untuk jaringan private di azure. Sebuah instance dari service virtual network dapat membuat beberapa tipe resouce untuk berkomunikasi satu sama lain secara aman melalui internet maupun jaringan lokal. Sumber daya dari azure ini mencangkup *Virtual Machine* (VM). Sebuah virtual network bekerja mirip dengan jaringan tradisional yang digunakan di dalam data center. Tapi *virtual network* memberikan manfaat tambahan pada infrastruktur azure seperti scalability, availability dan isolation.



Gambar 9.6. Azure Virtual Network (VNet)
(sumber: Microsoft.com)

Azure Virtual Network mempunyai kemampuan untuk mendukung beberapa koneksi jaringan yang berbeda. Berikut ini adalah beberapa konetivitas yang didukung oleh Vnet :

1. Komunikasi internet
   Azure memiliki fungsi default untuk melakukan outbound communication ke internet publik dengan semua sumber daya yang terdapat dalam Vnet. Untuk melakukan inbound communication, seorang user harus menetapkan IP publik atau load balancer.
2. *Azure Resource Communication*
   Azure dapat membuat seorang user untuk berkomunikasi dengan sumber daya yang dimilikinya di dalam sebuah *virtual network, virtual network service end-point, dan VNet Peering*.

3. Komunikasi on-premise resource
   Virtual network yang dimiliki oleh azure memberikan pilihan yang berbeda kepada user untuk mengkoneksikan jaringan lokal dengan beberapa metode konektivitas seperti *Site-site* VPN, *Point-to-site* VPN, *Azure ExpressRoute*.
4. *Netork Traffic Routing dan Filtering*
   VNet terdiri dari beberapa tools yang membantu user untuk melakukan routing dan filtering lalu lintas jaringan dalam masing-masing subnet. Filtering dilakukan dengan menerapkan group keamanan atau tool keamanan tertentu. Dengan tools keamanan ini, seorang user akan dapat membuat beberapa VM untuk menjalankan fungsi seperti implementasi WAN optimization, firewall, dan lain sebagainya.
5. Integrasi VNet dengan layanan Azure
   Fitur yang paling utama dari VNet adalah dapat terintegrasi langsung dengan layanan azure lain di dalam lingkungan *Azure Virtual Private Cloud* dengan menggunakan satu atau beberapa pilihan yang ada di dalam platform yang telah disediakan. User dapat melakukan deploy dedicated instance dalam sebuah virtual network, lalu dapat diakses melalui jaringan lokal atau jaringan virtual.

DAFTAR PUSTAKA

Larry L. Peterson, Bruce S. Davie. 2011. *Computer Networks A System Approach: Fifth Edition*. Elsevier

A. Shaji George, A. S. Hovan George. 2021. *A Brief Overview of VXLAN EVPN*. IJIREEICE

Mora Gozani. 2016. *Network Virtualizatin for Dummies: Vmware Special Edition*.

Oracle Cloud Infrastructure. 2019. *Virtual Cloud Network Overview and Deployment Guide.* Oracle White Paper

Ankur Chowdary. 2019. *Virtual Networking: From Theory to Practice*. Software-Defined Networking and Security

Buresh, dkk. *A Modern, Open, And Scalable Fabric VXLAN EVPN*. Cisco Book

Fernando Lama Ruano. 2017. *Reation Of A Virtual Overlay Network With SDN And VXLAN*

Andry Maulana, Ahmad Fauzi. 2018. *Buku Jaringan Komputer*.

Deploy dedicated Azure services into virtual networks. https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-for-azure-services

Virtual Cloud Network. https://www.oracle.com/id/cloud/networking/virtual-cloud-network/

Virtual Networking. https://www.vmware.com/topics/glossary/content/virtual-networking.html

BAB 10
PENGELOLAAN JARINGAN

Oleh Iwan Adhicandra

10.1 Pendahuluan

Di era digital saat ini, jaringan telah menjadi bagian integral dari kehidupan sehari-hari, memungkinkan individu dan organisasi untuk terhubung, berkomunikasi, dan berkolaborasi dengan mudah. Dengan meningkatnya kompleksitas dan skala jaringan, kebutuhan untuk mengelolanya dengan efisien menjadi semakin penting. Dalam konteks ini, mari kita pelajari lebih lanjut tentang pengelolaan jaringan.

10.1.1 Definisi Pengelolaan Jaringan

Pengelolaan jaringan adalah serangkaian aktivitas, metode, prosedur, dan alat yang digunakan untuk mengoperasikan, mengelola, memelihara, dan mengadministrasikan infrastruktur jaringan. Hal ini mencakup pemantauan kinerja jaringan, deteksi dan perbaikan kesalahan, konfigurasi dan pemeliharaan perangkat keras jaringan, serta keamanan jaringan.

10.1.2 Tujuan dan Manfaat

Optimalisasi Kinerja Jaringan: Melalui pemantauan dan analisis kinerja jaringan secara berkelanjutan, organisasi dapat memastikan bahwa jaringan berfungsi pada kapasitas optimal dan memenuhi standar layanan yang ditetapkan.

Deteksi dan Pemulihan Cepat dari Gangguan: Dengan alat dan prosedur yang tepat, gangguan jaringan dapat dideteksi dengan cepat dan pemulihan dapat dilakukan segera, mengurangi downtime dan gangguan terhadap aktivitas bisnis.

Keamanan dan Perlindungan Data: Mengelola keamanan jaringan adalah prioritas utama. Hal ini melindungi data organisasi dari ancaman eksternal, seperti serangan siber, dan memastikan integritas dan kerahasiaan data.
Pengurangan Biaya Operasional: Dengan manajemen yang efektif, sumber daya jaringan dapat digunakan dengan lebih efisien, mengurangi biaya operasional dan perawatan.
Kemudahan dalam Skalabilitas: Seiring dengan pertumbuhan organisasi, jaringan mungkin perlu ditingkatkan atau diperluas. Manajemen jaringan yang baik memungkinkan organisasi untuk melakukannya dengan mudah dan efisiensi.
Peningkatan Pengalaman Pengguna: Jaringan yang dikelola dengan baik menawarkan pengalaman pengguna yang lebih baik, dengan latensi yang lebih rendah, kecepatan yang lebih tinggi, dan ketersediaan yang lebih andal.

Dengan memahami pengelolaan jaringan, organisasi dapat memastikan bahwa infrastruktur jaringan mereka tetap handal, aman, dan siap mendukung kebutuhan bisnis mereka sekarang dan di masa depan.

10.2 Komponen Dasar Jaringan

Dalam membangun dan mengelola jaringan, ada beberapa komponen dasar yang perlu dipahami. Komponen-komponen ini bekerja bersama-sama untuk memastikan transmisi data yang efisien dan andal antar perangkat dalam jaringan. Berikut adalah penjelasan lebih lanjut tentang komponen-komponen dasar jaringan:

1. **Perangkat keras**
   Router: Merupakan perangkat yang bertugas menghubungkan jaringan komputer ke jaringan lainnya, termasuk ke internet. Router bekerja pada lapisan jaringan (Layer 3) dari model OSI

dan dapat mengambil keputusan pengalihan berdasarkan alamat IP.

Switch: Berfungsi untuk menghubungkan perangkat dalam jaringan lokal (LAN). Switch bekerja pada lapisan data link (Layer 2) dan memungkinkan perangkat untuk berkomunikasi dengan satu sama lain melalui frame Ethernet.

Hub: Perangkat yang lebih sederhana dibandingkan dengan switch, hub menghubungkan perangkat dalam LAN dengan mengirimkan data yang diterimanya ke semua port lainnya. Akibatnya, hub kurang efisien dibandingkan switch.

2. Perangkat lunak

Sistem Operasi Jaringan: Seperti Cisco IOS atau JunOS, yang berfungsi untuk mengoperasikan perangkat keras jaringan dan memberikan layanan serta fungsionalitas yang diperlukan untuk transmisi data.

Software Monitoring: Aplikasi yang digunakan untuk memantau kinerja, trafik, dan status dari berbagai komponen jaringan. Contohnya termasuk Nagios, SolarWinds, dan PRTG Network Monitor.

Software Manajemen Konfigurasi: Aplikasi yang membantu administrator jaringan mengelola konfigurasi perangkat jaringan. Beberapa alat populer termasuk Ansible, Puppet, dan Chef.

3. Media transmisi

Kabel UTP (Unshielded Twisted Pair): Adalah tipe kabel yang paling umum digunakan dalam jaringan LAN. Terdiri dari empat pasang kawat tembaga yang dipilin, kabel UTP seperti kabel kategori 5 (Cat5) atau kategori 6 (Cat6) mendukung transmisi data dengan kecepatan yang berbeda.

Fiber Optik: Menggunakan impuls cahaya untuk mengirimkan data, menawarkan kecepatan transmisi yang jauh lebih cepat

dan jarak yang lebih jauh dibandingkan dengan kabel tembaga. Fiber optik biasanya digunakan untuk backbones jaringan dan koneksi jarak jauh.

Kabel Koaksial: Meskipun kurang umum di jaringan modern, kabel ini masih digunakan dalam beberapa aplikasi, terutama untuk transmisi TV kabel.

Memahami masing-masing komponen ini adalah langkah awal penting dalam merencanakan, mendesain, dan mengelola jaringan yang efisien dan andal.

10.3 Konsep Dasar Pengelolaan Jaringan

Pengelolaan jaringan adalah salah satu aspek krusial dalam jaringan komputer untuk memastikan operasi yang lancar, optimal, dan aman. Ada beberapa konsep kunci yang diperkenalkan untuk memandu proses manajemen ini:

1. **FCAPS**

   FCAPS adalah sebuah model konseptual yang dikembangkan oleh ISO untuk klasifikasi fungsi manajemen jaringan. Ini adalah singkatan dari lima fungsi manajemen utama:

   Fault Management (Manajemen Kesalahan): Tujuannya adalah untuk mendeteksi, melaporkan, dan memperbaiki kesalahan dalam jaringan. Ini melibatkan pemantauan jaringan untuk kesalahan, diagnosa masalah, dan pemulihan dari kesalahan.

   Configuration Management (Manajemen Konfigurasi): Melibatkan pemeliharaan dan manajemen konfigurasi semua perangkat dalam jaringan. Hal ini memungkinkan administrator jaringan untuk melacak dan mengendalikan perubahan dalam jaringan.

   Accounting Management (Manajemen Akuntansi): Berfokus pada pelacakan penggunaan jaringan oleh pengguna individu atau departemen. Tujuannya adalah untuk memfasilitasi

penetapan biaya, alokasi sumber daya, dan pemantauan aktivitas pengguna.

Performance Management (Manajemen Kinerja): Mengukur dan membuat jaringan berfungsi pada tingkat kinerja yang optimal. Ini melibatkan pemantauan lalu lintas jaringan, latensi, bandwidth yang digunakan, dan metrik kinerja lainnya.

Security Management (Manajemen Keamanan): Melindungi jaringan dari akses yang tidak sah, kerusakan, atau pencurian data. Ini melibatkan implementasi firewall, sistem deteksi intrusi, otentikasi pengguna, dan kontrol akses lainnya.

2. Protokol Pengelolaan Jaringan

Protokol pengelolaan jaringan memungkinkan perangkat untuk berkomunikasi informasi status dan kinerja ke sistem manajemen jaringan. Beberapa protokol pengelolaan jaringan yang umum adalah:

SNMP (Simple Network Management Protocol): Ini adalah protokol standar untuk pengelolaan jaringan yang digunakan pada jaringan IP. SNMP memungkinkan informasi untuk dikumpulkan dari berbagai perangkat jaringan, seperti server, router, dan switch.

NetFlow: Dikembangkan oleh Cisco, NetFlow adalah protokol yang digunakan untuk mengumpulkan dan menganalisis lalu lintas jaringan. Ini memberikan visibilitas ke dalam lalu lintas jaringan, memungkinkan administrator untuk memahami sumber, tujuan, volume, dan jenis lalu lintas.

RMON (Remote Monitoring): Adalah sebuah standar untuk pemantauan jaringan dan analisis informasi lalu lintas. RMON memungkinkan informasi untuk dikumpulkan dari perangkat jarak jauh dalam jaringan.

Syslog: Adalah standar untuk mengirimkan pesan log dari perangkat jaringan ke server log. Ini digunakan untuk pemantauan dan analisis kegiatan perangkat jaringan.

Memahami konsep-konsep dasar pengelolaan jaringan ini memungkinkan organisasi untuk mengelola, mengoperasikan, dan memelihara jaringan mereka dengan cara yang lebih efisien dan efektif.

10.4 Perangkat Pengelolaan Jaringan

Perangkat pengelolaan jaringan merupakan instrumen kunci yang memungkinkan administrator jaringan untuk memantau, menganalisis, dan mengkonfigurasi komponen jaringan dengan efektif. Berikut adalah penjelasan lebih lanjut tentang jenis alat-alat ini:

1. **Alat Pemantauan Jaringan**

   Alat-alat ini membantu dalam pemantauan kesehatan, status, dan kinerja dari berbagai komponen jaringan seperti perangkat keras, server, aplikasi, dan koneksi.

   Nagios: Salah satu platform pemantauan jaringan open source yang paling populer, memungkinkan pemantauan komprehensif dari jaringan, server, dan aplikasi.

   PRTG Network Monitor: Sebuah solusi pemantauan jaringan yang menyediakan berbagai sensor untuk berbagai aspek jaringan dan infrastruktur TI.

   SolarWinds Network Performance Monitor: Solusi berbasis komersil yang menawarkan pemantauan kinerja jaringan mendalam dan alat analisis lalu lintas.

2. **Alat Analisis Jaringan**

   Alat analisis membantu dalam memahami dan mendiagnosis lalu lintas jaringan, masalah kinerja, dan keamanan.

Wireshark: Sebuah analisis lalu lintas jaringan open-source yang memungkinkan perekaman dan pemeriksaan detil paket-paket yang melewati jaringan.

NetFlow Analyzer: Menggunakan protokol NetFlow untuk memantau dan menganalisis lalu lintas jaringan, memberikan wawasan tentang siapa yang menggunakan bandwidth dan apa aplikasi yang paling banyak mengkonsumsinya.

tcpdump: Sebuah alat perekam paket yang memungkinkan penganalisisan lalu lintas jaringan pada tingkat paket.

3. Alat Manajemen Konfigurasi

Membantu dalam pengaturan, perubahan, dan pengelolaan konfigurasi perangkat jaringan.

Ansible: Sebuah platform otomasi IT yang memungkinkan otomatisasi tugas-tugas seperti konfigurasi perangkat jaringan, penerapan aplikasi, dan orkestrasi infrastruktur.

RANCID (Really Awesome New Cisco confIg Differ): Sebuah alat yang memonitor perubahan dalam konfigurasi perangkat jaringan, khususnya perangkat Cisco, dan menyimpan perubahan dalam sistem kontrol versi.

Cisco Prime Infrastructure: Solusi komprehensif dari Cisco untuk manajemen konfigurasi, operasi, dan pemantauan jaringan nirkabel dan kabel.

Pemilihan perangkat pengelolaan jaringan terbaik bergantung pada kebutuhan spesifik, ukuran, dan kompleksitas jaringan, serta anggaran yang tersedia. Dengan menggunakan kombinasi dari alat-alat tersebut, administrator jaringan dapat memastikan operasional jaringan yang lancar, aman, dan optimal.

10.5 Pemeliharaan Jaringan

Pemeliharaan jaringan adalah elemen esensial dalam siklus hidup manajemen jaringan. Upaya pemeliharaan membantu memastikan bahwa jaringan beroperasi dengan andal, aman, dan efisien. Berikut adalah beberapa aspek kunci dalam pemeliharaan jaringan:

1. **Backup & Restore Konfigurasi**
   Membuat cadangan konfigurasi perangkat jaringan adalah langkah penting untuk memastikan bahwa, dalam kasus kegagalan atau kesalahan konfigurasi, ada cara untuk memulihkan jaringan ke keadaan operasional sebelumnya.
   Pentingnya Backup: Dengan memiliki backup konfigurasi yang up-to-date, perusahaan dapat cepat mengembalikan perangkat ke konfigurasi yang diketahui baik setelah kegagalan perangkat atau kesalahan manusia.
   Frekuensi Backup: Sebaiknya lakukan backup secara reguler, khususnya setelah setiap perubahan konfigurasi signifikan.
   Penyimpanan: Cadangan harus disimpan di lokasi yang aman dan, jika memungkinkan, di luar lokasi (off-site) untuk proteksi tambahan.

2. **Pembaruan Perangkat Lunak dan Firmware**
   Pembaruan perangkat lunak dan firmware seringkali diperlukan untuk menambal kelemahan keamanan, memperbaiki bug, atau menambahkan fitur baru.
   Pentingnya Pembaruan: Pembaruan dapat membantu menjaga jaringan agar tetap aman dan berfungsi dengan optimal.
   Pengujian: Sebelum menerapkan pembaruan di seluruh jaringan, penting untuk mengujinya di lingkungan yang terkendali untuk memastikan tidak ada masalah kompatibilitas atau gangguan lainnya.

Jadwal: Pembaruan sebaiknya dilakukan pada waktu-waktu di luar jam kerja atau saat lalu lintas jaringan rendah untuk mengurangi gangguan.

3. **Pemantauan Kesehatan dan Kapasitas Jaringan**
   Memantau kesehatan dan kapasitas jaringan memungkinkan administrator untuk mendeteksi dan menangani masalah sebelum mereka mempengaruhi kinerja atau ketersediaan.
   Peralatan Pemantauan: Menggunakan alat pemantauan jaringan, seperti Nagios atau PRTG, untuk mengawasi status perangkat, utilitas bandwidth, dan metrik kinerja lainnya.
   Pemberitahuan: Konfigurasikan pemberitahuan otomatis untuk menginformasikan administrator tentang kondisi yang memerlukan perhatian, seperti kegagalan perangkat atau lalu lintas yang tidak biasa.
   Pengoptimalan: Berdasarkan data dari pemantauan, lakukan penyesuaian untuk mengoptimalkan kinerja dan kapasitas, misalnya dengan menambah bandwidth, mengganti perangkat yang sudah tua, atau mengubah konfigurasi.
   Pemeliharaan jaringan yang proaktif dapat mencegah banyak masalah dan memastikan bahwa jaringan terus beroperasi dengan kinerja puncak.

10.6 Keamanan Dalam Pengelolaan Jaringan

Keamanan jaringan adalah prioritas utama dalam pengelolaan jaringan. Serangan siber dan ancaman keamanan terus berkembang, sehingga penting bagi organisasi untuk memastikan bahwa jaringan mereka dilindungi dengan baik. Berikut adalah beberapa komponen kunci dari strategi keamanan jaringan:

1. **Pencegahan Serangan dan Ancaman**
   Pembaruan dan Patching: Memastikan bahwa perangkat lunak dan firmware selalu diperbarui adalah salah satu cara

terbaik untuk melindungi jaringan dari kerentanan yang diketahui.

Edukasi Pengguna: Pelatihan pengguna tentang ancaman seperti phishing dan praktik keamanan yang baik dapat mengurangi risiko serangan.

Penilaian Keamanan: Melakukan audit keamanan dan penilaian kerentanan secara berkala untuk menemukan dan memperbaiki potensi celah keamanan.

2. **Firewall dan Sistem Deteksi Intrusi**

Firewall: Sebuah perangkat atau perangkat lunak yang memantau dan mengontrol lalu lintas masuk dan keluar dari jaringan berdasarkan aturan keamanan yang ditentukan.

IPS/IDS (Intrusion Prevention System/Intrusion Detection System): Sistem ini memantau lalu lintas jaringan untuk aktivitas mencurigakan dan dapat memblokir atau memberi tahu administrator tentang ancaman potensial.

Zonasi Keamanan: Menggunakan firewall untuk membuat zona keamanan dalam jaringan, seperti DMZ (De-Militarized Zone), untuk melindungi aset kritis dari akses langsung dari internet.

3. **Otentikasi dan Otorisasi Pengguna**

Otentikasi: Proses memastikan bahwa pengguna atau perangkat adalah siapa yang mereka klaim. Hal ini seringkali dicapai melalui kombinasi username dan kata sandi, kartu pintar, atau metode otentikasi dua faktor.

Otorisasi: Setelah otentikasi, otorisasi menentukan apa yang bisa dilakukan oleh pengguna atau perangkat di jaringan, berdasarkan kebijakan hak akses yang ditentukan.

Manajemen Hak Akses: Menggunakan perangkat seperti LDAP (Lightweight Directory Access Protocol) atau Active

Directory untuk mengatur dan mengenforce kebijakan hak akses pengguna.

Protokol Keamanan: Menggunakan protokol yang aman, seperti HTTPS, SSH, dan TLS, untuk mengenkripsi komunikasi dan melindungi data sensitif selama transmisi.

Keamanan jaringan adalah proses berkelanjutan yang memerlukan pemantauan, adaptasi, dan respons terhadap ancaman yang selalu berubah. Dengan menerapkan pendekatan berlapis dan komprehensif untuk keamanan, organisasi dapat melindungi aset mereka dari ancaman siber yang semakin kompleks.

10.7 Kasus Studi: Implementasi Pengelolaan Jaringan dalam Organisasi XYZ

Latar Belakang

Organisasi XYZ adalah perusahaan multinasional yang bergerak di bidang teknologi. Dengan ribuan karyawan yang bekerja di beberapa lokasi di seluruh dunia, organisasi ini mengandalkan infrastruktur jaringan yang kuat untuk mendukung operasinya. Namun, dengan pertumbuhan pesat dan adopsi teknologi baru, tim TI XYZ merasa perlu untuk meningkatkan pengelolaan jaringannya.

1. **Perencanaan**

   Analisis Kebutuhan: Melalui serangkaian wawancara dengan pemangku kepentingan dan audit jaringan, tim TI mengidentifikasi kebutuhan utama, termasuk kebutuhan keamanan, kinerja, dan kapasitas.

   Pembuatan Blueprint: Berdasarkan analisis kebutuhan, tim TI mengembangkan blueprint jaringan yang mencakup desain topologi, perangkat keras, perangkat lunak, dan protokol yang akan digunakan.

Strategi Keamanan: Mengingat sifat bisnisnya yang sensitif, XYZ merancang strategi keamanan yang komprehensif, termasuk firewall, IDS/IPS, dan solusi otentikasi multi-faktor.
Rencana Implementasi: Tim TI mengembangkan rencana fased dengan jadwal yang jelas, tugas, dan tanggung jawab untuk setiap tahap implementasi.

2. Implementasi

Pengadaan Peralatan: Sesuai dengan blueprint, XYZ mengadakan peralatan jaringan yang diperlukan, termasuk router, switch, server, dan perangkat keamanan.
Pengaturan dan Konfigurasi: Setelah peralatan tiba, tim TI mulai mengatur dan mengkonfigurasi perangkat sesuai dengan rencana yang telah ditetapkan.
Pelatihan: Untuk memastikan transisi yang mulus, tim TI menyelenggarakan sesi pelatihan bagi karyawan tentang fitur-fitur baru dan praktik terbaik dalam menggunakan jaringan.
Transisi: Organisasi XYZ melakukan transisi ke sistem jaringan baru dalam tahapan, memulai dengan departemen-departemen kunci sebelum akhirnya menggulirkannya ke seluruh organisasi.

3. Evaluasi

Pemantauan: Dengan bantuan alat pemantauan jaringan, tim TI mulai memantau kinerja jaringan, mencari tanda-tanda masalah atau kebutuhan optimasi.
Feedback: Tim TI menerima feedback dari karyawan tentang pengalaman mereka dengan jaringan baru, termasuk masalah atau saran perbaikan.
Analisis Kinerja: Setelah beberapa bulan operasi, tim TI melakukan analisis kinerja mendalam, membandingkan metrik sebelum dan sesudah implementasi untuk menentukan perbaikan yang dicapai.

Penyesuaian: Berdasarkan feedback dan analisis, tim TI membuat beberapa penyesuaian untuk meningkatkan efisiensi, keamanan, dan keandalan jaringan.

Kesimpulan

Dengan pendekatan yang terstruktur dan pemikiran mendalam tentang kebutuhan dan tujuannya, Organisasi XYZ berhasil mengimplementasikan pengelolaan jaringan yang lebih efisien dan aman. Keberhasilan ini tidak hanya meningkatkan produktivitas karyawan tetapi juga memberikan dasar yang kuat untuk pertumbuhan dan inovasi di masa mendatang.

10.8 Teknologi Terkini dalam Pengelolaan Jaringan

1. Software-Defined Networking (SDN)

Definisi: SDN adalah pendekatan untuk desain jaringan di mana proses pengambilan keputusan terpusat dan terpisah dari perangkat keras yang sebenarnya, memungkinkan manajemen jaringan yang lebih fleksibel dan responsif.

Keunggulan:

Kontrol Terpusat: SDN menawarkan kontrol terpusat dari seluruh jaringan, memungkinkan administrator untuk memprogram dan mengoptimalkan aliran lalu lintas secara dinamis.

Ketangkasan: SDN memungkinkan organisasi untuk menyesuaikan lalu lintas jaringan sesuai dengan kebutuhan bisnis, seperti mengalokasikan bandwidth lebih banyak untuk aplikasi kritis.

Integrasi dengan Cloud: SDN memudahkan integrasi dengan solusi cloud, mendukung infrastruktur hybrid dan virtualisasi.

2. ***Network Function Virtualization*** **(NFV)**

Definisi: NFV adalah konsep menggantikan fungsi jaringan berbasis perangkat keras (seperti *firewall, load balancer*) dengan solusi berbasis virtual yang berjalan di atas infrastruktur standar.

Keunggulan:

Skalabilitas: Kemampuan untuk menambah atau mengurangi instance fungsional dengan cepat sesuai kebutuhan.

Efisiensi Biaya: Dengan menggantikan perangkat keras khusus dengan solusi virtual, organisasi dapat menghemat biaya modal dan operasional.

Ketangkasan: NFV memungkinkan layanan baru untuk diterapkan dan diuji dengan cepat tanpa perlu investasi perangkat keras baru.

3. **Otomasi Jaringan dengan AI dan ML**

Definisi: Pemanfaatan teknologi kecerdasan buatan (AI) dan pembelajaran mesin (ML) untuk mengotomatiskan tugas-tugas pengelolaan jaringan dan meningkatkan kinerja serta keamanan.

Keunggulan:

Deteksi dan Respons Otomatis: AI dan ML dapat digunakan untuk mendeteksi pola lalu lintas jaringan yang tidak biasa dan meresponsnya secara otomatis, seperti isolasi lalu lintas yang mencurigakan.

Prediksi Kegagalan: Dengan analisis data historis dan real-time, sistem dapat memprediksi potensi kegagalan jaringan dan mengambil langkah-langkah pencegahan.

Optimasi Kinerja: AI dan ML dapat mengidentifikasi area-area di mana jaringan dapat dioptimalkan, menyesuaikan konfigurasi secara dinamis untuk memastikan kinerja optimal.

Manajemen Bandwidth: Teknologi ini dapat memahami kebiasaan penggunaan bandwidth dan menyesuaikan alokasi sumber daya sesuai kebutuhan secara *real-time*.

Teknologi-teknologi di atas menandai era baru dalam pengelolaan jaringan, di mana adaptasi dan otomasi menjadi kunci dalam menjawab tantangan dan kebutuhan yang terus berkembang. Seiring dengan kemajuan teknologi, diharapkan akan ada lebih banyak inovasi yang muncul untuk membuat pengelolaan jaringan lebih efisien, aman, dan responsif.

10.9 Tantangan dan Masa Depan Pengelolaan Jaringan

10.9.1 Tantangan dalam Pengelolaan Jaringan

Kompleksitas Jaringan yang Meningkat: Dengan pertumbuhan IoT (Internet of Things) dan diversifikasi perangkat yang terhubung, jaringan menjadi semakin kompleks untuk dikelola dan dimonitor.

Keamanan: Ancaman keamanan terus berkembang dan menjadi semakin canggih, memerlukan solusi keamanan yang berkelanjutan dan adaptif.

Scalability: Dengan pertumbuhan data dan kebutuhan pengguna, jaringan harus dapat menyesuaikan diri tanpa mengalami gangguan signifikan.

Integrasi Teknologi Baru: Memasukkan teknologi baru seperti SDN, NFV, atau layanan cloud ke dalam jaringan yang ada bisa menjadi tantangan.

Ketergantungan pada Vendor: Terikat dengan solusi vendor tertentu dapat membatasi fleksibilitas dan inovasi.

Keterampilan dan Pelatihan: Teknologi baru memerlukan keahlian baru. Ada kebutuhan konstan untuk pelatihan dan pendidikan bagi tim TI untuk menjaga mereka tetap relevan.

10.9.2 Masa Depan Pengelolaan Jaringan

Otomasi Melalui AI dan ML: Seperti yang disebutkan sebelumnya, otomasi dengan bantuan AI dan ML akan memainkan peran penting dalam pengelolaan jaringan, membantu mendeteksi masalah dan mengoptimalkan kinerja secara real-time.

Jaringan yang Lebih Otonom: Jaringan masa depan mungkin memerlukan sedikit intervensi manusia, dengan keputusan pengelolaan yang dibuat oleh sistem berdasarkan data dan analisis.

Integrasi Cloud: Dengan semakin banyak organisasi yang mengadopsi solusi cloud, pengelolaan jaringan akan semakin terintegrasi dengan layanan cloud, memungkinkan infrastruktur hybrid yang lebih fleksibel.

Pengelolaan Jaringan Terpusat: Dengan teknologi seperti SDN, jaringan akan lebih terpusat, memberikan gambaran holistik dan kontrol yang lebih baik atas seluruh infrastruktur.

Keamanan yang Diperkuat: Mengingat pertumbuhan ancaman keamanan, fokus akan terus ditingkatkan pada solusi keamanan proaktif yang dapat mendeteksi dan menanggapi ancaman sebelum mereka menyebabkan kerusakan.

Integrasi Dengan Teknologi lain: Seiring berkembangnya teknologi seperti edge computing dan 5G, jaringan akan semakin terintegrasi dengan teknologi-teknologi ini, memungkinkan latensi yang lebih rendah dan kinerja yang lebih tinggi.

Secara keseluruhan, masa depan pengelolaan jaringan tampaknya akan dipenuhi dengan inovasi dan perubahan. Meskipun tantangan-tantangan tertentu akan tetap ada, perkembangan teknologi akan terus memberikan alat dan solusi baru untuk mengatasi mereka.

10.10 Kesimpulan

Pengelolaan jaringan adalah aspek kritis dari infrastruktur TI di setiap organisasi. Ini mencakup berbagai elemen, mulai dari komponen dasar seperti perangkat keras dan perangkat lunak,

hingga konsep-konsep tingkat tinggi seperti SDN dan NFV. Dengan pertumbuhan teknologi, ada peningkatan kebutuhan untuk jaringan yang lebih cepat, fleksibel, dan aman.

Namun, dengan kemajuan ini datang tantangan baru. Kompleksitas jaringan, keamanan, integrasi teknologi baru, dan kebutuhan untuk keterampilan baru adalah beberapa hambatan yang dihadapi oleh administrator jaringan saat ini. Terlepas dari tantangan ini, masa depan pengelolaan jaringan tampak cerah dengan otomasi melalui AI dan ML, integrasi cloud, dan pengelolaan jaringan terpusat yang diharapkan mendominasi lanskap tersebut.

Untuk menghadapi tantangan ini dan memanfaatkan peluang yang ada, organisasi perlu memastikan bahwa tim TI mereka dilengkapi dengan pengetahuan dan alat yang diperlukan untuk mengelola jaringan di era modern ini. Dengan demikian, mereka dapat memastikan bahwa infrastruktur jaringan mereka tetap stabil, aman, dan siap mendukung pertumbuhan dan inovasi di masa depan.

DAFTAR PUSTAKA

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

Stallings, W. 2017. Network Security Essentials: Applications and Standards (6th ed.). Pearson.

Hall, D. E. 2003. Network management: principles and practices (2nd ed.). Addison-Wesley.

Clemm, A. 2006. Network Management Fundamentals. Cisco Press.

Subramanian, M. 2010. Network Management: Principles and Practice. Addison-Wesley.

Case, J., Mundy, R., Partain, D., & Stewart, B. 2002. Introduction to version 3 of the Internet-standard Network Management Framework. RFC 3410.

Zhang, Q., Zheng, L., & Boutaba, R. 2010. Cloud computing: state-of-the-art and research challenges. Journal of Internet Services and Applications, 1(1), 7-18.

Kreutz, D., Ramos, F. M. V., Veríssimo, P. E., Rothenberg, C. E., Azodolmolky, S., & Uhlig, S. 2015. Software-defined networking: A comprehensive survey. Proceedings of the IEEE, 103(1), 14-76.

Feamster, N., Rexford, J., & Zegura, E. 2014. The road to SDN. ACM Queue, 11(12), 20.

Jain, R., & Paul, S. 2013. Network virtualization and software defined networking for cloud computing: a survey. IEEE Communications Magazine, 51(11), 24-31.

BAB 11
CLOUD COMPUTING DAN JARINGAN

Oleh Yuniansyah

11.1 Pengantar Cloud Computing

Teknologi komputer dan Internet semakin hari semakin berkembang, salah satu teknologi yang menggabungkan teknologi komputer dan internet adalah cloud computing atau komputasi awan. Beberapa contoh penggunaan cloud computing yang dapat kita gunakan pada aktivitas sehari-hari, diantaranya adalah :

1. **Email**
   Layanan email dapat memudahkan kita untuk mengirim atau menerima surat elektronik. Kita dapat menggunakan layanan ini tanpa harus mengeluarkan biaya, serta dapat menggunakannya dimana saja dan kapan saja melalui perangkat yang terhubung ke Internet. Beberapa layanan email yang dapat kita gunakan adalah : gmail.com, yahoo.com, outlook, 10minute mail dan lainnya.
2. **Layanan Dokumen Online**
   Layanan ini menyediakan aplikasi yang dapat kita gunakan untuk membuat berbagai macam dokumen, seperti file teks, presentasi, spreadsheet dan lainnya yang dapat kita digunakan secara online. Beberapa aplikasi yang biasa digunakan untuk layanan dokumen online, seperti Google Docs, Microsoft Office Online, Zoho Doc dan lain sebagainya.
3. **Layanan Penyimpanan file**
   Jenis layanan ini memungkinkan kita untuk menyimpan file-file di Internet. Kita dapat kapan saja mengakses file-file yang kita butuhkan. Banyak perusahaan teknologi yang

menyediakan layanan ini secara gratis, diantaranya Dropbox, Google Drive, pCloud, Mediafire, one drive dan lainnya.

4. **Layanan Streaming musik**
   Pada layanan ini kita dapat mengakses dan menikmati musik (audio dan video) tanpa harus mendownload file-file nya. Contoh layanan Cloud ini adalah : Spotify, Youtube, Deezer, Pandora, Joox music dan lain sebagainya.
5. **Layanan Cloud gaming**
   Layanan cloud gaming menyediakan aplikasi untuk kita bermain game yang dapat dilakukan dimana saja melalui internet. Untuk menggunakan game-game ini kita tidak dapat menggunakan komputer atau peralatan lainnya yang langsung terhubung ke Server penyedia game online. Contoh penyedia layanan ini adalah : Google Stadia, PlayStation Now, dan Xbox Game Pass.

Teknologi cloud computing banyak memberikan keuntungan bagi pengguna baik individu , oragnisasi maupun perusahaan. Beberapa kelebihan teknologi cloud computing adalah:

1. **Efektif dan Efisien**
   Salah satu alasan penggunaan teknologi cloud computing adalah pengguna tidak perlu memiliki peralatan-peralatan teknologi seperti server, media penyimpanan, jaringan serta tidak perlu juga melakukan konfigurasi server dan jaringan.
2. **Hemat Biaya**
   Penggunaan cloud computing dapat menghemat biaya yang dikeluarkan perusahaan untuk penyimpanan data, untuk pembelian perangkat seperti server dan peralatan serta perawatan peralatan yang diperlukan, karena semua keperluan untuk ini telah disediakan oleh penyedia layanan cloud computing
3. **Kapasitas Penyimpanan**

Salah satu keuntungan lainnya adalah dengan menggunakan cloud computing, pengguna dapat mempunyai tempat penyimpanan yang sangat besar. Penyedia layanan cloud computing menyediakan tempat penyimpanan yang sangat besar dari ratusan Gigabytes (GB) sampai dengan terabytes (TB). Ruang penyimpanan ini jelas sangat dibutuhkan oleh perusahaan-perusahaan besar.

4. **Mempunyai Fitur Backup dan Revovery**
   Penyedia layanan cloud computing menyediakan fitur untuk Backup dan Recovery yang menjamin data pengguna aman terhadap kerusakan ataupun kehilangan data. Fitur ini sangat dibutuhkan oleh perusahaan-perusahaan, karena kerusakan atau kehilangan data dapat menyebabkan kerugian yang sangat besar bagi perusahaan.
5. **Kehandalan Sistem**
   Penyedia layanan Cloud Computing juga memiliki peralatan dan sistem yang sangat baik untuk menjamin sistem yang digunakan dapat berjalan dengan baik dan stabil serta memiliki tingkat downtime yang sangat kecil.
6. **Update Sistem**
   Penyedia layanan cloud computing selalu melakukan proses update sistem secara berkala. Sehingga pengguna selalu mendapatkan fitur terbaru dari sistem yang digunakan. Hal ini tentu memudahkan pengguna untuk bekerja dengan baik.
7. **Meningkatkan Kerjasama**
   Manfaat yang tidak kalah pentingnya menggunakan Cloud Computing adalah memudahkan pengguna untuk bekerja sama dan mengakses data secara bersama sama tanpa dibatasi ruang dan waktu. Teknologi cloud computing memudahkan kolaborasi antar departemen maupun perusahaan yang berada pada beberapa Kota maupun Negara.

11.2 Layanan Cloud Computing

Cloud Computing melakukan virtualisasi komputer server untuk berbagai proses dan penyimpanan. *Cloud Computing* dapat dibedakan menjadi beberapa tipe berdasarkan jenisnya. Berikut ini adalah adalah tipe *Cloud Comptuting* :

1. **Public Cloud**

   Public Cloud adalah layanan *cloud computing* yang disediakan oleh penyedia layanan yang mempunyai infrastruktur jaringan yang tersebar diseluruh Dunia. Layanan ini biasanya bersifat free atau tanpa biaya untuk akses atau kapasitas tertentu, serta dapat digunakan oleh siapa saja yang memiliki akses Internet. Untuk menggunakan layanan Public Cloud dengan fasilitas atau fitur-fitur tambahan kita dapat berlangganan dengan membayar biaya yang telah ditentukan. Contoh pada aktivitas sehari-hari layanan ini adalah Gmail, Google Drive, Youtube dan aplikasi-aplikasi sejenis lainnya.

2. **Private Cloud**

   Private Cloud adalah layanan cloud yang terbatas tidak bersifat terbuka. Layanan Cloud ini hanya dapat digunakan untuk pengguna yang diberikan akses untuk menggunakan layanan. Private Cloud biasanya dapat digunakan dengan cara membayar untuk membeli atau berlangganan layanan yang disediakan. Penyedia layanan Private Cloud biasanya memberikan layanan penyimpanan, akses jaringan dan fasilitas lainnya yang telah disesuaikan dengan paket langganan yang ada. Private Cloud mempunyai tingkat keamanan yang sangat baik kepada para penggunanya. Selain itu keuntungan menggunakan Private Cloud adalah maintenance atau pemeliharaan yang lebih mudah dan pengaturan akses penuh terhadap sumber daya dan perangkat yang digunakan lebih mudah dilakukan oleh perusahaan atau pengguna yang menggunakan layanan ini karena hanya dapat dilakukan didalam organisasi atau pihak yang menggunakan.

Perbedaan yang mendasar antara *Public Cloud* dan *Private Cloud,* yaitu :

a. **Infastruktur**, pada *Private Cloud* infrastruktur layanan dikelola secara khusus untuk suatu organisasi atau perusahaan, berbeda dengan *Public Cloud* yang infrastruktur nya sama untuk semua pengguna yang bisa mengaksesnya.
b. **Fasilitas dan Kemudahan**, layanan *Private Cloud* berbeda dengan *Public Cloud* yang terbatas pada akses dan ruang penyimpanan. Pada Private Cloud akses data pengguna dapat dibatasi sesuai dengan ketentuan organisasi serta ruang penyimpanan data juga bisa disesuaikan dengan kebutuhan
c. **Keamanan**, perbedaan lainnya antara *Public Cloud* dan *Private Cloud* terletak pada sisi keamanan karena *Public Cloud* aksesnya terbuka untuk siapa saja sedangkan *Private Cloud* hanya untuk lingkungan tertentu.
d. **Biaya**, perbedaan yang paling mendasar antara *Public Cloud* dan *Private Cloud* adalah biaya. Untuk menggunakan layanan *Private Cloud* Perusahaan atau organisasi harus mengerluarkan biaya yang disesuaikan dengan kebutuhan. Sedangkan untuk Public Cloud bisa diakses secara gratis.

3. **Hybrid Cloud**

Hybrid Cloud adalah layanan *cloud* yang menggabungkan *Public Cloud* dan *Private Cloud*. Pada *Cloud* model ini perusahaan dapat memiliki pengaturan yang baik pada proses dan penyimpanan data. Pada *Hybrid Cloud* perusahaan dapat menyimpan data yang lebih besar karena telah terintegrasi dengan *Public Cloud* dan *Private Cloud*. Selain itu perusahaan juga akan mendapatkan dukungan keamanan yang lebih baik.

4. ***Community Cloud***
   Community Cloud adalah layanan cloud yang digunakan untuk komunitas atau beberapa organisasi yang memiliki kebutuhan, fasilitas serta keamanan yang sama. *Community Cloud* memungkinkan beberapa organisasi atau perusahaan untuk bekerja pada platform atau proyek yang sama dengan biaya yang lebih murah.

Sedangkan untuk layanan yang dapat digunakan oleh penggunanya secara garis besar dibagi menjadi tiga jenis layanan Cloud Computing , yaitu :

1. ***Software as a Service* (SaaS)**
   Layanan *Software as a Service* adalah layanan perangkat lunak yang dapat digunakan oleh pengguna melalui peralatan yang dimilikinya, seperti komputer, laptop, android dan lainnya. Layanan ini memungkinkan kita untuk bekerja dimana saja secara gratis atau membayar sesuai kebutuhan. Banyak kelebihan dan kemudahan untuk menggunakan layanan ini, seperti pembaruan perangkat lunak yang selalu dilakukan oleh pengembang atau penyedia layanan, menghemat waktu dan biaya operasional, serta dapat meningkatkan kinerja karyawan di perusahaan. Contoh layanan *Software as a Service* adalah : Email, Microsoft Office 365, *Customer Relationship Management* (CRM), *Enterprise Resource Planning* (ERP) dan banyak lagi yang lainnya.

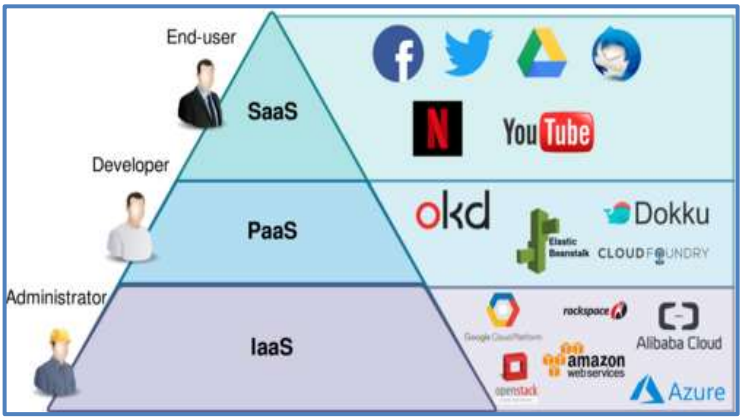
2. ***Platform as a Service* (PaaS)**
   Layanan *Platform as a Service* adalah layanan yang dapat digunakan oleh pengguna untuk mengembangkan atau membangun perangkat lunak atau aplikasi yang sesuai dengan kebutuhan pengguna. Pada layanan ini penyedia menyediakan Platform seperti sistem operasi, database, maupun server yang dapat digunakan oleh pengguna untuk

melakukan hosting aplikasi. Pada layanan ini pengguna dapat menggunakan framework yang disediakan sehingga memudahkan pengguna untuk mengembangkan aplikasi. Beberapa contoh penyedia layanan ini adalah : *Amazon Web Service, Microsoft Azure*, IBM BlueMix, RedHat OpenShift, VMWare dan banyak lagi yang lainnya.

3. Infrastructure as a Service

Layanan *Infatstructure as as Service* adalah layanan *Cloud Computing* yang menyediakan infrastruktur lengkap, seperti server, jaringan, tempat penyimpanan, databse secara virtual. Perusahaan atau organisasi tidak perlu lagi mengeluarkan biaya untuk membeli atau memiliki peralatan yang digunakan untuk keperluan operasional dan penyimpanan data. Perusahaan atau organisasi pengguna hanya cukup membayar biaya berlangganan sesuai kebutuhan.

Berdasarkan level pengguna dari jenis layanan Cloud diatas dapat dibedakan menjadi beberapa tingkatan. Level pengguna pada layanan Cloud Computing dapat dilihat pada Gambar 11.1 berikut ini



Gambar 11.1. Tiga Tingkatan Pengguna Cloud Computing
Sumber : https://www.cetic.be

11.3 Penyedia Layanan Cloud Computing

Saat ini banyak perusahaan yang menyediakan layanan Cloud Computing.

1. Amazon Web Service

Amazon awalnya adalah situs perdagangan yang didirikan oleh Jeff Bezos pada tahun 1995, seiring perkembangan jaman pada tahun 2002 Amazon meluncurkan Amazon Web Service yang menyediakan layanan-layanan berbasis cloud computing atau komputasi awan. Saat ini layanan yang disediakan oleh Amazon Web Service adalah komputasi, penyimpanan, basis data, jaringan dan pengiriman konten, analitik, machine learning dan keamanan. Sebagai perusahaan yang pertama kali mengembangkan layanan cloud computing Amazon Web Service menawarkan kemudahan pada proses pendaftaran, pengelolaan dan pembayaran. Amazon Web Service juga menyediakan layanan gartis untuk mencoba produk-produk layanannya. Kita dapat mengakses layanan ini di https://aws.amazon.com/id/

2. **Microsoft Azure**

Microsoft Azure adalah penyedia layanan cloud computing yang disediakan oleh Microsoft. Platform ini menyediakan layanan-layanan yang biasa digunakan oleh perusahaan-perusahaan teknologi maupun pengguna aplikasi-aplikasi teknologi informasi. Microsoft Azure menyediakan layanan seperti Mesin virtual, komputasi, tools pengembang, database, azure SQL, integrasi, Internet of Thing, manajemen dan tata kelola, Artificial Intelligence dan Machine Learning. Pengguna Microsoft Office juga dapat menggunakan layanan ini untuk bekerja dan menyimpan data-data mereka. Untuk pengguna di Indonesia yang ingin mengetahui produk-produk, biaya dan informasi lainnya kita dapat mengakses layanan Microsoft Azure di halaman https://azure.microsoft.com/id-id/

3. Google Cloud

Google Cloud atau Google Cloud Platform adalah layanan cloud computing yang disediakan oleh Google. Platform ini menyediakan layanan komputasi, penyimpanan, komputasi serverless, database, analisis data, developer tools, pengelolaan API, Artificial Intelligence dan Machine Learning dan layanan lainnya. Untuk melihat produk-produk berserta biaya-biaya nya atau untuk mencoba gratis layanan kita dapat mengakses alaman resmi google gloud di https://cloud.google.com/?hl=id

4. Alibaba Cloud

Alibaba adalah perusahaan teknologi yang awalnya bergerak di bidang e-commerce. Alibaba didirikan Pada Tahun 1999 oleh Jack Ma bersama teman-temannya. Setelah sepuluh tahun tepatnya pada September 2009 Alibaba mengakuisisi HiChina perusahaan layanan infrastruktur internet dan mendirikan Alibaba Cloud. Saat ini banyak layanan yang disediakan oleh Alibaba Cloud, diantaranya Komputasi, Kontainer, penyimpanan, database, analisis data, Internet of Thing, Artificial Intelligence dan Machine Learning, Serverless dan layanan-layanan Cloud Computing lainnya. Untuk melihat layanan atau produk-layanan yang ada beserta informasi biaya dan fasilitas lainnya dapat dilihat di : https://www.alibabacloud.com/id

5. Oracle Cloud Infrastructure

Oracle adalah salah satu perusahaan teknologi yang dikembangkan oleh Lawrence Joseph Ellison. Untuk memberikan layanan *Cloud Computing*, Oracle mengembangkan *Oracle Cloud Infrastructure* (OCI) untuk segala layanan Cloud Computing. Perusahaan ini mempunyai platform yang sangat handal dan memiliki banyak fitur, terutama untuk *Internet of Think* (Iot), *Online Transaction Processing* (OLTP), Machine Learning. Oracle Cloud Infastructure juga menyediakan platform untuk *Software as a Servie* (SaaS) yang sangat baik untuk layanan *Human Capital*

Management (HCM), *Enterprise Performance Management* (EPM), *Supply Chain Management* (SCM) dan aplikasi-aplikasi lainnya. Untuk mendapatkan informasi dan layanan *Cloud Computing Oracle Cloud Infastructure* kita dapat mengakses di halaman : https://www.oracle.com/id/cloud/

6. Indonesian Cloud

Indonesian Cloud adalah salah satu perusahaan layanan *Cloud Computing* yang ada di Indonesia. Perusahaan ini juga menjadi pengembang pertama di Indonesia yang didirikan pada tahun 2011 oleh anak Perusahaan TRG Investama. Indonesian Cloud sebagai salah satu solusi untuk layanan penyimpanan data yang biaya yang ekonomis untuk penyimpanan data yang aman. Layanan ini dapat diakses di https://indonesiancloud.com/

7. Telkom Cloud

Selain *Indonesian Cloud* perusahaan yang menyediakan layanan *Cloud Computing* di Indonesia adalah Telkom Cloud. Telkom Cloud mempunyai dua produk layanan Cloud, yaitu Telkomsigma yang menyediakan layanan inftrstruktur website dan internet, produk ini dapat diakses di : https://www.telkomsigma.co.id/id/home/. dan telkomtelstra yang menyediakan layanan Cloud yang lainnya. Pada tahun 2021 diakuisisi dan berubah nama menjadi Digiserve dan dapat diakses di : https://www.digiserve.co.id/id/

Selain perusahaan-perusahaan ini, masih banyak lagi perusahaan layanan Cloud Computing, diantaranya : EranyaCloud, Zettagrid Indonesia, CBN Cloud, Lintasarta dan lainnya.

DAFTAR PUSTAKA

Bhowmik Sandeep. 2017. Cloud Computing, Cambridge University Press, hal 36-90

Abidah Nuril' Ika, dkk. 2020. Implementasi Sistem Basis Data Cloud Computing pada Sektor Pendidikan, Jurnal Sains dan Teknologi Vol.1 No.2 hal 77-84

Aprianto Ade. 2020. Penerapan Sistem Penyimpanan Cloud Computing Menggunakan Owncloud Untuk Pengolahan Dtaa Pada Universitas Islam Sumatera Utara, Buletin Utama Teknik Vol.16 No.1 hal 47-50

Suhendar Endang . 2022. Tinjauan Sistematis : Implementasi Cloud Computing Terhadap Keamanan Layanan Publik, Jurnal Smart Comp Vol.11 No.4 hal 599-606

Kurniawan Erik. 2015. Penerapan Teknologi Cloud Computing di Universitas : Studi Kasus Fakultas Teknologi Informasi UKDW, Jurnal EKSIS Vol.8 No.1 hal 29-36

Rumetna Supriyanto Matheus. 2018. Pemanfaatn Data Cloud Computing pada Dunia Bisnis : Studi Literatur, Jurnal Teknologi Infomasi dan Ilmu Komputer (JTIIK) Vol.5 No.3 hal 305-314

Bakri Muhammad. 2020. Arsitektur Teknologi Komputasi Awan Untuk Sistem Informasi Layanan Kesehatan daerah, Jurnal Komputer dan Informatika Vol.15 No.1 hal 201-208

BAB 12
INTERNET OF THINGS (IOT) DAN JARINGAN

Oleh Amna

12.1 Pengenalan *Internet of Things* (IoT)

Internet of Things yaitu sebuah konsep yang dimiliki oleh objek tertentu dengan kemampuan untuk transfer atau mengirim data melalui jaringan tanpa membutuhkan interaksi manusia ke manusia atau manusia ke perangkat komputer dalam prosesnya. *Internet of Things* juga sering disingkat sebagai *IoT* (Rachmadi, 2020). Menurut (Yudhanto & Azis, 2019), *IoT* merupakan sebuah penemuan yang bermanfaat untuk menyelesaikan permasalahan dengan menggabungkan antara teknologi dan dampak sosial. Secara infrastruktur global, *IoT* memungkinkan layanan yang dapat tersambung dengan baik secara fisik dan virtual pada apa yang telah ada dan mendukung perkembangan informasi maupun teknologi komunikasi (ICT). Kevin Ashton sebagai pencetus dari *IoT* menjelaskan bahwa *IoT* merupakan sensor yang banyak dan dapat terhubung dengan internet dan berperilaku mirip dengan internet sehingga dapat membuat koneksi-koneksi dan dapat berbagi data dengan bebas sehingga memungkinkan aplikasi-aplikasi baru. Dengan *IoT*, komputer dapat lebih memahami dunia sekitarnya dan dapat menjadi bagian dari kehidupan manusia.

IoT dapat menghubungkan berbagai macam objek yang tersambung di dalam jaringan dengan adanya identitas pengenal serta alamat IP yang dapat membantu setiap objek

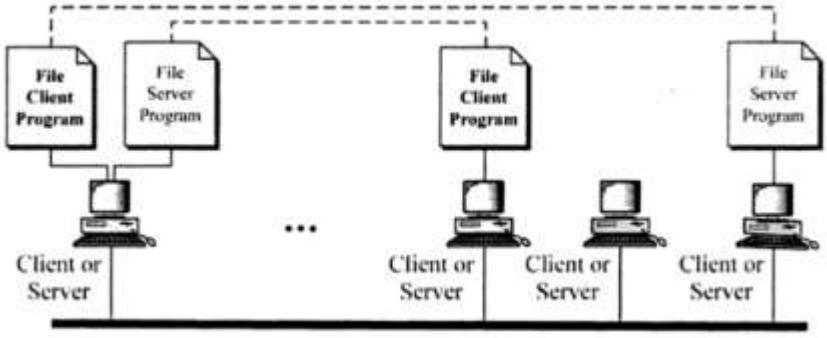
tersebut untuk melakukan komunikasi dan melakukan pertukaran data atau informasi mengenai dirinya atau lingkungan yang diindera oleh objek. Tujuan dilakukannya penyambungan antar objek dalam *IoT* yaitu agar dapat menyediakan layanan-layanan untuk mempermudah dan membantu manusia dalam kehidupan sehari-hari. Istilah "benda" dalam *IoT* dijabarkan sebagai subjek seperti hewan peternakan yang memiliki transponder *biochip* atau mobil yang memiliki *build-in* sensor sehingga dapat memberikan peringatan kepada pengemudi saat tekanan ban rendah. Berkembang pesatnya infrastruktur internet membuatkan tidak hanya *smartphone* atau komputer saja yang dapat terhubung dengan internet, tetapi benda nyata juga dapat tersambung dengan internet seperti mobil, peralatan elektronik, peralatan yang dikenakan oleh manusia (*wearables*), mesin produksi dan lainnya yang dapat terhubung ke jaringan lokal dan global dengan sensor atau akuator tertanam (Adani & Salsabil, 2019).

12.2 Pengenalan Jaringan

Jaringan komputer adalah hubungan antar dua buah simpul atau lebih yang umumnya berupa komputer dengan tujuan untuk melakukan pertukaran data atau informasi. Jaringan komputer digunakan ketika ingin berbagi sumber daya, berkomunikasi atau mengakses informasi yang diinginkan. Tujuannya yaitu untuk mencapai tujuan dengan memanfaatkan jaringan komputer maka komputer dapat meminta dan memberikan layanan (*service*). Klien dapat meminta atau menerima layanan maka *server* akan memberikan atau mengirimkan permintaan tersebut kepada klien. Menurut Indra W (2012), jaringan komputer merupakan kelompok komputer dan peralatan lain yang tersambung sehingga membentuk sebuah kesatuan sistem. Jaringan komputer dapat membantu perpindahan informasi dan data dari suatu jaringan ke

jaringan yang lain. Misalnya pengguna akan dapat mencetak pada sebuah *printer* yang sama dan menggunakan *printer* tersebut bersama (Doni, 2014).

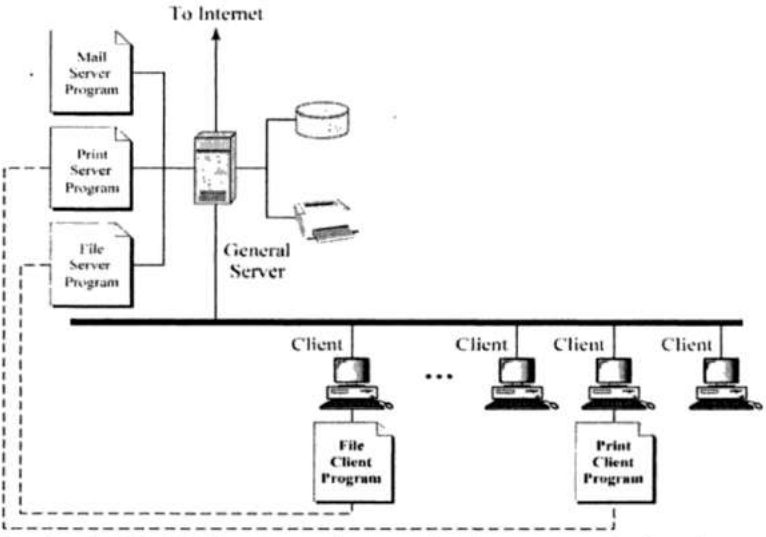
Jaringan komputer memiliki sistem koneksi antar node (komputer) yang bersifat *Peer-to-Peer* dan *Client-Service*. Menurut (Syafrizal, 2005), Jaringan *Peer-to-Peer* yaitu jaringan yang terdiri dari dua komputer atau lebih yang melakukan komunikasi dan pembagian data tanpa melalui sebuah *server*. Dalam jaringan *Peer-to-Peer*, komputer memiliki kebolehan yang sama dan sesi komunikasi tidak dapat berjalan jika ia hanya sendiri tanpa komputer yang lain. Hal ini karena setiap komputer dianggap memiliki kedudukan yang sama dan setiap *peer* dapat menjadi *server* bagi *peer* lainnya yang merupakan klien dalam jaringan tersebut. Untuk komputer yang ada dalam suatu jaringan yang sama akan melakukan sebuah kelompok kerja.



Gambar 12.1. *Peer-to-Peer* (Syafrizal, 2005)

Client-Service merupakan jaringan yang diterapkan dalam jaringan internet dengan sebuah komputer yang bekerja sebagai *server* yang hanya memberikan layanan kepada komputer lainnya. Klien juga akan meminta layanan dari *server* itu. Klien dapat mengakses *server* ketika telah melakukan *login* untuk mendapatkan akses ke *server*. Klien dapat meminta sumber daya

apa saja yang akan diberikan oleh *server* yang akan disesuaikan dengan hak atau otoritas yang diberikan oleh administrator.



Gambar 12.2. Model *Client-Service* dengan sebuah server umum (Syafrizal, 2005)

12.3 Cara Kerja *Internet of Things* (IoT)

IoT bekerja dengan memanfaatkan perintah-perintah yang telah dibentuk ke dalam program atau pemrograman. Program akan saling berinteraksi antara mesin dan perangkat yang telah terhubung dengan internet tanpa ruang dan waktu. Manusia bertugas sebagai pembuat atau pengatur pada interaksi tersebut. Tahapan dalam kerja *IoT* dilakukan dengan menganalisis permasalahan yang ada, membuat desain penyelesaian dari masalah, melakukan perintah-perintah yang dapat dieksekusi oleh program, dan membuat pemeliharaan yang berisi *bug report* seperti log pemakaian dan mencari *error* untuk memperbaiki program agar koneksi yang dimiliki oleh perangkat *IoT* dapat berjalan dengan baik dan tepat (Amane et al., 2023).

Cara kerja IoT terdiri dari 4 komponen yaitu *sensors/devices*, *connectivity*, *data processing* dan *user interface*. Sensor atau perangkat sebagai komponen pertama dapat membantu manusia melakukan pengumpulan data langsung dari lingkungan sekitar dengan tingkat kompleksitas yang berbeda. Sensor dapat mengambil data yang dibutuhkan dari suatu objek yang dapat berbentuk pemantau suhu udara atau sebuah video. Misalnya seperti sensor GPS, sensor bahan bakar dan lainnya. Konektivitas sebagai komponen kedua dimana sensor akan dihubungkan dengan *cloud* melalui media komunikasi seperti *wifi, bluetooth*, satelit, jaringan seluler dan sebagainya. Media komunikasi dapat dipengaruhi oleh jarak, konsumsi daya atau *bandwidth*. Pengolahan data dilakukan setelah pengumpulan data selesai dan akan dihubungkan pada *cloud* sehingga *software* dapat memproses data yang ada. Komponen terakhir yaitu *user interface* yaitu dengan menyediakan pengingat dalam bentuk *alarm* atau email pada pengguna atas apa saja yang terjadi pada sistem *IoT* sebagai salah satu langkah pemeriksaan yang dilakukan pada sistem *IoT.* Ia juga berguna untuk memberikan informasi yang diminta oleh pengguna untuk berinteraksi atau menggunakan perangkat *IoT* yang terhubung pada objek tertentu (Laksmana *et al.,* 2022).

Menurut (Marlina *et al.,* 2022), perintah-perintah yang terdapat dalam program berfungsi agar mesin tidak lagi memerlukan bantuan dari manusia karena mesin dapat mengendalikannya secara otomatis. Manusia cukup menjadi pengawas yang akan memonitor setiap perilaku dan tindakan mesin ketika bekerja. Kendala yang terjadi dalam pengembangan *IoT* yaitu sumber daya yang cukup mahal dan penyusunan yang rumit dan kompleks pada jaringan. Biaya yang dikeluarkan untuk pengembangan terlalu mahal dan *IoT* belum termasuk atau tidak menjadi kebutuhan primer di

semua kota atau negara. Namun, *IoT* masih terus dikembangkan untuk membantu kehidupan sehari-hari.

Gambar 12.3. Aplikasi Berbasis IoT (Marlina et al., 2022)

12.4 Cara Kerja Jaringan

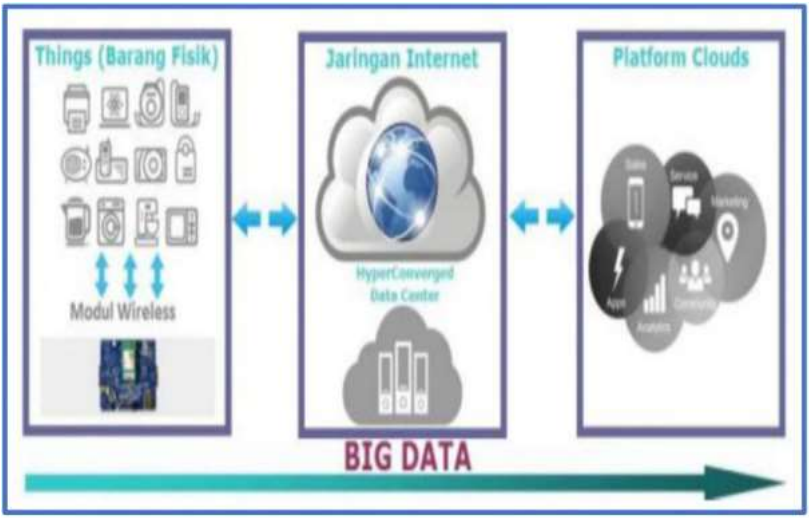
Terdapat dua konsep prinsip kerja dalam jaringan yaitu *Transmission Control Protocol* (TCP) dan *Internet Protocol* (IP). TCP memiliki cara kerja mirip dengan "virtual circuit" dalam jaringan telepon. TCP mementingkan tata-cara dan keandalan pengiriman data antara dua komputer dalam jaringan. TCP tidak mementingkan pekerjaan yang dilakukan oleh IP asalkan kedua komputer dapat berkomunikasi dengan baik dan lancar. TCP akan mengatur agar hubungan komunikasi terbuka dan mengatur jenis aplikasi yang akan dilakukan dalam komunikasi itu seperti mengirimkan *e-mail*, mengirimkan file dan sebagainya. Selain itu, ia juga dapat mendeteksi dan membetulkan kesalahan pada data. TCP bertugas untuk mengatur koneksi semua komputer yang ada

dalam jaringan. Sedangkan IP bekerja dengan cara: dimana data akan dikirimkan melalui rute yang dipilih secara acak sehingga pengirim dan penerima tidak mengetahui jalur yang dilewati oleh data. Rute antar satu data dengan data yang lain bisa jadi sampai ke tempat tujuan tidak bersamaan (Haryanto, 2012).

12.5 Konsep Internet of Things (IoT)

Konsep *Internet of Things* muncul pada tahun 1982 yang dilakukan pada sebuah mesin yang menjual minuman. Mesin minum itu dapat memberikan informasi mengenai stok minuman yang ada di dalam mesin dan mengirimkan laporan melalui internet kepada pemantau mesin sehingga ia tidak perlu membuka atau memeriksa mesin setiap saat untuk mengetahui jumlah atau sisa persediaan minuman yang ada di dalam mesin. Dari perangkat tersebut, konsep *IoT* semakin diperluas dimana perangkat yang terhubung dengan internet dapat digunakan untuk berkomunikasi dan mengumpulkan data (Erwin et al., 2023).

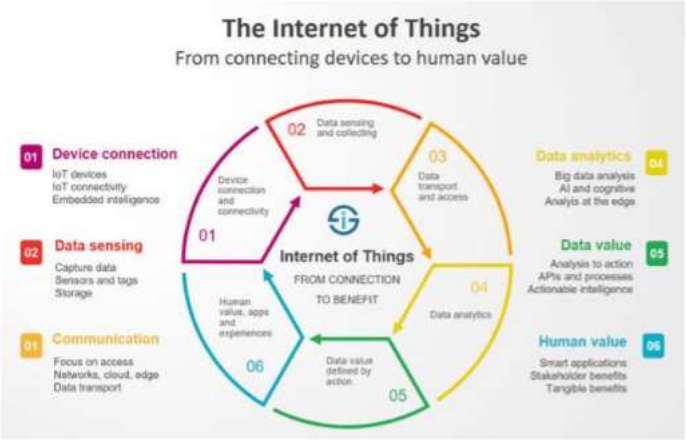
IoT dapat mengirimkan data melalui jaringan internet tanpa perlu adanya interaksi manusia ke manusia atau manusia ke komputer. Konsep *IoT* cukup sederhana dimana terdapat 3 elemen utama dari arsitektur *IoT* yang membantunya dalam bekerja. Elemen pertama yaitu barang fisik yang memiliki modul *IoT* sehingga dapat diakses tanpa kabel. Elemen kedua adalah koneksi internet misalnya modem atau *router wireless speedy*. Elemen yang terakhir yaitu *cloud data center* yang merupakan tempat penyimpanan aplikasi dan basis data (Suparjiman et al., 2023). *IoT* yaitu konsep yang memanfaatkan konektivitas internet yang terhubung dengan tujuan untuk menghubungkan suatu perangkat dengan perangkat lainnya. Perangkat-perangkat yang terhubung membentuk sebuah sistem yang dapat membantu orang ketika mengerjakan suatu tugas atau pekerjaan. Ketika mengimplementasikan konsep *IoT*, diperlukan protokol dalam proses pembagian atau pengiriman data (Hasiholan et al., 2018).



Gambar 12.4. (Suparjiman et al., 2023)

12.6 Infrastruktur Internet of Things (IoT)

Infrastruktur *IoT* yaitu *hardware* yang ditanam (*embedded*) yang memiliki elektronik, perangkat lunak, sensor dan konektivitas. Perangkat dengan *embedded system* dapat membuat komputasi untuk mengolah data menggunakan *input* sensor dan beroperasi dengan infrastruktur internet. Melalui penelitian yang dilakukan oleh Juniper *Research*, perangkat *IoT* bertambah tiga kali lipat dari tahun 2016 hingga 2021 dengan perkiraan sebanyak 46 bilion peralatan *IoT* yang dihubungkan internet baik itu *device,* sensor atau ekuator ((Mahali, 2016).



Gambar 12.5. *Internet of Things* (Mahali, 2016).

Dari definisi Casagras (*Coordination and support action for global RFID-related activities and standardization*) tentang pengertian *IoT* , *IoT* berfungsi sebagai infrastruktur jaringan global yang menghubungkan antara objek fisik dan virtual dengan melakukan pengumpulan data dan komunikasi. Infrastruktur *IoT* terdiri dari jaringan eksisting, *internet* dan pengembangan jaringan. Infrastruktur pada *IoT* dapat memberikan kemampuan deteksi objek, penginderaan serta konektivitas yang umum dalam pengembangan independen layanan dan aplikasi kolaboratif. Hal tersebut dapat dilihat dengan adanya otonomi tinggi pada pengumpulan data, transmisi peristiwa, koneksi jaringan dan interoperabilitas (Megantoro, 2023).

12.7 Internet of Things (IoT) dalam Era 5.0

Di era digital yang semakin mendominasi dunia saat ini, teknologi mempengaruhi hidup dan cara bekerja yang dilakukan oleh manusia. Klien berekspektasi tinggi terhadap layanan yang diterima. Layanan diharapkan dapat lebih mudah diakses, lebih *secure* dan terintegrasi. Industri dan perusahaan yang berbasis

teknologi harus beradaptasi dan mengubah strategi dengan memanfaatkan teknologi digital yang dikembangkan lagi sehingga dapat memenuhi kebutuhan klien yan semakin kompleks dan dapat menjaga keunggulan kompetitif perusahaan dalam bersaing dengan perusahaan lain. Salah satu teknologi yang dimanfaatkan yaitu *IoT* atau *Internet of Things*. *IoT* memberi pengaruh yang besar terhadap cara perusahaan dan industri melayani pelanggan. Ia dapat meningkatkan pengalaman pelanggan atau klien dalam membantu membuat layanan yang mudah diakses, lebih *secure* dan lebih terintegrasi. *IoT* membantu perusahaan dalam mengumpulkan data dari berbagai perangkat dan objek yang terhubung sehingga perusahaan dapat mengetahui dan menganalisa perilaku serta preferensi dari pelanggannya. Hal ini dapat membantu perusahaan untuk menyediakan layanan yang lebih berfokus pada pelanggan yang dimiliki dan membuat pelanggan lebih mudah dan nyaman dalam menggunakan layanannya (Wahyuddin et al., 2023).

Dalam bidang bisnis di era 5.0, *IoT* digunakan untuk menghubungkan antar jaringan dan perangkat fisik seperti sensor, perangkat elektronik dan objek lainnya ke internet sehingga perangkat dapat berkomunikasi dan berbagi data secara *real-time*. Data dikumpulkan dari banyak sumber termasuk juga lingkungan fisik dan infrastruktur agar dapat digunakan ketika harus menganalisis dan melakukan keputusan dengan lebih baik. *IoT* membantu dalam melakukan pertimbangan dalam menghitung biaya pembelian, melakukan implementasi dan pelatihan. *IoT* mampu mengotomatisasikan tugas-tugas rutin, mengoptimalkan rantai pasokan dan meningkatkan efisiensi operasional secara menyeluruh. Memanfaatkan *IoT* dapat membantu industri untuk memaksimalkan layanan yang responsif dan berkualitas tinggi sehingga dapat membantu menciptakan loyalitas pelanggan dengan lebih kuat lagi (Chatra et al., 2023).

Dengan memanfaatkan teknologi *IoT*, industri dan perusahaan dapat terhubung pada pelanggan menggunakan perangkat pintar dan dapat membuat sebuah solusi yang inovatif. Mengenali ketertarikan dan kebutuhan pelanggan dapat membangun identitas *brand* yang lebih kuat. Pengalaman yang diberikan kepada pelanggan menjadi lebih personal seperti memberikan konten tertentu, rekomendasi produk yang sering dicari atau dibeli oleh pelanggan atau layanan tertentu yang dapat memenuhi kebutuhan pelanggan. Selain itu, *IoT* dapat menyiapkan industri atau perusahaan untuk beradaptasi dengan perubahan teknologi, tren pasar dan kebutuhan pelanggan sehingga industri dapat peka dengan perubahan yang terjadi dan mengubah strategi dengan tepat waktu jika dibutuhkan (Fahrurrozi, 2023).

Internet of Thing berpotensi dalam mendukung era digital dalam pendidikan apalagi di masa pandemi Covid-19 yang serta menyiapkan masyarakat dalam menghadapi era *society 5.0*. *IoT* berdampak besar dalam menyelesaikan permasalahan pendidikan yang belum diselesaikan dengan memberikan solusi baru. *IoT* membentuk pengetahuan menjadi sebuah model kolaboratif aktif yang mandiri sehingga dapat membantu dalam melakukan perubahan dalam sistem pendidikan yang diberikan kepada siswa. Hal ini dapat dilihat dengan adanya sistem belajar yang berbasis *e-learning* yang tersusun dan menghubungkan antara basis data dan perangkat pengguna yang mempermudah pemberian atau pemberitahuan informasi yang diberikan oleh dosen atau guru kepada para mahasiswa atau siswanya. Basis data akan menyimpan informasi dari sensor *device IoT* dan data dari mahasiswa. Infrastruktur yang disediakan oleh *IoT* memungkinkan penggunaan data dari sensor yang digunakan oleh mahasiswa untuk keperluan pembelajaran. Komponen infrastruktur pada *e-learning* dan *IoT* tersebut juga akan di satukan menjadi sebuah layanan *IoT* (Arsana, 2021).

12.8 Kelebihan dan Kelemahan Internet of Things (IoT)

Menurut (Marlina et al., 2022), *Internet of Things* dapat memberikan solusi efisien dari permasalahan kompleks dengan sumber daya yang lebih sedikit. Ia dapat mengerjakan tugas tanpa membutuhkan bantuan tugas dari manusia sehingga lebih menghemat waktu. Hal ini bermanfaat agar karyawan perusahaan dapat mengalihkan waktu bekerjanya sehingga menjadi berkurang atau berfokus pada pekerjaan lain yang lebih darurat dan penting. Solusi yang ditawarkan oleh *IoT* bersifat lebih dinamis dan minimalis dengan menyesuaikan dengan gaya hidup manusia zaman sekarang dalam memberikan sebuah layanan atau produk misalnya seperti peralatan elektronik di rumah yang dapat bekerja atau menanggapi perintah manusia hanya melalui suara. Namun, di sisi lain *Internet of Things* dapat terkena serangan atau *hack* di dunia maya sehingga data yang dikandung olehnya dapat saja bocor ke orang yang tidak bertanggung jawab.

Selain memberikan solusi yang efisien, *IoT* juga dapat mengoptimalkan proses produksi dan membantu dalam melakukan penghematan biaya. Ia mampu menganalisis dan mengelola data atau informasi dengan efisien dan akurat. Hal itu dapat membantu manusia dalam meningkatkan kinerjanya dalam suatu bidang pekerjaan. Prediksi dan pemantauan lebih mudah untuk dilakukan sehingga penyediaan layanan yang diberikan kepada masyarakat lebih terarah dan *up-to-date*. Tantangan yang harus dihadapi yaitu interoperabilitas karena adanya perbedaan protokol dalam setiap perangkat yang digunakan dalam ekosistem *IoT*. Pertumbuhan yang cukup cepat pada perangkat yang terhubung dan penambahan data yang semakin banyak dan kompleks juga dapat menjadi tantangan pada *IoT*. Data yang banyak itu haruslah mengandung data yang berkaitan dan dapat digunakan atau diolah sehingga menjadi sebuah informasi yang

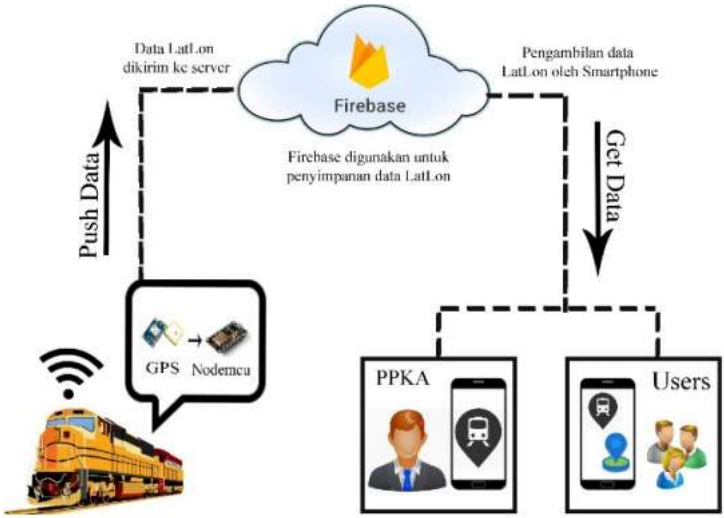
berguna dan mampu memberikan wawasan baru (Erwin et al., 2023).

12.9 Implementasi Internet of Things (IoT)

Mesin memang sejak awal diciptakan untuk membuat pekerjaan manusia lebih mudah dilakukan. Dulu mesin dioperasikan dengan manual sampai akhirnya berkembang sehingga mesin dapat bekerja secara otomatis. Kendala yang terjadi yaitu mengenai jarak dan waktu untuk mesin-mesin terhubung dengan mesin lain yang pada akhirnya ditemukan konsep *Internet of Things* sehingga mesin mempunyai pengenal yang berupa *IP address* melalui jaringan internet dalam mengirimkan dan menerima data. Beberapa implementasi dari *Internet fo Things* yaitu dalam bidang keamanan untuk mengatur sistem, implementasi dalam bidang properti contohnya untuk mengendalikan eskalator, *cctv*, sistem administrasi, kelistrikan dan lainnya. Selain itu, implementasi *IoT* dapat diterapkan dalam bidang medis seperti penggunaan RFID dan NFC *tag* yang disambungkan pada perangkat medis sehingga pengelolaan dan pemeliharaan alat cukup dilakukan dengan memindai alat tersebut (Akmal, 2019).

Perkembangan teknologi terus dilakukan agar masyarakat dan pemerintah siap berekspansi ke beberapa layanan baru yang dapat mendukung kemudahan masyarakat seperti *e-transportation, smarthome, smart business district* dan lainnya. Untuk mencapai dan membangun sebuah *smart city*, diperlukan penerapan dari *Internet of Things* sebagai salah satu atributnya. Dimulai dari menerapkan metode pembayaran secara *cashless* ketika berbelanja. Sistem tersebut menggunakan teknologi NFC atau *Near Field Communication* dan sudah mulai diterapkan oleh perusahaan besar seperti *Apple* dan *Google* dalam bentuk *Android Pay* dan *Apple Pay*. Selain itu, *IoT* telah banyak digunakan untuk mendukung pelayanan publik seperti kartu Jakarta *one card* yang

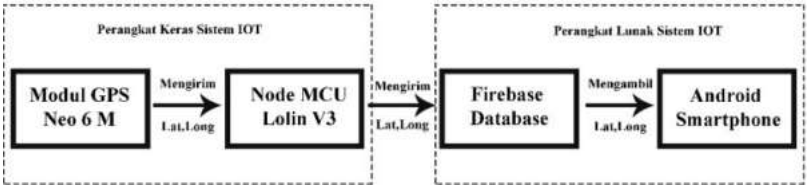
berfungsi sebagai e-KTP, kartu BPJS dan kartu yang dapat digunakan ketika berbelanja di toko yang sudah mendukung kartu tersebut (Fandeli & Muhamad, 2020).



Gambar 12.6. Desain arsitektur penggunaan IoT pada sistem kereta api (Borman et al., 2018)

Internet of Things juga dimanfaatkan dalam mengembangkan sistem kereta api dimana terdapat dua jenis pengguna yang dapat mengetahui data lokasi kereta api dari *database online* Firebase yang dapat diakses melalui *smartphone* dengan memanfaatkan API Google Maps. Pada *database online* Firebase, data ditampilkan setelah data lokasi dibaca oleh modul GPS yang ada pada kereta api. GPS atau *Global Position System* yaitu sistem radio navigasi yang dapat menentukan posisi dengan menyediakan data lokasi dan waktu secara terus menerus di seluruh dunia. Lokasi yang telah dibaca akan disimpan di *database online* Firebase dengan memanfaatkan mikrokontroler Node MCU yang merupakan sistem mikroprosesor yang mengandung CPU,

ROM (*Read Only* Memory), RAM (*Random Acces Memory*), *Interface* untuk *input* atau *output*, *Clock* dan sebuah *chip* yang mengandung peralatan mendukung lainnya (Borman et al., 2018).



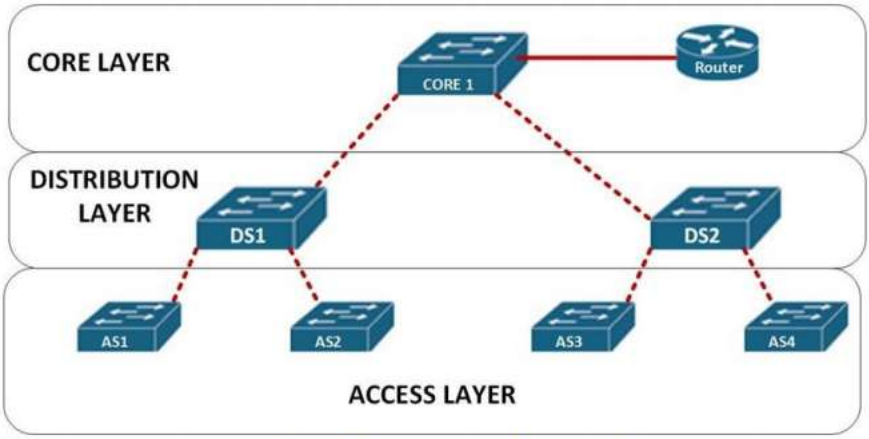
Gambar 12.7. Diagram blok (Borman et al., 2018)

12.10 Internet of Things (IoT) dan Jaringan

Internet of Things memanfaatkan jaringan internet untuk dapat bekerja dan digunakan. Menurut (Junaidi, 2015), Penemuan konsep *IoT* menjadi isu penting yang dibincangkan di internet. Miliaran peralatan atau benda dapat memiliki berbagai jenis sensor yang kemudian terhubung dengan internet melalui jaringan. Konsep *Internet of Things* termasuk ke dalam sistem fisik siber atau dalam kata lain yaitu jaringan di dalam jaringan. Dengan peralatan yang menerapkan konsep *IoT* yang terhubung dengan internet, aliran data dari sensor dapat dikumpulkan dan disimpan secara *real-time* secara otomatis. Tujuannya yaitu agar data mentah yang diperoleh dengan efisien dan merupakan data yang penting dapat dianalisis dan diolah menjadi informasi yang berharga. Informasi tersebut kemudian dapat membawa dampak baik kepada masyarakat maupun pemerintah dalam bidang manajemen ekonomi, produksi, sosial manajemen dan kehidupan pribadi.

Banyak masalah pendidikan yang terjadi di kampus dapat diselesaikan dengan memanfaatkan komputer dan jaringan. Masalah yang timbul dapat melibatkan dosen, mahasiswa atau pegawai kampus misalnya seperti pembelajaran tradisional yang kekurangan interaksi dengan kampus lainnya karena jarak dan cara mengajar guru maupun dosen yang masih kurang. Dengan

menggunakan *Internet of Things*, masalah ini dapat diselesaikan dengan memenuhi aktivitas kampus dengan menghubungkannya dengan *cloud computing*. Jaringan pada ruang lingkup kampus dapat dibentuk dengan *Local Area Network* (LAN). Jaringan dapat menghubungkan antar satu gedung dengan gedung lainnya yang ada di kampus. Jaringan area kampus dapat menggunakan model hirarki tertentu untuk dapat mengoptimalkan jaringan kampus (Sulaiman & Widarma, 2017).



Gambar 12.8. Hirarki jaringan (Sulaiman & Widarma, 2017)

Model hirarki jaringan memiliki tiga lapisan dalam pembentukan jaringannya yang terdiri dari *core layer, distribution layer* dan *access layer*. *Core layer* adalah lapisan sumber internet yang disebarkan ke seluruh wilayah kampus yang memiliki *server*. Layanannya kemudian akan dilanjutkan atau diberikan ke lapisan kedua yang merupakan *distribution layer* yang akan diteruskan pada *end user* yang berada di lapisan *access layer*.

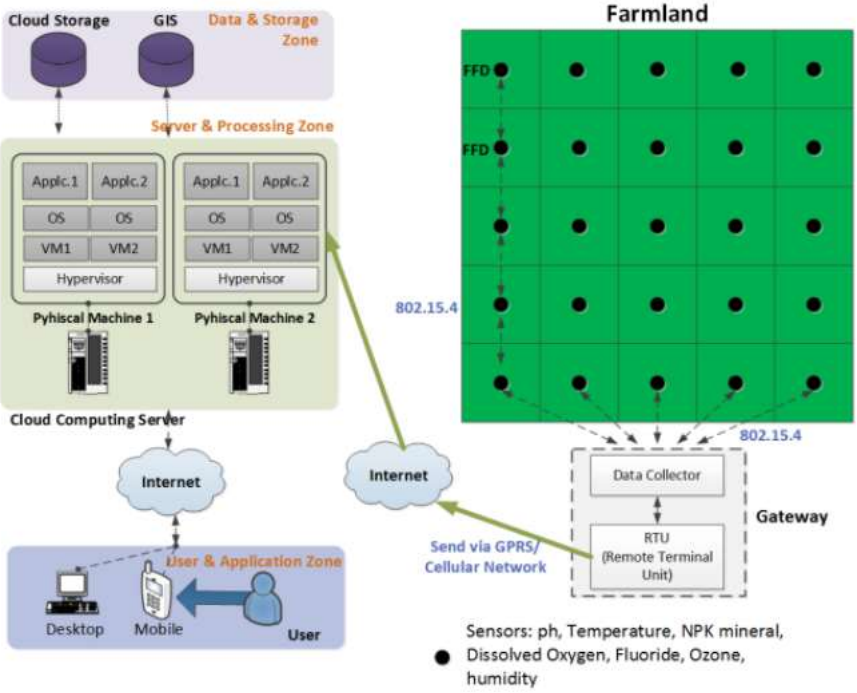
12.11 Internet of Things (IoT) dan Teknologi Jaringan

Dalam *Internet of Things*, teknologi jaringan dan komunikasi memiliki peranan yang penting dalam interkoneksi antar benda pada jarak jauh yang mana komunikasi dapat terjalin hanya dengan adanya bantuan dari internet. Berikut perkembangan teknologi jaringan dan komunikasi yang ada:

1. Teknologi komunikasi *mobile* telah berkembang sejak generasi pertama (1G) pada jaringan analog seluler dan 2G yang digunakan dalam sistem global pada komunikasi seluler yang kemudian berkembang menjadi standar 3G dan 4G.
2. Teknologi jaringan 3G merupakan generasi standar pada telepon seluler dan layanan telekomunikasi seluler dan memenuhi *International Mobile Telecommunications* yang mana layanannya termasuk telepon suara nirkabel area luas, akses internet seluler, panggilan video dan TV seluler.
3. Selanjutnya, Jaringan Area Lokal Nirkabel atau WLAN berkembang yaitu sebuah nirkabel teknologi distribusi dengan spektrum yang tersebar dengan adanya *multiplexing* pembagian frekuensi secara ortogonal (OFDM) untuk mencapai ke banyak perangkat yang terhubung. WLAN memiliki dua mode operasi utama yang dasar yaitu mode infrastruktur dan mode ad *hoc*. Pada mode infrastruktur, unit seluler nirkabel dapat berkomunikasi dari titik akses ke infrastruktur jaringan kabel sedangkan dalam mode ad hoc, unit seluler berkomunikasi secara *peer-to-peer*.
4. Teknologi 4G yaitu integrasi dan pengembangan dari teknologi 3G dan WLAN yang merupakan perpanjangan dari teknologi 3G yang memiliki *bandwidth* dan layanan yang lebih banyak.

5. Teknologi Internet generasi selanjutnya yaitu jaringan global yang digunakan untuk terhubung dengan memanfaatkan protokol internet standar Kontrol Transmisi Protokol/Internet Protokol (TCP/IP). Teknologi jaringan elektronik, nirkabel, dan optik diterapkan untuk membentuk suatu kompositif. Struktur jaringannya mampu mencapai banyak hal seperti jaringan area swasta, publik, lokal, industri, dan nasional. Teknologi ini digunakan dalam pengembangan *IoT* karena *IoT* membutuhkan alamat dalam pengembangannya dan jaringan menjadi salah satu tantangan dalam pengembangan *IoT* (Ning, 2013).

Menurut penelitian yang telah dilakukan (Engel & Suakanto, 2016), membahas mengenai konsep maupun teknologi implementasi *Internet of Things*. Penelitian dilakukan dengan membangun sebuah sistem pertanian cerdas yang menggunakan *sensing* data lingkungan sehingga dapat memudahkan pekerjaan manajemen pertanian.



Gambar 12.9. Arsitektur sistem pertanian cerdas (Engel & Suakanto, 2016)

Arsitektur pertanian cerdas itu terdapat enam modul konsep atau bagian yang terdiri dari pengawasa, pengelolaan, perencanaan, distribusi informasi, sistem pendukung keputusan, dan aksi kendali. Setiap petak lahan berukuran 2x2 meter dan memiliki *node* sensor. *Node* sensor berkomunikasi dengan *gateway* melalui protokol IEEE 802.15.4 dengan perangkat *Remote Terminal Unit* (RTU). Perpindahan data dari *gateway* ke *server* dapat menggunakan GPRS atau EDGE tanpa menggunakan koneksi 3G atau HSPA. *Server* dapat menyimpan data sensor pada basis data. Untuk menjamin ketersediaan *server, server* dapat memanfaatkan *cloud computing* sehingga dapat mempermudahkan konfigurasi.

Pengguna dapat melihat analisis data yang mana data tidak langsung diambil dari sensor tetapi melalui server *cloud*.

12.12 Tren Terkini dalam Internet of Things (IoT) dan Jaringan

Konsep *Internet of Things* memang telah ditemukan sejak dulu, namun pengimplementasian konsep ini terus menerus berkembang dan bertambah banyak. Salah satu tren yang dibahas oleh (Sitompul, 2023), Teknologi *Internet of Things* ini dapat membantu dalam peningkatan efisiensi penggunaan energi. *IoT* dapat menghubungkan antar perangkat-perangkat dengan penggunaan energi tertentu. Salah satu contohnya yaitu sistem pencahayaan, sistem pendingin ruangan, dan perangkat lainnya dengan dukungan jaringan internet. Data dari penggunaan energi dapat diperoleh dan dianalisis sehingga dapat dilakukan riset untuk menemukan cara baru yang akan lebih baik untuk meningkatkan efisiensi energi dan mengurangi konsumsi energi. Hal ini dapat membantu wilayah perkotaan untuk meningkatkan penggunaan teknologi *Internet of Things* sehingga dapat mengurangi pengaruh buruk yang dapat terjadi pada lingkungan sekitar. Beberapa implementasi yang dilakukan di lingkungan kota untuk meningkatkan efisiensi energi yaitu seperti *Smart Grid* atau kelistrikan pintar, pemantauan lingkungan bangunan (suhu, cahaya dan kelembapan), transportasi pintar dan pengelolaan sampah cerdas *IoT*.

Selain itu, *Internet of Things* juga mulai banyak diterapkan di bidang kesehatan sebagai salah satu solusi yang inovatif dan efisien dalam mengetahui atau memantau kesehatan pasien atau orang sakit secara *real-time*. Semakin banyak aplikasi yang bermunculan dengan menerapkan konsep *Internet of Things* dalam mengetahui kondisi pengguna yang ingin mengecek kesehatan tanpa perlu bertemu dengan dokter atau pergi ke rumah sakit. Dari perancangan dan pengembangan yang dilakukan (Laksmiwati,

2023), aplikasi yang dirancang mampu berinteraksi melalui perangkat kesehatan dengan yang dihubungkan oleh jaringan *IoT* yaitu melalui sensor suhu tubuh, deteksi detak jantung dan perangkat untuk melacak aktivitas pengguna. Data yang didapatkan kemudian akan dikirimkan kepada aplikasi dan ditampilkan kepada pengguna secara *real-time*. Dengan menerapkan protokol keamanan yang ketat, dapat membantu mencegah terjadinya pelanggalan privasi dan memastikan data pengguna tetap aman dienkripsi dan disimpan.

Di bidang pertanian, *Internet of Things* dapat mendukung pembudidayaan pertumbuhan tanaman dengan memenuhi beberapa variabel tertentu. Implementasi *IoT* dilakukan untuk menutupi kendala atau kekurangan pengguna dalam mengontrol dan memonitor tanaman tanpa perlu datang ke lokasi. Dengan penggunaan *Internet of Things,* pengguna dapat melihat tumbuh kembang tanamannya. Muncul konsep baru yaitu *smart greenhouse* yang mampu memberikan kondisi dan memodifikasi iklim untuk memberikan kondisi terbaik dan mendukung proses pertumbuhan tanaman yang diletakkan di dalam *greenhouse* dengan menggunakan alat mikrokomputer dan memanfaatkan sensor-sensor yang dapat dikendalikan secara jarak jauh (Nababan et al., 2023).

DAFTAR PUSTAKA

Adani, F. dan Salsabil, S. 2019. Internet of Things: Sejarah Teknologi dan Penerapannya. *Jurnal Isu Teknologi*. 14(2). 92-99.

Akmal. 2019. *Lebih Dekat dengan Industri 4.0*. Penerbit Deepublish: Yogyakarta.

Amane, A. P. O., Febriana, R.W., Artiyasa, I. M., Cahyaningrum, A. O., Husain, Fachruzzaki, M. N. A., Asman, N. A., Ridwan, A., Suraji, I. A., Aritonang, L. dan Srifitriani, A. 2023. *Pemanfaatan dan Penerapan Internet of Things (IOT) di Berbagai Bidang*. Penerbit PT. Sonpedia Publishing: Jambi.

Arsana, N. A. 2021. Internet of Things pada Bidang Pendidikan dalam Masa Pandemi Covid-19 dan Menghadapi Era Society 5.0. *Prosiding Webinar Nasional*. 3. 195-202.

Borman, R. I., Syahputra, K., Jupriyadi dan Prasetyawan, P. 2018. Implementasi Internet of Things pada Aplikasi Monitoring Kereta Api dengan Geolocation Information System. *Jurnal Seminar Nasional Teknik Elektro 2018*. 322-327.

Chatra, M. A., Setiawan, Z., Aulia, M. R., Adhicandra, I., Ariasih, M. P., Antesty, S., Dewi, D. L. P., Ambulani, N., Barlian, A., Waty, E. dan Afriyadi, H. 2023. *Kewirausahaan 5.0: Membangun Keberhasilan Wirausaha pada Era Society 5.0*. Penerbit PT. Sonpedia Publishing: Jambi.

Doni, F. R. 2014. Optimalisasi Jaringan Wireless dengan Router Mikrotik. *Jurnal Sains dan Manajemen*. 2(1). 37-45.

Engel, V. J. L. dan Suakanto, S. 2016. Model Inferensi Konteks Internet of Things pada Sistem Pertanian Cerdas. *Jurnal Telematika*. 11(2). 49-54.

Erwin, Datya, A. I., Nurohim, Sepriano, Waryono, Adhicandra, I., Budihartono, E. dan Purnawati, N. W. 2023. *Pengantar dan Penerapan Internet of Things*. Penerbit PT. Sonpedia Publishing: Jambi.

Fahrurrozi, M. 2023. *Entrepreneurship dan Digitalisasi: Mengembangkan Bisnis di era 5.0*. Penerbit Universitas Hamzanwadi Press: Lombok.

Fandeli, C. dan Muhamad. 2020. *Pembangunan Kota Hijau*. Penerbit Gajah Mada University Press: Yogyakarta.

Haryanto, E. V. 2012. *Jaringan Komputer*. Penerbit ANDI: Yogyakarta.

Hasiholan, C., Primananda, R. dan Amron, K. 2018. Implementasi Konsep Internet of Things pada Sistem Monitoring Banjir menggunakan Protokol MQTT. *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*. 2(12). 6128-6135.

Junaidi, A. 2015. Internet of Things, Sejarah, Teknologi dan Penerapannya: Review. *Jurnal Ilmiah Teknologi Informasi Terapan*. 1(3). 62-66.

Laksmana, I., Jingga, T. Z., Febrina, W., Khomarudin, A. N., Putri, E. E., Nazli, R., Novita, R. dan Amrizal. 2022. *Teknologi Internet of Things (IoT) dan Hidroponik*. Penerbit Goresan Pena: Kuningan.

Laksmiwati, P. 2023. Rancang Bangun Aplikasi Mobile untuk Monitoring Kesehatan Berbasis Internet of Things (IoT). *Jurnal Cyber Area*. 3(2). 1-20.

Mahali, M. I. 2016. Smart Door Locks Based on Internet of Things Concept with Mobile Backend as a Service. *Jurnal Electronics, Informatics, and Vocational Education (ELINVO)*. 1(3). 171-181.

Marlina, E., Afroni, M. J., Noerhayati, E., Choirotin, I., Yunior, Y. T. K., Badri, F. dan Ingsih, I. S. 2022. *Kredensial Mikro Mahasiswa Indonesia: Technopreneurship Berbasis Internet of Things (IoT)*. Penerbit Unisma Press: Malang.

Megantoro, P. 2023. *Aplikasi Sistem Automasi Dasar Berbasis Internet of Things*. Penerbit Airlangga University Press: Surabaya.

Nababan, D., Nipu, V. F. A., Rizald, Baso, B. dan Arisandi, D. 2023. Optimalisasi Kinerja Mikrokomputer Raspberry Pi pada Smart Greenhouse Berbasis Internet of Things (IoT) dengan Algoritma Forecasting Moving Average. *Jurnal Teknologi dan Sistem Informasi Univrab*. 8(2). 164-172.

Ning, Huansheng. 2013. *Unit and Ubiquitous Internet of Things*. Penerbit CRC Press: Florida.

Rachmadi, T. 2020. *Mengenal Apa itu Internet of Things*. Penerbit TIGA Ebook: Lampung.

Sitompul, P. 2023. Analisis Penggunaan Teknologi Internet of Things (IoT) dalam Meningkatkan Efisiensi Energi di Lingkungan Perkotaan. *Jurnal Cyber Area*. 3(7). 1-18.

Sulaiman, O. K., dan Widarma, A. 2017. Sistem Internet of Things (IoT) Berbasis Cloud Computing dalam Campus Area Network. 9-12.

Suparjiman, Nuryanto, I. U. W., Amrullah, Y. A., Ramadhan, N., Anantadjaya, S., Yulianto, A. R., Subariyanti, H., Nugroho, A. dan Ilham, B. U. 2023. *Pengelolaan Sumber Daya Manusia pada Era Internet of Things*. Penerbit Intelektual Manifes Media: Bali.

Syafrizal, M. 2005. *Pengantar Jaringan Komputer*. Penerbit ANDI: Yogyakarta.

Wahyuddin, S., Pasaribu, J. S., Bau, R. T. R. L., Munawar, Z., Hermila, A., Harto, B., Joshua, S. R., Putri, N. I., Safii, M., Amna, Sophian, S., Rukmana, A. Y. dan Hariyadi. 2023. *Layanan Digital di Era 5.0*. Penerbit Global Eksekutif Teknologi: Padang.

Yudhanto, Y. dan Azis, A. 2019. *Pengantar Teknologi Internet of Things (IoT)*. Penerbit UNS Press: Surakarta.

BAB 13
JARINGAN SENSOR DAN AKTUATOR

Oleh Purnawarman Musa

13.1 Pendahuluan

Jaringan komputer modern telah mengalami perkembangan yang pesat, dan pengenalan *Internet of Things* (IoT) telah mengubah cara perangkat terhubung berinteraksi dalam dunia digital (Savitri, 2019). Sensor adalah perangkat yang mengukur berbagai parameter fisik seperti suhu, kelembaban, cahaya, atau gerakan. Di sisi lain, aktuator adalah perangkat yang bertindak berdasarkan informasi yang diterima dari sensor atau perintah dari jaringan. Kombinasi sensor dan aktuator membuka berbagai peluang dalam berbagai aplikasi, termasuk smart home, smart cities, industri otomasi, pertanian pintar, dan kesehatan pintar (Erwin et al., 2023).

Pada pembahasan 0 akan mengeksplorasi peran penting yang dimainkan oleh sensor dan aktuator dalam konteks jaringan komputer yang terhubung, khususnya dalam konteks *Internet of Things* (IoT). IoT telah menjadi salah satu tren terpenting dalam teknologi informasi, dan sensor serta aktuator adalah komponen kunci yang memungkinkan berbagai perangkat untuk berkomunikasi dan berinteraksi dengan dunia fisik.

Dalam era *Internet of Things*, sensor dan aktuator menjadi elemen kunci dalam membangun sistem cerdas dan terhubung secara sistem (Musa and Manurung, 2018). Perkembangan teknologi sensor dan aktuator dimasa depan jaringan komputer semakin cerah dengan potensi inovasi yang tak terbatas dan membuka peluang dalam berbagai aplikasi yang luas.

13.1.1 Peran Sensor

Sensor merupakan mata dan telinga dalam sistem IoT. Sensor adalah perangkat yang mengubah fenomena fisik atau kimia menjadi sinyal elektrik yang dapat diinterpretasikan oleh perangkat elektronik (Kurniawan et al., 2013). Sensor mengumpulkan data dari lingkungan fisik dan mengubahnya menjadi sinyal yang dapat diolah oleh komputer atau perangkat terhubung lainnya. Contoh aplikasi penggunaan sensor meliputi pengukuran suhu dan kelembaban untuk mengendalikan sistem pendingin dalam ruangan, sensor gerakan yang digunakan dalam sistem keamanan rumah pintar, atau sensor kelembaban tanah dalam pertanian pintar.

13.1.2 Peran Aktuator

Aktuator adalah tangan dan kaki dalam sistem IoT. Aktuator adalah perangkat yang mengubah sinyal listrik menjadi aksi fisik dalam lingkungan. Aktuator digunakan untuk merespons data yang diterima dari sensor. Dengan kata lain, aktuator bertindak berdasarkan informasi yang diterima dari sensor atau perintah yang diterima dari jaringan oleh pengguna atau sistem otomatis. Aktuator dapat mengontrol perangkat fisik seperti lampu, kipas, atau perangkat elektronik lainnya. Dalam industri otomasi, aktuator dapat menggerakkan mesin, robot, atau sistem produksi lainnya (Musa, 2023).

13.2 Pengenalan Sensor dan Aktuator dalam Jaringan Komputer

Pengenalan sensor dan aktuator adalah komponen penting dalam jaringan komputer yang berkontribusi pada konsep *Internet of Things* (IoT). Sensor berfungsi untuk mengumpulkan data dari lingkungan fisik, sementara aktuator bertanggung jawab untuk mengendalikan atau merespons lingkungan tersebut berdasarkan data yang dikumpulkan oleh sensor (Alfstudio, 2021). Dalam

jaringan komputer, sensor dan aktuator bekerja bersama-sama untuk menciptakan sistem cerdas yang dapat memantau dan mengontrol berbagai aspek dalam kehidupan sehari-hari. Contoh sensor dan aktuator ditunjukkan pada **Gambar** .

Gambar 13.1. Sensor dan Aktuator
(Sumber: www.belajaronline.net dan www.edukasielektronika.com)

13.2.1 Sensor dalam Jaringan Komputer

Beberapa contoh sensor yang sering digunakan dalam jaringan komputer dan IoT adalah:

1. Sensor Cahaya (*Light Sensor*): Mendeteksi intensitas cahaya disekitarnya. Digunakan dalam otomatisasi pencahayaan, pengaturan kecerahan layar, dan lain-lain.
2. Sensor Suhu (*Temperature Sensor*): Mengukur suhu lingkungan. Digunakan dalam pengendalian suhu dalam ruangan, peralatan pendingin, dan lain-lain.
3. Sensor Kelembaban (*Humidity Sensor*): Mengukur tingkat kelembaban udara. Digunakan dalam sistem pengatur kelembaban, pertanian pintar, dan lain-lain.
4. Sensor Gerakan (*Motion Sensor*): Mendeteksi gerakan manusia atau objek. Digunakan dalam sistem keamanan, pencahayaan otomatis, dan lain-lain.

5. Sensor Gas (*Gas Sensor*): Mendeteksi keberadaan gas tertentu di lingkungan. Digunakan dalam deteksi kebocoran gas, pemantauan kualitas udara, dan lain-lain.

13.2.2 Aktuator dalam Jaringan Komputer

Contoh aktuator dalam jaringan komputer dan IoT meliputi:

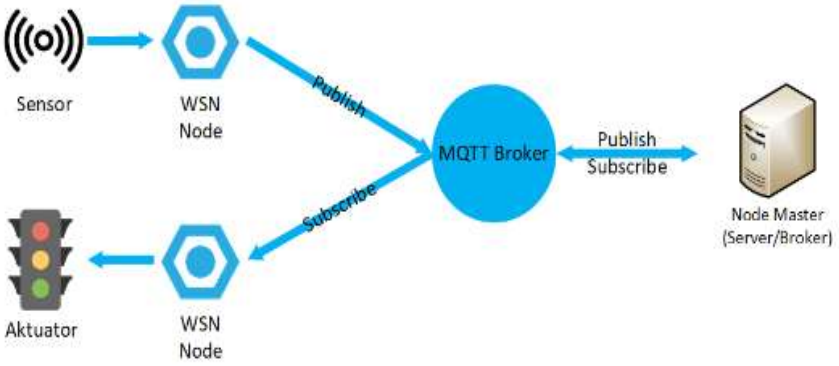
1. Kontroler Pintu (*Door Controller*): Mengendalikan buka-tutup pintu berdasarkan sinyal dari sensor gerakan atau sinyal otentikasi.
2. Kontroler Suhu (*Temperature Controller*): Mengontrol peralatan pemanas atau pendingin berdasarkan data suhu yang diterima dari sensor suhu.
3. Kontroler Pencahayaan (*Lighting Controller*): Mengatur intensitas pencahayaan berdasarkan data sensor cahaya.
4. Katup Pemutus (*Switch Valve*): Mengontrol aliran cairan atau gas berdasarkan informasi dari sensor.
5. Motor Elektrik (*Electric Motor*): Menggerakkan perangkat fisik, seperti kipas atau roda gigi, berdasarkan data sensor dan instruksi kontrol.

13.2.3 Integrasi dan komunikasi dalam Jaringan Sensor dan Aktuator

Sensor dan aktuator berfungsi dalam konteks jaringan komputer yang kompleks. Dalam komunikasi antara sensor dan aktuaktor akan mengirimkan/menerima data ke/dari server atau cloud untuk pemrosesan lebih lanjut dan dapat menerima perintah dari perangkat lain melalui jaringan untuk mentransfer data antara sensor, aktuator, dan perangkat lain dalam jaringan.

Gambar merupakan integrasi dari sensor dan aktuator yang dapat saling berkomunikasi dengan jaringan komputer melalui protokol komunikasi seperti MQTT (*Message Queuing Telemetry Transport*). Data yang dikumpulkan oleh sensor dikirim melalui jaringan untuk dianalisis atau digunakan untuk mengambil

keputusan, dan instruksi kontrol dari aktuator dikirim kembali melalui jaringan untuk mengendalikan perangkat fisik.



Gambar 13.2. Proses komunikasi jaringan sensor nirkabel
(Sumber: teknikelektro.com(Hozanna et al., 2021))

13.2.4 Keamanan dan Privasi

Dalam konteks IoT, kemampuannya untuk terhubung dengan jaringan membawa risiko terhadap potensi serangan siber. Perangkat yang tidak memiliki jaminan keamanan dapat berpotensi menjadi titik pintu bagi pihak yang tidak sah untuk mengakses informasi pribadi, mengambil kendali atas perangkat tersebut, atau bahkan mengakibatkan gangguan pada infrastruktur yang krusial. Penting untuk memperhatikan keamanan dan privasi dalam penggunaan sensor dan aktuator dalam jaringan komputer. Data yang dikumpulkan oleh sensor dapat berisi informasi sensitif, dan rentan terhadap peretasan atau penyalahgunaan. Menerapkan enkripsi, otentikasi, dan protokol keamanan lainnya adalah langkah penting untuk melindungi data dan perangkat. Dalam penggunaannya, perlu diperhatikan jaringan IoT dapat beroperasi dengan aman dan andal. Ketika sensor dan aktuator terhubung dalam jaringan, penting untuk memperhatikan masalah keamanan dan privasi. Data yang dikirimkan oleh sensor harus dienkripsi dan

dikelola secara aman untuk menghindari potensi risiko keamanan. Selain itu, perlu diterapkan mekanisme otentikasi yang kuat untuk menghindari akses yang tidak sah ke aktuator yang dapat mengendalikan perangkat fisik.

13.3 Penerapan sistem *Smart Home* (Rumah Pintar)

13.3.1 Perangkat Sensor pada Rumah Pintar

Smart Home, atau rumah pintar, mengintegrasikan teknologi digital dan jaringan komputer untuk menciptakan lingkungan rumah yang lebih efisien, nyaman, dan terhubung. Sensor-sensor yang terpasang di dalam rumah mengumpulkan data dari lingkungan fisik dan mengirimkannya ke sistem otomatisasi yang mengontrol berbagai perangkat sensor. Sensor-sensor ini berinteraksi dengan sistem otomatisasi dalam rumah pintar. Sistem otomatisasi adalah pusat kontrol yang mengambil data dari sensor-sensor tersebut dan mengirimkan instruksi ke perangkat-perangkat lainnya.

1. Sensor Gerakan (*Motion Sensor*): Sensor gerakan mendeteksi pergerakan manusia atau objek di area tertentu. Dalam rumah pintar, sensor gerakan dapat ditempatkan di berbagai ruangan. Ketika sensor mendeteksi gerakan, sistem dapat mengaktifkan pencahayaan secara otomatis. Misalnya, ketika seseorang akan masuk ke ruangan, sensor gerakan dapat menyala secara otomatis.
2. Sensor Suhu (Temperature Sensor): Sensor tersebut akan mengukur suhu lingkungan. Dalam rumah pintar, sensor suhu dapat membantu mengatur sistem pemanasan/pendinginan. Jika berdasarkan pengaturan suhu turun/naik di bawah/atas ambang tertentu, sistem pemanasan akan diaktifkan, maka sistem dapat menjaga suhu yang nyaman di dalam ruangan di rumah.

3. Sensor Cahaya (*Light Sensor*): Sensor cahaya berfungsi mengukur suatu intensitas cahaya di sekitarnya. Dalam rumah pintar, sensor cahaya dapat digunakan untuk mengatur tingkat pencahayaan. Misalnya, saat hari kondisi di rumah gelap, sistem sensor cahaya dapat mengaktifkan lampu secara otomatis.
4. Sensor Pintu/Jendela (*Door*/*Window Sensor*): Sensor pintu/jendela mendeteksi apakah pintu atau jendela terbuka atau tertutup. Sensor ini dapat digunakan untuk mengirimkan pemberitahuan jika pintu atau jendela dibiarkan terbuka. Ini bisa membantu dalam menjaga keamanan dan menghindari pemborosan energi.

13.3.2 Manfaat Penggunaan Sensor dan aktuator dalam Rumah Pintar

1. Kenyamanan: Sistem otomatisasi diaktifkan membantu penghuni rumah lebih nyaman dengan melakukan tindakan secara otomatis, seperti menyalakan lampu atau mengatur suhu sesuai preferensi.
2. Efisiensi Energi: Penggunaan sensor suhu, cahaya, dan lainnya dapat membantu mengoptimalkan penggunaan energi. Misalnya, sistem secara efisien dapat mengukur suhu ruangan, sehingga menghentikan pemanasan atau pendinginan ketika suhu sudah ideal.
3. Keamanan: Sensor untuk pintu/jendela dan gerakan (aktuator) membantu meningkatkan keamanan dengan memberi tahu pemilik rumah jika ada aktivitas mencurigakan atau jika pintu/jendela terbuka.
4. Kustomisasi: Pengguna dapat mengatur preferensi baik pada sensor atau aktuaor diberbagai situasi. Misalnya, pengguna dapat mengatur pengaturan pencahayaan sesuai dengan waktu hari atau aktivitas yang berbeda.

13.3.3 Tahapan pemanfaatan Sensor dan aktuator di Rumah Pintar dengan Jaringan Komputer

Tahapan dalam konteks penerapan sensor dan aktuator dalam jaringan komputer dalam rumah pintar (*smart home*) melibatkan beberapa tahapan, berikut adalah langkah-langkah yang terlibat dalam program tersebut:

1. Pengumpulan Data dari Sensor:
   Tahap mengakses data yang dikumpulkan oleh sensor-sensor seperti sensor gerakan, suhu, cahaya, dan lainnya. Melalui antarmuka atau protokol yang sesuai dengan jenis sensor yang digunakan. Sensor dapat mengirim data dalam bentuk analog atau digital.
2. Komunikasi Jaringan:
   Data yang dikumpulkan oleh sensor harus dikirim melalui jaringan komputer untuk diolah lebih lanjut. Tahap tersebut melibatkan penggunaan protokol komunikasi seperti MQTT (*Message Queuing Telemetry Transport*), CoAP (*Constrained Application Protocol*), atau HTTP (*Hypertext Transfer Protocol*).
3. Pengolahan Data:
   Data yang diterima dari sensor perlu diolah dalam program. Namun, proses pengolahan data perlu dipastikan tipe data yang didapatkan dari suatu sensor. Apabila jenis sensor analog atau sinyal, maka proses perlu konversi data dari format sensor menjadi format yang dapat diinterpretasikan oleh program, atau pengolahan data lebih lanjut seperti penggabungan data dari sensor-sensor untuk mengambil keputusan.
4. Pengambilan Keputusan:
   Berdasarkan data yang diterima dari sensor, tahapan berikutnya perlu mengambil keputusan mengenai tindakan yang harus diambil. Misalnya, jika sensor mendeteksi aktivitas, program dapat mengaktifkan pencahayaan atau mengirim notifikasi ke pengguna.

5. Pengendalian Aktuator:
   Tahapan ketika suatu keputusan diambil, maka program dapat mengirim instruksi ke aktuator (pengerak) untuk mengambil tindakan fisik. Tahapan tersebut dapat direalisasikan pada fungsi gerakan atau aksi tertentu berupa menghidupkan atau mematikan lampu, mengatur suhu ruangan, atau menggerakkan perangkat fisik lainnya.
6. Respon Kembali ke Pengguna:
   Umumnya tahapan akhir berupa proses atau program yang dapat mengirim respon kembali ke pengguna atau perangkat lainnya melalui jaringan. Misalnya, sistem dapat mengirim notifikasi ke aplikasi ponsel pengguna tentang perubahan status di rumah.

13.3.4 Implementasi Sistem Rumah Pintar dalam Jaringan Komputer

Dalam sub bagian 13.3.4, penulis akan memandang implementasi praktis dari pemanfaatan sensor dan aktuator di dalam sebuah Rumah Pintar yang telah terhubung secara canggih dengan Jaringan Komputer (Dept, 2019). Contoh implementasi langkah-langkah dalam bahasa pemrograman Arduino yang telah umum diterapkan dan mudah dipahami. Dalam pemograman sederhana, ilustrasi implementasi sistem seperti pada gambar 13.3. Penulis mengasumsikan penggunaan Arduino untuk mengontrol lampu berdasarkan sensor gerakan dan suhu badan manusia.

Gambar13.3.. Otomasi Rumah Pintar (kasus: lampu On/Off)
(Sumber:asmag.com)

13.4 Sistem pembacaan data dari sensor

13.4.1 Sensor Deteksi Gerakan seri PIR HC-SR501

Untuk mendeteksi pergerakan objek, program hanya perlu mengevaluasi kondisi deteksi dalam bentuk logika biner, yaitu "ya" atau "tidak," yang diterima dari sensor. Salah satu jenis sensor yang sering digunakan untuk mendeteksi pergerakan ini adalah sensor PIR (*Passive InfraRed*). Sensor PIR memiliki banyak keunggulan, termasuk ukuran yang kecil, biaya yang terjangkau, konsumsi daya yang rendah, dan kemudahan penggunaannya. Oleh karena itu, sensor ini sering digunakan dalam skala rumah tangga maupun bisnis.

Sensor PIR, singkatan dari "Passive InfraRed" sensor, umumnya menggunakan sensor pyroelektrik (seperti yang terlihat pada gambar 13.4) yang sensitif terhadap radiasi inframerah. Semua benda atau makhluk mengeluarkan sedikit radiasi inframerah, tetapi semakin panas objek tersebut, semakin tinggi tingkat radiasi yang dipancarkannya. Sensor PIR ini dibagi menjadi dua bagian untuk mendeteksi pergerakan, bukan hanya tingkat radiasi inframerah secara keseluruhan. Dua bagian ini terhubung satu sama lain, sehingga jika keduanya mendeteksi tingkat radiasi inframerah yang sama, outputnya akan berstatus "LOW." Namun, jika keduanya mendeteksi tingkat radiasi inframerah yang berbeda

(menunjukkan adanya pergerakan), maka outputnya akan berubah secara bergantian antara "HIGH" dan "LOW."

Gambar 13.4. Sensor Deteksi Gerak
(Sumber: Ichibot Store)

Penelitian sebelumnya menemukan kelemahan dari sensor PIR, dimana ketika dimusim panas sensor tidak dapat mendeteksi beberapa manusia, terutama pada masyarakat dari negara India. Kelemahan lainnya dari sensor PIR hanya bisa mendeteksi terjadinya gerak dari suatu objek, sehingga sistem sensor akan mendapat informasi terjadi erakan selain manusia. Hal ini tidak efisien untuk penghematan energi di rumah pintar. Untuk membuat suatu sistem yang dapat efektif, maka perlu didukung oleh sensor yang dapat menunjang prosesnya seperti hanya bisa mendeteksi suhu badan manusia secara global.

13.4.2 Sensor Suhu seri MLX90614

Dalam implementasi program ini, sistem mendapat dukungan dari sensor MLX90614 yang digunakan untuk mendeteksi suhu. Sensor ini termasuk dalam kategori sensor non-kontak, dengan kata lain, sensor ini memungkinkan untuk mengukur suhu objek tanpa harus bersentuhan langsung dengan objek tersebut. Sebaliknya, sensor ini menggunakan sinar

inframerah untuk mengukur suhu objek tersebut (lihat gambar 13.5).

Gambar 13.5. Sensor Deteksi Suhu
(Sumber: nn-digital.com)

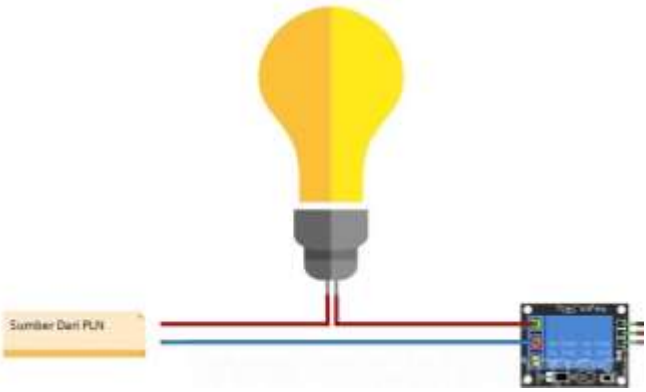
Cara kerja sensor ini terkait dengan kemampuannya dalam hal penyerapan radiasi sinyal dalam bentuk IR (inframerah) yang dipancarkan oleh objek. Prinsip dasarnya adalah bahwa intensitas energi inframerah yang dipancarkan oleh suatu objek akan berbanding lurus dengan suhu objek tersebut. Radiasi inframerah sendiri merupakan spektrum gelombang elektromagnetik yang mencakup panjang gelombang dari 0.7 hingga 1000 mikron. Dalam konteks pengukuran suhu badan seseorang, sistem hanya memanfaatkan pengukuran pada rentang 0.7 hingga 14 mikron.
Untuk mengubah energi inframerah menjadi informasi yang dapat diproses, sensor ini dilengkapi dengan detektor fotosensitif. Detektor ini berfungsi merubah energi inframerah yang diterima menjadi sinyal listrik. Besarnya sinyal listrik ini sebanding dengan suhu objek yang menjadi sumber radiasi inframerah tersebut.

13.4.3 Sistem Aktuator dalam aktivasi lampu

Pengendalian pencahayaan tradisional seringkali melibatkan tindakan manual, seperti menekan sakelar fisik untuk menghidupkan atau mematikan lampu. Namun, dalam era

teknologi yang terkoneksi dalam jaringan komputer, telah mengalami pergeseran menuju kontrol yang lebih maju. Salah satu pendekatan yang muncul adalah mengendalikan pencahayaan menggunakan perintah suara melalui fitur pengenalan suara pada smartphone, yang dapat dilakukan dari jarak jauh melalui koneksi internet. Prinsip kerja dari sistem ini adalah ketika perintah untuk mengontrol pencahayaan diberikan melalui aplikasi khusus pada smartphone, perintah tersebut akan dikirimkan melalui jaringan internet ke server yang relevan. Selanjutnya, server ini akan meneruskan perintah tersebut ke perangkat mikrokontroler, seperti NodeMCU, yang bertugas untuk menjalankan instruksi tersebut, mengaktifkan atau menonaktifkan pencahayaan sesuai dengan keinginan pengguna. Dengan cara ini, kontrol pencahayaan telah berkembang menjadi suatu sistem yang lebih terintegrasi dan terotomatisasi.

Terapan dalam otomatisasi dalam menghidupkan atau mematikan lampu dari suatu lokasi membutuhkan suatu aktuator seperti relay yang ditunjukkan pada gambar 13.6.



Gambar 13.6. Aktuator pengaktif lampu
(Sumber: sekolahotomasi.com)

Relay adalah salah satu jenis aktuator yang umum digunakan dalam aplikasi jaringan komputer, terutama dalam kontrol perangkat fisik seperti lampu, motor, atau peralatan listrik lainnya. Relay terhubung secara fisik antara sumber daya listrik (misalnya, sumber listrik AC atau DC) dan perangkat atau beban yang akan dikendalikan. Ini dilakukan melalui terminal kumparan (*coil*) dan terminal kontak (*contact*). Fungsinya komponen elektromekanik yang digunakan untuk mengontrol aliran listrik ke perangkat atau komponen lain. Relay biasanya memiliki dua set kontak elektrik utama: kontak *Normally Open* (NO), dimana kondisi awal (tanpa energi ke kumparan), kontak NO terbuka. Ini memutuskan aliran listrik ke perangkat atau beban yang dikendalikan. Sedangkan Kontak *Normally Closed* (NC) pada kondisi awal (tanpa energi ke kumparan), kontak NC tertutup.

Relay dapat dikendalikan dari jaringan komputer melalui perangkat seperti mikrokontroler (seperti Arduino atau Raspberry Pi), papan pengembangan IoT, atau modul relay khusus yang terhubung ke jaringan (biasanya melalui protokol seperti MQTT atau HTTP). Ketika perangkat komputer mengirimkan perintah untuk mengaktifkan atau menonaktifkan relay, perangkat tersebut mengirimkan arus ke kumparan relay dan menciptakan medan elektromagnetik yang menggerakkan mekanisme sakelar internal. Akibatnya, kontak relay berubah posisi, mengubah aliran listrik ke perangkat atau beban yang dikendalikan dari jarak jauh melalui koneksi jaringan. Ini memungkinkan pengguna untuk mengendalikan perangkat atau beban dari aplikasi atau perangkat yang terhubung ke internet.

13.4.4 Pemograman Rumah Pintar

Penulis akan merinci langkah-langkah dalam pembuatan program Arduino yang mengilustrasikan penerapan sensor dan aktuator dalam sebuah Rumah Pintar yang terkoneksi dengan Jaringan Komputer.

Untuk membaca suhu dan deteksi gerak serta mengontrol lampu di rumah pintar melalui protokol MQTT dengan Arduino, Anda perlu mengikuti langkah-langkah berikut:

Siapkan Perangkat dan Library:

1. Menghubungkan sistem pengkabelan yang akan dihubungkan pada sensor suhu, deteksi gerak, dan saklar relay untuk lampu.
2. Pastikan Anda memiliki Arduino yang kompatibel dengan koneksi WiFi, seperti Arduino ESP8266 atau ESP32 serta telah menginstal library WiFi, misal ESP8266WiFi.
3. Instal library MQTT di Arduino IDE. Anda dapat menggunakan library seperti "*PubSubClient*" untuk komunikasi MQTT. Instal library ini melalui "Library Manager" di Arduino IDE.

Hubungkan Arduino ke WiFi:

Konfigurasikan koneksi WiFi di Arduino untuk terhubung ke jaringan Wifi Anda. Di bawah ini adalah contoh kode untuk menghubungkan Arduino ke WiFi:

```
#include <ESP8266WiFi.h>

const char* ssid = "NamaWiFi";
const char* password = "PasswordWiFi";

void setup() {
Serial.begin(115200);
WiFi.begin(ssid, password);

while (WiFi.status() != WL_CONNECTED) {
delay(1000);
Serial.println("Connecting to WiFi...");
}
```

```
Serial.println("Connected to WiFi");
}
```

Jika berhasil terkoneksi dan mendapatkan Alamat IP, maka pesan melalui serial komunikasi adalah **Connected to WiFi**. Namun, jika gagal terhubungan ke Wifi, pesan yang ditampilkan selalu berulang-ulang dengan pesan "**Connecting to WiFi...**".

Konfigurasi MQTT:

Konfigurasikan pengaturan MQTT seperti alamat broker MQTT, port, dan informasi otentikasi. Di bawah ini adalah contoh kode untuk menghubungkan Arduino ke broker MQTT:

```
#include <PubSubClient.h>
#include <WiFiClient.h>

const char* mqttServer = "alamat.broker.mqtt";
const int mqttPort = 1883;
const char* mqttUser = "username";
const char* mqttPassword = "password";

WiFiClient espClient;
PubSubClient client(espClient);

void setup() {
// Setup WiFi (seperti pada langkah sebelumnya)

client.setServer(mqttServer, mqttPort);
client.setCallback(callback);
}

void loop() {
if (!client.connected()) {
reconnect();
```

```
}
client.loop();
// Kode utama di sini
}
```

Baris program ini merupakan fungsi mengkoneksikan perangkat dengan server MQTT yang telah ditentukan Port yang digunakan, username dan password saat register. Dengan kelanjutan dari program sebelumnya, maka proses konfigurasi akan proses ketika telah mendapatkan alamat IP. Proses loop() terlihat pada baris 35, dimana menanyakan kondisi perangkat apakah terhubung dengan server MQTT, jika tidak makan akan dihubungkan kembali dengan perintah reconnect(). Apabila hubungan dengan MQTT terhubung, maka akan selalu mengakses topik tertentu dengan perintah reconnect()yang ditunjukkan pada baris 40, dimana prosedur telah tersedia pada library MQTT.

Kode Utama:

Selain itu, program akan mengirimkan data gerakan dan suhu ke topik MQTT yang sesuai. Anda dapat menghubungkan perangkat MQTT klien (misalnya, aplikasi ponsel atau perangkat lain) untuk menerima dan mengirimkan perintah ke Arduino melalui topik MQTT yang telah ditentukan. Di dalam loop utama, dimana pada contoh program sebelumnya tidak terdapat proses utama, kecuali koneksi dengan server MQTT. Tahan selanjutnya Anda dapat mengirimkan data sesuai topik yang ditentukan. Berdasarkan program sebelumnya, pada bari 40 disisipkan program untuk membaca data dari sensor deteksi gerakan dan suhu sebagai berikut:

```
// Membaca status sensor gerakan
int motionStatus = digitalRead(motionSensorPin);

// Membaca suhu dari sensor suhu
float temperature = mlx.readObjectTempC();
```

Baris program untuk proses pembacaan data-data dari setiap sensor yang telah siap membaca dan menerima data dari setiap sensor, maka diteruskan ke tahap pengiriman pada MQTT server untuk dilaksanakan, seperti baris program berikut:

```
// Mengirim data gerakan ke MQTT
if (motionStatus == HIGH) {
  client.publish("rumah/gerakan", "Gerakan Terdeteksi");
}

// Mengirim data suhu ke MQTT
String temperatureMessage = "Suhu: " + String(temperature) + "C";
client.publish("rumah/suhu", temperatureMessage.c_str());

// Menunggu sejenak sebelum mengulang loop
delay(1000);
```

Sistem di rumah pintar terdapat perintah user dapat mengendalikan lampu dari jarak jauh melalui protokol MQTT, dimana Anda dapat menggunakan aplikasi MQTT client pada perangkat Anda (seperti smartphone) untuk mengirim pesan "1" dan "0" ke topik yang telah Anda tentukan dalam kode Arduino. Kode pesan tersebut akan memicu pengontrolan lampu sesuai dengan pesan yang Anda kirim. Program pada perangkat arduino akan membaca terlebih dahulu apakah ada perintah untuk menyalakan atau memadamkan lampu. Contoh pada baris program berikut merupakan program yang akan mengendalikan lampu berdasarkan pesan yang diterima melalui MQTT.

```
// Mengendalikan lampu berdasarkan pesan yang diterima melalui MQTT
if (client.available()) {
  char command = client.read();
  if (command == '1') {
    digitalWrite(lampPin, HIGH); // Menyalakan lampu
```

```
  } else if (command == '0') {
    digitalWrite(lampPin, LOW); // Mematikan lampu
  }
}
```

Perangkat akan menunggu pesan dari broker MQTT yang memberi instruksi untuk mengontrol lampu. Misalnya, jika pesan yang diterima ”1”, maka dapat mengaktifkan lampu, dan jika pesan ”0” dapat mematikan lampu.

Beberapa catatan penting yang harus diperhatikan, yaitu:

1. Pastikan untuk mengganti variabel atau nomor pin dengan label "lampuPin" pada baris program 66 dan 69 sesuai dengan pin Arduino yang digunakan untuk mengendalikan lampu. Dengan langkah-langkah diatas, Anda akan dapat mengontrol lampu dengan menggunakan protokol MQTT melalui jaringan komputer.
2. Pastikan untuk mengganti nilai-nilai seperti ssid, password, mqttServer, mqttUser, dan mqttPassword sesuai dengan konfigurasi Anda. Juga, Anda perlu menginstal library yang diperlukan seperti Adafruit_MLX90614 dan PubSubClient melalui Arduino Library Manager.
3. Untuk mendapatkan data dari sensor yang dikirimkan ke broker MQTT (misal alamat test.mosquitto.org), seorang pengguna (atau aplikasi) dapat menggunakan klien MQTT untuk berlangganan (subscribe) ke topik (topic) yang digunakan oleh perangkat untuk mengirimkan data. Klien MQTT akan menerima pesan yang dikirimkan oleh perangkat ke topik tersebut.

Berikut adalah langkah-langkah umum yang perlu diikuti oleh pengguna untuk mendapatkan data dari sensor melalui broker test.mosquitto.org:

Instalasi Klien MQTT:

Pengguna menginstal klien MQTT pada perangkat atau aplikasi yang akan digunakan untuk berlangganan ke topik MQTT. Beberapa contoh klien MQTT populer termasuk mqtt.js (untuk JavaScript), paho-mqtt (untuk Python), atau aplikasi MQTT client seperti MQTT.fx.

Berlangganan ke Topik:

Pengguna menggunakan klien MQTT untuk berlangganan ke topik yang digunakan oleh perangkat untuk mengirimkan data. Topik ini harus sesuai dengan topik yang diterbitkan oleh perangkat ke broker. Misalnya, jika perangkat Anda menerbitkan data ke topik "rumah/suhu", "rumah/gerakan" dan "rumah/suhu", dimana pengguna harus berlangganan ke topik yang sama.

Menerima Data:

Setelah berlangganan ke topik, klien MQTT akan menerima pesan yang dikirimkan oleh perangkat ke topik tersebut. Pesan tersebut akan berisi data yang dikirimkan oleh sensor.

DAFTAR PUSTAKA

Alfstudio, A., 2021. Perbedaan Sensor dan Aktuator. Tek. Elektro. URL https://www.teknikelektro.com/2021/10/sensor-dan-aktuator.html (accessed 9.13.23).

Dept, M.W., 2019. Improving lighting efficiency in buildings with low-power occupancy-detecting radar sensors - asmag.com Rankings [WWW Document]. URL https://www.asmag.com/rankings/m/content.aspx?id=30803 (accessed 9.13.23).

Erwin, E., Datya, A.I., Nurohim, N., Sepriano, S., Waryono, W., Adhicandra, I., Budihartono, E., Purnawati, N.W., 2023. Pengantar & Penerapan Internet of Things: Konsep dasar & Penerapan IoT di berbagai Sektor. PT. Sonpedia Publishing Indonesia.

Hozanna, G., Nur, D., Kasim, K., 2021. Sistem Monitoring Dan Controlling Lampu Lalu Lintas Berbasis Wireless Sensor Network Menggunakan Lora. Semin. Nas. Tek. Elektro Dan Inform. SNTEI 223–228.

Kurniawan, E., Suhery, C., Triyanto, D., 2013. Sistem Penerangan Rumah Otomatis Dengan Sensor Cahaya Berbasis Mikrokontroler 01.

Musa, P., 2023. Artikulasi Mekanik: Arms, Wrist, End-Effector, in: Robotika. Global Eksekutif Teknologi.

Musa, P., Manurung, A.N.H., 2018. Penerapan Sistem Pemantauan Dan Pengaturan Cerdas Untuk Unsur Hara Pada Sistem Hidroponik NFT. J. Pertan. Presisi J. Precis. Agric. 2. http://dx.doi.org/10.35760/jpp.2018.v2i1.2006

Savitri, A., 2019. Revolusi Industri 4.0: Mengubah Tantangan Menjadi Peluang di Era Disrupsi 4.0. Penerbit Genesis.

BAB 14
PENGGUNAAN JARINGAN KOMPUTER DALAM BISNIS

Oleh Erick Fernando

14.1 Pendahuluan

Jaringan sangat penting bagi kehidupan ini, tetapi harus menguasai konsep komputasi jaringan yang penting (S.Tanenbaum, Feamster and Wetherall, 2020). Organisasi modern tidak hanya menggunakan komputer. Namun, organisasi akan terus berbagi data. Teknologi telekomunikasi memungkinkan pertukaran data, yang sangat menguntungkan perusahaan. Konektivitas menjadikan komputer sebagai alat yang ampuh untuk memperoleh informasi dari ribuan sumber, menjadikan pengguna dan perusahaan lebih produktif. Jaringan dan Internet telah mengubah cara kita berbisnis di bidang manufaktur, jasa keuangan, dan layanan kesehatan, serta industri lainnya. Pemasaran, rantai pasokan, layanan pelanggan, dan manajemen SDM mendapat manfaat dari jaringan. Internet dan jaringan memiliki dampak besar pada kehidupan pribadi dan profesional kita.

Perusahaan modern saat ini sangat memerlukan jaringan komputer. Pertama, sistem komputer jaringan memungkinkan perusahaan beradaptasi terhadap situasi bisnis yang semakin berubah. Perusahaan dapat berbagi perangkat keras, perangkat lunak, dan data antar perusahaan melalui jaringan. Jaringan memungkinkan pekerja jarak jauh berbagi file, ide, dan kreativitas. Berbagi meningkatkan kolaborasi, kreativitas, dan produktivitas. Jaringan menghubungkan bisnis, mitra, dan pelanggan.

Saat ini bisnis membutuhkan jaringan agar dapat berfungsi saling berkomunikasi antar pelanggan, mitra bisnis, pemasok, karyawan, dan pihak-pihak yang terkait harus cepat. Komunikasi bisnis dilakukan melalui layanan surat melalui suara atau faks hingga tahun 1990. Dengan perkembangan saat ini, penggunaan komputer, email, Internet, ponsel pintar, dan perangkat seluler lainnya diperlukan untuk mengimbangi laju yang cepat ini. Terakhir, jaringan akan menghubungkan teknologi-teknologi ini sehingga pengguna dapat berkomunikasi, berkolaborasi, dan bersaing secara global. Maka perdagangan modern sangat bergantung pada jaringan dan Internet.

Maka, Jaringan komputer telah berkembang menjadi landasan suatu bisnis modern saat ini dijalankan. Contohnya, di dunia perdagangan online yang terus berkembang. Karena, memberikan dukungan untuk platform penjualan online, mengoordinasikan proses pembayaran, dan mengawasi tingkat inventaris. Akses terhadap data tentang pelanggan dan analisis pasar yang disediakan. Semua ini, memungkinkan bisnis memberikan informasi yang lebih baik dalam pengambilan keputusan strategis.

Selain itu, Memastikan Jaringan komputer yang aman menjadi sangat penting di dunia yang penuh dengan potensi serangan siber, dunia usaha mempunyai kewajiban untuk melindungi data sensitif dan infrastruktur yang mendukungnya.

Oleh karena itu, jaringan komputer merupakan tulang punggung bisnis modern. Jaringan inilah yang memungkinkan organisasi untuk beroperasi secara efektif, bersaing di pasar yang kompetitif, dan mengatasi rintangan teknologi yang terus berkembang. Hal-hal tersebut merupakan landasan bagi perluasan dan kesuksesan bisnis di era digital saat ini.

14.2 Apa itu Jaringan Komputer ?

Jaringan komputer merupakan rangkaian sistem yang menghubungkan perangkat komputer dengan perangkat lainnya menggunakan media komunikasi (S.Tanenbaum, Feamster and Wetherall, 2020; Kuzmiakova, 2021). Sehingga, data dan informasi dapat dikirimkan dan bertukar diantar satu sama lain. Jaringan komunikasi data dan informasi dapat lebih cepat dengan mempunyai bandwith yang terus meningkat dan lebih murah. Komunikasi data dalam jaringan mengggunakan bandwidth dan mengacu pada kapasitas transmisi (bit per detik). Koneksi internet berkecepatan tinggi selalu aktif melalui fasilitas ISP (Internet Service Provider).

Jaringan Komputer terdiri dari berap jenis yaitu : *personal area networks* (PANs), *local area networks* (LANs), *metropolitan area networks* (MANs), *wide area networks* (WANs), *and the ultimate* WAN, *the Internet*. PANs adalah jaringan jarak pendek dan pada umumnya hanya kisara beberapa meter. Jaringan ini juga digunakan untuk komunikasi antar perangkat yang dekat dengan satu orang. Jaringan dapat berupa kabel atau nirkabel. MANs adalah jaringan yang cukup besar yang mencakup wilayah metropolitan. Jaringan ini bisanya di antara LAN dan WAN. WAN merupakan jaringan yang mencakup wilayah geografis yang sangat luas. Jariangan ini dapat menjangkau seluruh planet dan menjangkau dari Bumi hingga Mars dan sekitarnya (S.Tanenbaum, Feamster and Wetherall, 2020; Kuzmiakova, 2021).

14.3 Jaringan Komputer dalam E-commerce

Pembelian, penjualan, pemindahan, atau pertukaran barang, jasa, atau informasi yang terjadi melalui jaringan komputer seperti Internet merupakan contoh perdagangan elektronik (EC) atau e-commerce. E-commerce membawa perubahan besar tidak hanya pada aspek operasional bisnis tetapi juga pada tugas-tugas penting yang di jalankan, seperti periklanan dan pembayaran

tagihan. Karena sifat pengaruhnya yang ada di mana-mana, hal ini berdampak pada semua bisnis kontemporer. Perusahaan masa depan hampir pasti akan terlibat dalam perdagangan internet, jadi tidak masalah di mana akan bekerja. Banyak sekali dampak yang dirasakan oleh dunia usaha akibat maraknya perdagangan elektronik. Untuk memulainya, hal ini memperluas jangkauan organisasi, yaitu jumlah calon pembeli yang dapat dipromosikan oleh bisnis tersebut. Ini adalah keuntungan yang signifikan bagi bisnis apa pun. Faktanya, e-commerce menawarkan peluang yang tak tertandingi bagi bisnis untuk memperluas operasi secara global dengan biaya rendah, meningkatkan pangsa pasar, dan menurunkan biaya operasional. Maka, memiliki peluang luar biasa untuk memulai bisnis sendiri berkat menjamurnya e-commerce. Di sisi lain, perusahaan e-commerce besar dan terkenal menggunakan Internet untuk bersaing dalam skala global (R. Kelly Rainer Jr., Brad Prince, 2020).

14.4 Manfaat Jaringan Komputer dalam Bisnis

14.4.1 Komunikasi yang Efisien dan mudah

Komunikasi dan kerja sama di tempat kerja telah mengalami revolusi sebagai akibat dari menjamurnya jaringan komputer dan program untuk bekerja bersama, seperti Slack, Microsoft Teams, Zoom dan lain-lainnya. Hal ini memungkinkan berbagai pihak yang terlibat dalam bisnis untuk berkomunikasi dengan cara yang lebih efektif, berbagi file, dan mengadakan pertemuan online. Hal ini telah menghilangkan hambatan komunikasi tradisional (langsung), yang mengakibatkan perubahan besar dalam cara kelompok mengatur konferensi dan proyek kelompok.

Selain itu, perubahan yang disebabkan oleh jaringan komputer dan aplikasi yang memfasilitasi kerja sama juga memengaruhi cara masyarakat beroperasi secara umum. Karyawan tidak lagi dibatasi oleh batasan wilayah atau jam kerja

tradisional. Karena, dapat melakukan tugas kapan saja dan dari lokasi mana saja, lingkungan kerja mempunyai tingkat kemampuan beradaptasi yang lebih besar.

Teknologi jaringan komputer ini juga membantu bisnis menghemat waktu dan uang dengan mengurangi kebutuhan akan pertemuan tatap muka, yang memakan waktu dan biaya. Perjalanan bisnis, yang sering kali diperlukan untuk rapat atau pertemuan kelompok, dapat diminimalkan dengan penggunaan konferensi virtual dan kolaborasi online, yang pada akhirnya mengurangi biaya terkait dan dampak terhadap lingkungan.

Penggunaan jaringan komputer dan aplikasi yang memfasilitasi kolaborasi, secara umum, mempunyai dampak positif terhadap cara perusahaan dan organisasi menjalankan operasional sehari-hari. Maka, memungkinkan tercapainya efisiensi yang lebih tinggi, meningkatkan produksi, dan menciptakan lingkungan kerja yang lebih mudah beradaptasi. Kita dapat mengantisipasi perubahan tambahan dalam cara kita bekerja sama dan berinteraksi di masa depan sebagai akibat dari kemajuan teknologi yang tiada henti.

14.4.2 Memudahkan Proses Pengiriman Data

Proses penyampaian data melalui internet atau perangkat lain dapat disederhanakan dengan menggunakan jaringan komputer. Hal ini dapat dicapai dengan membuat prosedurnya tidak terlalu rumit untuk mencapai tujuan. Transmisi data dapat dilakukan secara tepat waktu dan tanpa adanya hambatan sama sekali bila memanfaatkan jaringan komputer yang kuat yang memungkinkan pembagian informasi secara efektif. Hal ini disebabkan oleh jaringan komputer yang beroperasi dengan sangat efisien dalam waktu dan sumber daya.

14.4.3 Akses Jarak Jauh dan Fleksibilitas Kerja

Dunia bisnis telah banyak berubah dengan diperkenalkannya akses jarak jauh dan pengaturan kerja fleksibel yang dimungkinkan oleh infrastruktur jaringan komputer. Model kerja jarak jauh memungkinkan pekerja melakukan pekerjaan dengan baik dari kenyamanan rumah sendiri atau dari lokasi yang pilihnya, baik di mana pun di dunia. Oleh karena itu, dunia usaha kini memiliki akses terhadap talenta yang berasal dari berbagai konteks dan lokasi, sehingga terbentuklah tim multikultural yang bekerja di seluruh dunia.

Selain itu, dunia usaha telah mampu menerapkan gaya kerja yang lebih responsif karena adanya peningkatan fleksibilitas kerja baik dari segi jadwal maupun lokasi. Misalnya, tim dapat segera beradaptasi dengan perubahan pasar atau kebutuhan pelanggan tanpa dibatasi oleh batasan lokasi yang ditentukan oleh lokasi fisik.

Namun demikian, transisi ke model kerja jarak jauh juga membawa permasalahan baru, termasuk manajemen kinerja jarak jauh, pemantauan produktivitas, dan perlindungan keamanan informasi. Agar dunia usaha berhasil menerapkan dan mempertahankan pengaturan kerja seperti ini, maka perlu merumuskan peraturan yang dipertimbangkan dengan cermat serta membangun dan memelihara infrastruktur teknologi yang aman.

Secara keseluruhan, akses jarak jauh dan fleksibilitas kerja yang dimungkinkan oleh jaringan komputer telah membawa perubahan signifikan dalam cara organisasi beroperasi. Perubahan ini menghasilkan lebih banyak kebebasan bagi karyawan, akses terhadap talenta dari seluruh dunia, dan peningkatan efisiensi operasional.

14.4.5 Arus informasi menjadi cepat

Pemanfaatan jaringan komputer dalam suatu perusahaan atau organisasi lainnya mengarah pada percepatan arus informasi di seluruh perusahaan atau organisasi. Hal ini disebabkan oleh sifat penerapan teknologi jaringan yang ada di mana-mana. Jaringan ini memungkinkan transfer informasi, yang tidak hanya memungkinkannya berjalan lebih cepat tetapi juga membebaskannya dari batasan yang ditentukan oleh variabel geografis seperti jarak dan lokasi. Karyawan atau anggota staf tidak lagi perlu berpindah secara fisik dari satu area ke area lain untuk memperoleh informasi karena informasi dapat mengalir dengan bebas antar divisi atau cabang berkat jaringan komputer yang mendukung aliran informasi yang bebas tersebut. Dengan kata lain, karyawan atau anggota staf tidak perlu lagi berpindah secara fisik dari satu lokasi ke lokasi lain untuk memperoleh informasi. Sebagai konsekuensi langsung dari hal ini, karyawan atau staf tidak perlu lagi berpindah secara fisik dari satu lokasi ke lokasi lain untuk memperoleh informasi. Hal ini disebabkan oleh fakta bahwa jaringan komputer memungkinkan informasi untuk dengan mudah berpindah antar beberapa departemen atau komponen yang berbeda.

14.4.6 Keamanan Data

Jaringan komputer juga merupakan komponen yang sangat signifikan dalam proses menjamin kerahasiaan data. Hak akses data dapat diatur sesuai dengan kebutuhan dengan memanfaatkan jaringan komputer yang berada di bawah kendali administratif yang ketat. Hal ini memastikan bahwa hanya individu yang berwenang yang dapat mengakses data sensitif, sehingga melindungi kerahasiaan dan integritas informasi penting.

Hal ini mencakup pemasangan protokol keamanan siber yang ketat, seperti firewall, enkripsi data, pemantauan keamanan, dan sistem pemantauan, serta pemanfaatan data terenkripsi. Selain

itu, jaringan membuat mobilitas menjadi lebih mudah. Misalnya, karyawan yang memiliki akses jarak jauh ke pekerjaannya dapat meningkatkan fleksibilitas dan produktivitas karena memungkinkan bekerja dari lokasi mana pun. Keuntungan lainnya adalah dunia usaha kini mampu mengikuti tren bekerja jarak jauh yang semakin meningkat, hal ini dimungkinkan oleh hal ini.

14.4.7 Integrasi data

Data yang kini tersedia di suatu organisasi atau bisnis dapat dihubungkan dengan data yang sudah ada di database jenis lain, seperti data penjualan, data pembelian, data stok gudang, data keuangan, dan data dari database jenis lainnya. Contoh data semacam ini antara lain data penjualan, data pembelian, dan data stok gudang. Informasi semacam ini dapat berisi hal-hal seperti data penjualan, data pembelian, data stok gudang, dan data keuangan, sebagai beberapa contohnya. Ungkapan "penjualan" dan "pembelian" selain "stok gudang" adalah contoh dari jenis data ini. Ini adalah sesuatu yang dapat dicapai dengan menghubungkan data yang saat ini ada dalam suatu organisasi atau perusahaan dengan data yang sudah ada dalam database jenis lain. Menghubungkan data dalam suatu organisasi atau perusahaan merupakan salah satu metode untuk mencapai tujuan tersebut. Sekalipun datanya berasal dari sejumlah departemen yang berbeda, jaringan komputer akan digunakan untuk menghubungkan semua file menjadi satu sehingga semua file dapat diakses secara bersamaan. Hal ini akan membuat data dapat digunakan secara efektif. Ini akan memungkinkan file-file tersebut dihubungkan satu sama lain sehingga dapat diakses semuanya secara bersamaan.

14.4.9 *Customization*

Kekuatan untuk mengotomatiskan penyampaian informasi dan layanan untuk memenuhi kebutuhan spesifik setiap pelanggan merupakan komponen penting dari setiap strategi sukses dalam menjalankan bisnis online. Tergantung pada kebutuhan pengguna sistem, informasi dapat diperoleh dan ditransfer dari jaringan server baik dalam konteks lokal atau global. jaringan komputer berbasis web Misalnya, formulir pendaftaran yang hanya meminta pelanggan memberikan informasi dalam jumlah minimal agar memungkinkan pemilihan tingkat situs web secara cepat harus digunakan. Penggunaan internet dalam bisnis dapat membantu perusahaan memperoleh keunggulan kompetitif dalam beberapa cara penting. Cara-cara ini mencakup peningkatan produktivitas dan penurunan biaya overhead, serta kemampuan untuk menyediakan pemasaran yang disesuaikan dan interaktif kepada setiap pelanggan perusahaan. Penggunaan internet dalam lingkungan komersial dapat memberikan sejumlah manfaat bagi perusahaan, salah satu yang paling penting adalah pencapaian keunggulan kompetitif.

14.4.9 Manfaat Biaya dalam Jaringan Komputer

Salah satu keuntungan menggunakan jaringan komputer yang tepercaya adalah kemampuan untuk berbagi sumber daya di antara berbagai perangkat berbeda. Ketika komputer terhubung ke jaringan bersama, kebutuhan akan perangkat keras yang mahal akan berkurang. Ketika komputer yang digunakan oleh karyawan terhubung satu sama lain, dan tidak lagi memerlukan printer masing-masing atau ruang penyimpanan untuk cadangan masing. Karena karyawan akan dapat berbagi perangkat lunak pemindaian dokumen, jumlah peningkatan perangkat lunak yang perlu diinstal akan dikurangi, dan secara keseluruhan akan lebih sedikit. Potensi untuk memfasilitasi pembagian aset teknologi oleh anggota staf adalah salah satu keuntungan paling signifikan yang ditawarkan

oleh solusi jaringan ini, dan memberikan kontribusi signifikan terhadap potensi penghematan biaya dari solusi tersebut.

Manfaat yang diberikan oleh jaringan komputer tidak diragukan lagi menguntungkan. Meskipun memerlukan investasi awal yang signifikan, hal ini akan mengurangi biaya perawatan di masa depan. Selain itu, teknologi ini memiliki potensi untuk menggantikan peran seorang karyawan dalam tugas pengiriman dokumen atau data, yang di sekitarnya dapat mengurangi biaya operasional. Masalah biaya merupakan salah satu keunggulan jaringan komputer yang biasanya paling diperhatikan oleh pemilik bisnis.

14.4.10 Peningkatan Layanan Pelanggan

Ketika karyawan suatu perusahaan memiliki akses terhadap informasi tentang perusahaan tersebut, maka berada dalam posisi yang lebih baik untuk memberikan kualitas layanan yang lebih baik kepada pelanggan dan klien. Serta, mampu dengan cepat mengumpulkan semua informasi tentang pelanggan yang perlukan untuk memberikan tanggapan atas pertanyaan yang diajukan oleh pelanggan. Sehingga mempunyai kesempatan untuk mengirimkan informasi tentang pelanggan ke dalam sistem, yang memungkinkan karyawan lain tetap mendapatkan informasi terbaru secara real-time.

Tingkat kualitas layanan pelanggan yang diberikan oleh perusahaan Persepsi ini dapat dipengaruhi dalam beberapa cara berbeda. Ada kemungkinan bahwa keputusan masyarakat mengenai pembelian yang dilakukan juga akan terpengaruh oleh faktor ini.

Proses memberikan layanan pelanggan yang luar biasa dapat menghasilkan penjualan yang lebih tinggi berkat rekomendasi positif dari mulut ke mulut dan online yang dibuat oleh klien yang puas. jumlah rata-rata dolar yang lebih besar yang dibelanjakan oleh setiap pelanggan di setiap transaksi, serta

kunjungan kembali pelanggan dan peningkatan jumlah rekomendasi pelanggan ke perusahaan. Dengan secara hati-hati menetapkan, membangun, dan memelihara program layanan pelanggan, dapat menanamkan dalam perusahaan kita budaya yang mengutamakan pemberian dukungan unggul kepada klien. Tidak peduli bagaimana berinteraksi dengan konsumen, baik secara langsung, melalui telepon, atau melalui Internet; memberikan layanan pelanggan yang sangat baik sangat penting dalam semua pengaturan ini.

Sebagai ilustrasi, memberikan layanan pelanggan yang luar biasa dapat menghasilkan manfaat berikut: peningkatan jumlah pelanggan sebagai akibat langsung dari rujukan positif dari mulut ke mulut dan internet. jumlah rata-rata dolar yang lebih besar yang dibelanjakan oleh setiap pelanggan di setiap transaksi, serta kunjungan kembali pelanggan dan peningkatan jumlah rekomendasi pelanggan ke perusahaan.

Melalui desain yang cermat, pengembangan menyeluruh, dan pemeliharaan program layanan pelanggan yang konsisten, perusahaan dapat menumbuhkan budaya yang mengutamakan pemberian bantuan unggul kepada kliennya. Tidak peduli bagaimana berinteraksi dengan konsumen, baik secara langsung, melalui telepon, atau melalui Internet; memberikan layanan pelanggan yang sangat baik sangat penting dalam semua pengaturan ini.

14.4.11 Informasi Real Time

Perusahaan yang menggunakan jaringan komputer untuk mengumpulkan informasi ini seringkali dapat mengaksesnya dengan cepat dan akurat (*real time*) tanpa harus menunggu lama karena data telah didigitalkan dan tersedia untuk semua orang. Oleh karena itu, pekerja tidak perlu menunggu terlalu lama. Ketika karyawan menggunakan jaringan komputer untuk memperoleh data, data tersebut hampir selalu bersifat digital, dapat diakses oleh

semua orang, diperbarui secara real-time, dikirim secara instan, dan tidak mengalami latensi. Ketika karyawan menggunakan jaringan komputer untuk memperoleh data, data tersebut tidak rentan terhadap latensi.

14.4.12 Skalabilitas

Bisnis mendapatkan manfaat dari kemampuan beradaptasi jaringan komputer, yang memungkinkan dengan cepat menyesuaikan dan mengembangkan jaringan sebagai respons terhadap persyaratan yang diberlakukan oleh lingkungan bisnis. Hal ini memungkinkan bisnis untuk lebih memenuhi kebutuhan pelanggan dan tetap kompetitif. Misalnya, jika suatu perusahaan ingin menambah tenaga kerjanya, jaringan komputer perusahaan dapat dengan mudah dimodifikasi untuk memungkinkan penambahan lebih banyak pengguna. Pengguna baru ini kemudian akan dapat mengakses jaringan setelah jaringan tersebut diperbarui untuk mengakomodasi. Selain itu, jika suatu perusahaan memutuskan untuk memindahkan sebagian operasinya ke lokasi baru, jaringan komputer dapat diubah sehingga dapat menjalin hubungan dengan lokasi baru tersebut. Hal ini dapat dilakukan jika perusahaan mengambil keputusan tersebut. Korporasi berada dalam posisi di mana dapat mengambil tindakan ini sebagai sebuah pilihan. Sebagai akibat langsung dari hal ini, perusahaan kini memiliki kemampuan untuk menyesuaikan operasi dengan cepat sebagai respons terhadap perubahan kondisi dalam bisnis.

14.4.13 Akses Terpusat ke Informasi

Organisasi memiliki kemampuan untuk menyimpan dan mengelola data dan informasi secara terpusat melalui pemanfaatan jaringan komputer. Sistem ini memungkinkan karyawan untuk mengakses informasi yang dibutuhkan dengan mudah, sehingga menghilangkan kebutuhan untuk berpartisipasi dalam pencarian yang melelahkan di banyak sumber. Sebagai contoh, jika seorang

karyawan membutuhkan data penjualan terkini, mereka dapat dengan mudah mendapatkannya melalui jaringan komputer. Fenomena ini menghasilkan pengurangan waktu yang dibutuhkan untuk mengambil informasi penting dan peningkatan produktivitas secara keseluruhan.

DAFTAR PUSTAKA

Kuzmiakova, A. 2021. *Computer Networks and Communications*. Burlington, Canada: arclerpress.

R. Kelly Rainer Jr., Brad Prince, C.C. 2020. *Introduction to Information Systems Supporting and Transforming Business Fifth Canadian Edition*, *Wiley*.

S.Tanenbaum, A., Feamster, N. and Wetherall, D. 2020. *Computer Networks*. Sixth Edit. United States: Pearson Education Limited.

BIODATA PENULIS

Wahyuddin S., S.Kom., M.Kom
Dosen STMIK Amika Soppeng

Wahyuddin S. was born at Malaka-Bone-Sulawesi Selatan in 1992. In 2011 he attended Dipa Makassar University (UNDIPA) and was completed in 2015. He was completed after attending 7 semesters and active on an XPcom (Extreme Programmer Computer) campus organization. He was also active as a lecturer assistant for three semesters and taught several courses on programming. He continued his Master of Information systems at Indonesia Computer University (UNIKOM) Bandung in 2016 and was completed in April 2019. In 2023, he continues his doctoral studies in the computer science study program at Sepuluh Nopember Institute of Technology (ITS) Surabaya. He worked as a lecturer at a campus (STMIK Amika Soppeng) 2019 to present and also a Freelance Web Programmer. Has competence in the field of software engineer, application developer, multimedia, web developer, network security, and data analyst.

BIODATA PENULIS

Wirawan Istiono, S.Kom., M.Kom.
Dosen Informatika
Fakultas Teknik dan Informatika, Universitas Multimedia Nusantara

Penulis lahir di Jakarta tanggal 13 April 1983. Penulis adalah dosen pada Program Studi Informatika Fakultas Teknik dan Informatika, Universitas Multimedia Nusantara. Menyelesaikan pendidikan S1 pada Jurusan Teknik Informatika dan melanjutkan S2 pada bidang jurusan yang Teknik Informatika. Pada saat ini, penulis menekuni bidang Penelitian terkait komputer sains, sistem komputer dan teknologi informasi

BIODATA PENULIS

Arief Yanto Rukmana, S.T., M.M., C.Ed., CBPA®
Mahasiswa Doktoral Universitas Pendidikan Indonesia
Dosen Perguruan Tinggi Indonesia Mandiri Bandung
Dosen Universitas Nurtanio Bandung

Penulis sebelumnya telah memegang posisi penting di sejumlah bisnis yang beroperasi pada skala nasional dan dunia. penulis saat ini berprofesi sebagai praktisi bisnis (Pemilik Perusahaan di Bidang Fashion, Kuliner dan Bisnis Digital juga sebagai seorang akademisi. Penulis mengajar di Universitas Nurtanio Bandung, dan dosen tetap di perguruan tinggi indonesia mandiri (STMIK IM & STIE STAN IM). alumni dari Program Studi Informatika (S1) Sekolah Tinggi Manajemen Informatika dan Komputer Indonesia Mandiri (STMIK IM), Program Magister Manajemen (S2) di Pasca Sarjana Universitas Widyatama dan sedang melanjutkan studi Pendidikan (S3) Program Doktoral Pendidikan Teknologi dan Vokasional di Universitas Pendidikan Indonesia. Penulis aktif sebagai pembicara dan narasumber kewirausahaan digital juga berdedikasi sebagai praktisi bisnis / owner / pemilik beberapa perusahaan yang bergerak pada industri food, fashion and fun. serta aktif dalam organisasi nasional maupun internasional. Penulis juga seorang profesional dalam bidang public

speaking & sebagai asesor kompetensi digital dan instruktur berpengalaman untuk sertifikasi kompetensi SKKNI BNSP Digital Marketing, Social Media Marketing dan Metodologi Pelatihan Level III, Graphic Design serta Sertifikasi Kompetensi beberapa lainnya yang diselenggarakan dinas tenaga kerja kota bandung, PT Rice INTI dan Balai Besar Pengembangan Latihan Kerja (BBPLK) Bandung. Selain itu pula penulis produktif sebagai pendamping UMKM dan pengelola Inkubator Bisnis Perguruan Tinggi Indonesia Mandiri dengan membina dan melatih / coaching, mentoring serta melakukan pendampingan bisnis UMKM / Start UP untuk mahasiswa yang berminat menjadi seorang Entrepreneur / Technopreneurship tangguh yang mampu berdayasaing pada kancah internasional.

BIODATA PENULIS

James Philip
Peneliti Aktif di Insitut Teknologi Sepuluh Nopember (ITS)

Penulis lahir di Bandung tanggal 26 Maret 2003 . Saat ini penulis merupakan peneliti aktif di Institut Teknologi Sepuluh Nopember (ITS).

BIODATA PENULIS

Angga Aditya Permana
Dosen Program Studi Informatika
Fakultas Teknik dan Informatika
Universitas Multimedia Nusantara

Angga Aditya Permana (lahir pada Desember 1989 di Jakarta) seorang dosen full time di bidang Computer Science pada Universitas Multimedia Nusantara sejak tahun 2021, fokus penelitian pada kriptografi, steganografi serta keamanan computer, namun pada tahun 2021 sedang mendalami topik bioinformatika dan network science. Angga juga memiliki hobi yaitu touring dan juga bermain bulutangkis, saat ini sedang menjadi mahasiswa program doctoral pada IPB University. Memulai karir pertama kali sebagai Network Enginner tahun 2011 dan memulai profesinya sebagai dosen pada 2013 di kampus swasta yang ada di Jakarta, pernah juga mengajar di kampus negri yang berada di Jakarta dan Tangerang, juga pernah di undang menjadi dosen tamu untuk mengenalkan Bioinformatika di kampus negeri di Jakarta. Terimakasih..

BIODATA PENULIS

Suwito Pomalingo, S.Kom., M.Kom
Dosen Program Studi Informatika
Universitas Multimedia Nusantara

Penulis adalah dosen tetap pada Program Studi Informatika Fakultas Teknik dan Informatika Universitas Multimedia Nusantara. Menyelesaikan pendidikan S1 pada Jurusan Teknik Informatika dan melanjutkan S2 pada Program Magister Informatika Universitas Islam Indonesia.

Saat ini sementara menyelesaikan studi Doktoral dengan topik penelitian di bidang Security Science dengan pendekatan Deep Learning. Penulis menekuni bidang keilmuan meliputi Cyber Security, Malware Analytics, Data Science, Machine Learning, dan Deep Learning, selain itu, penulis juga memiliki beberapa serifikasi internasional di bidang Cyber Security, Digital Forensics, Data Science dan Machine Learning.

BIODATA PENULIS

Ir. Johni S. Pasaribu, MT.
Dosen Program Studi Sistem Informasi
Fakultas IT Politeknik Piksi Ganesha

Penulis lahir di Medan tanggal 1 Juni 1966 dari pasangan HA Pasaribu (alm) dan Taruli Tambunan (alm). Penulis adalah anak keempat dari enam bersaudara. Pendidikan yang ditempuh yaitu SD Methodist Medan lulus tahun 1979, SMPN 88 Jakarta lulus tahun 1982 dan SMAN 3 Jakarta lulus tahun 1985. Kemudian melanjutkan studi di ITB jurusan Teknik Fisika spesialisasi Instrumentasi dan Kontrol. Penulis melakukan penelitian untuk tugas akhir di PT IPTN dengan judul Perancangan Sistem Kendali Fly By Wire Gerak Longitudinal Pada Engineering Flight Simulator Pesawat N250-100 dan menyelesaikan gelar sarjana teknik Insinyur (Ir) tahun 1992.

Kemudian penulis bekerja di PT. IPTN (sekarang PT Dirgantara Indonesia) di Departemen Iron Bird kemudian berpindah di Departemen Engineering Flight Simulator (EFS). Penulis terlibat dalam Operation and Maintenance untuk EFS sehingga simulator N250-100 ini dapat digunakan saat dilakukan pengujian-pengujian pesawat melalui simulator sebelum pengujian langsung pesawat di udara. Tahun 1998 penulis melanjutkan studi

S2 di ITB pada jurusan Teknik Informatika untuk spesialisasi Software Engineering, dimana ilmu yang diperoleh dapat diaplikasikan dalam pekerjaan di lapangan. Tahun 2001 penulis menyelesaikan pendidikan S2 dengan gelar MT mengambil penelitian yang berjudul Pengembangan Perangkat Lunak Simulasi Sistem Perasa Kendali Elevator Pesawat N250-100 dimana penelitian ini juga dilakukan di Engineering Flight Simulator (EFS) N250-100. Tahun 2004 penulis mulai aktif mengajar di Perguruan Tinggi di Bandung diantaranya pernah mengajar di Unikom, ITHB, STT Telkom (kini TelU). Kini penulis penuh mengajar dan menjadi dosen tetap di Politeknik Piksi Ganesha. Bidang keahlian mengajar dan penelitian penulis adalah Artificial Intelligence (AI), Decision Support System (DSS), Software Engineering dan Software Testing. Penulis juga aktif melakukan bimbingan mahasiswa S1 dan publikasi di jurnal-jurnal nasional maupun internasional.

BIODATA PENULIS

Rudi Sutomo, S.Kom., M.Si., M.Kom.
Dosen Program Studi Sistem Informasi
Fakultas Teknik dan Informatika
Universitas Multimedia Nusantara

Rudi Sutomo memulai karirnya di bidang IT sebagai *IT Lecturer* di tahun 2002 dan mendalami perkembangan Software Engineering di Kampus dan IT Development di bidang Hospitality (Perhotelan), terlibat dalam beberapa Project Pembangunan Aplikasi untuk menunjang kemajuan dan kelancaran sistem IT di Hotel Novotel di Kota Palembang sebagai Asisten IT Manager. Aktif dan giat sebagai Web Developer yang berpengalaman di pembangunan di bidang Aplikasi Perkantoran dan bidang Pengembangan Website terutama Project Web Desain dan Website Development dengan terlibat dalam beberapa pembangunan project aplikasi seperti Aplikasi Visual Basic "*Work Order Multi User*" digunakan untuk seluruh Divisi dalam Hotel Novotel Palembang, Sistem Informasi Akademik (SIA) Kampus Tanri Abeng University dan Project berhubungan dengan PUSMENJAR (Pusat Asesmen dan Pembelajaran) Kemendikbud yaitu Project PUSPENDIK AKSI dan beberapa Project Minor lainnya.

Beliau juga aktif berpatisipasi dalam workshop mengenai Pembuatan website baik di sekolah maupun di masyarakat dan beberapa kali dipercaya sebagai Narasumber salah satunya di "Pelatihan Pengenalan dan Pembangunan Website" di Sekolah SMKN 43 Jakarta Tahun 2019. Pada Event Penghargaan Website Tingkat Nasional diberi kepercayaan sebagai Juri pada IWA (Indonesia Website Awards) Penilaian periode Tahun 2018 dan 2019.

BIODATA PENULIS

Danang Haryo Sulaksono S.ST. M.T.
Dosen Program Studi Teknik Informatika
Fakultas Teknik Elektro Dan Teknologi Informasi

Penulis lahir di Yogyakarta tanggal 29 Desember 1986. Penuli adalah dosen tetap pada Institut Teknologi Adhi Tama Surabaya (ITATS). Menyelesaikan pendidikan D4 Teknik Informatika di Politeknik Elektronika Negri Surabaya (PENS), Dan S2 Jaringan Cerdas Multimedia di Institut Teknologi SepuluhNopember (ITS).

BIODATA PENULIS

Iwan Adhicandra, S.T., M.Sc.
Dosen Program Studi Informatika
Universitas Bakrie

Penulis lahir di Jakarta tanggal 1 Desember 1974. Penulis adalah dosen tetap pada Program Studi Informatika, Universitas Bakrie. Menyelesaikan pendidikan S1 pada Jurusan Teknik Elektro bidang Teknik Telekomunikasi di Universitas Trisakti, dan melanjutkan S2 pada Jurusan Teknik Elektro bidang Komunikasi Data di University of Sheffield, Inggris. Penulis adalah Senior Member di Institute of Electrical and Electronic Engineers (SMIEEE).

BIODATA PENULIS

Yuniansyah
Dosen di Kota Lubuk Linggau, Batam, dan Duri.

Yuniansyah. Mengenal Ilmu Komputer Pada Tahun 1995 dimana penulis mendapatkan kesempatan melanjutkan pendidikan Strata satu di Universitas Bina Darma Palembang dan selesai pada tahun 1999. Pada saat kuliah juga selama 2 tahun (1997-1999) sempat menjadi Asisten Dosen di Laboratorium komputer Universitas Bina Darma untuk beberapa matakuliah pemrograman.

Pada awal tahun 2002 melanjutkan pendidikan di Program Studi Magister Ilmu Komputer Fakultas Ilmu Matematika dan Ilmu Pengetahuan Alam (F-MIPA) Universitas Gadjah Mada – Yogyakarta dan selesai pada akhir tahun 2013. Selama di Yogyakarta juga penulis berkesempatan menjadi Dosen di salah satu Perguruan Tinggi yang ada di Yogyakarta.

Selepas meraih gelar Magister Komputer penulis menjadi dosen di beberapa Perguruan Tinggi swasta dan Universitas Negeri di Kota Palembang. Penulis juga pernah menjadi Dosen di Kota Lubuk Linggau, Batam, dan Duri.

Saat ini penulis menjadi dosen praktisi di salah satu perguruan tinggi ternama di Kota Pelembang Penulis ini dapat

dihubungi melalui email: yuniansyah.mr@gmail.com atau yuniansyah@palcomtech.ac.id serta dapat juga melalui WA / Telegram : 0812 3516 8181

BIODATA PENULIS

Drs Amna, MIT
Dosen tamu prodi teknik informatika di STTP Payakumbuh

Memulai pendidikan dasar dan menengah di kota kelahirannya Takengon Aceh Tengah dan kemudian melanjutkan pendidikan tinggi di bidang matematika di USK Banda Aceh pada tahun 1988 dan memperoleh gelar sarjana pada 1992. Tahun 1993 melanjutkan program Pra S2 Matematika di ITB Bandung. Program S2 pula di tempuh pada Mathematics Department Fakulti Sains matematik dan komputer Universiti Kebangsaan Malaysia (UKM). Akhir tahun 1994 menukar jurusan ke Sains Komputer seiring dengan terbentuknya Fakulti Teknologi dan Sains Maklumat UKM. Selama melanjutkan studi S2 sangat aktif sebagai Tutor sambilan untuk mata kuliah matematik, statistik dan ilmu komputer, juga sebagai Asisten Research untuk bidang ilmu komputer dan rekayasa perangkat lunak. Setelah menamatkan S2 tahun 1997 dunia Dosenpun digeluti dengan memulai sebagai Dosen program degree sains sistem di kolej Politek MARA Bangi untuk franchise program UKM-KYPM. Kemudian sebagai dosen D3 sains komputer prancise dengan UiTM Shah Alam, UPM Serdang juga program degree software engineering dengan MMU Cyberjaya di KYPM Kuala Lumpur. Tahun 2001 kembali ke Kampus UKM

Bangi sebagai dosen sains sistem. Tahun 2003 bergabung dengan Kolej SAL Kuala Lumpur sebagai dosen program prancise degree in software engineering dan degree in networking dengan Edith Cowan University Western Australia. Tahun 2004 bergabung dengan Universiti Tenaga Nasional (UNITEN) sebagai asisten research bidang parallel processing dan dosen matematik di college Of engineering sambil melanjutkan studi S3. Tahun 2008 bergabung dengan College of IT UNITEN sebagai dosen system and network departement. Tahun 2010 hingga sekarang bergabung dengan Universitas Gajah Putih sebagai dosen teknik informatika. Banyak jurnal dan proseding baik internasional dan nasional yang telah di hasilkan dalam jangka waktu tersebut. Juga mengisi berbagai macam konferensi, simposium, dan webinar. Sejak 2017 hingga sekarang sebagai dosen tamu prodi teknik informatika di STTP Paya kumbuh. Empat belas book chapter yang telah di hasilkan: *The art of digital marketing* strategi pemasaran generasi milanial, *Fintech innovation essence, posisition & strategy*, Sistem operasi, Tahapan rekayasa perangkat lunak dll. Hal terbaru dari riset pada 27 Desember 2021 mendapat tempat harapan 1 lomba Innovasi LISIK 2021menerusi judul riset Kamus Bahasa Gayo Berbasis android.

Lahir dari ayah Abdurrahman AS dan ibu Fatimah dan menikah dengan Dr. Anna Permatasari Kamarudin, S.Tp, MBA sejak tahun 2000 dan dikaruniakan dengan 3 putri diberi nama Adiba Imani Salsabila, Najla Raihana Kamila dan Khayla Rahadatul Fakhira.

Email Penulis: amnaa98@hotmail.com

BIODATA PENULIS

Dr. Purnawarman Musa, S.Kom., M.T., M.I.Kom
Dosen Program Studi Teknik Elektro
Fakultas Teknologi Industri

Penulis lahir di Gorontalo pada tahun 1975 sebagi dosen tetap di Universitas Gunadarma, menyelesaikan pendidikan pada program studi *Electronic Image and Informatic* dengan gelar Doktor (Dr.) pada bidang Teknologi Infomasi dari Burgundy of University di kota Dijon, France pada tahun 2013. Penulis memperoleh gelar *Master of Engineering* (M.T.) tahun 2006 di Universitas Gunadarma Jakarta - Indonesia, gelar *Master of Communication* (M.I.Kom) tahun 2021 di Universitas Gunadarma, Jakarta - Indonesia dan tahun 1999 menyelesaikan pendidikan S1 jurusan *Computer Engineering* (S.Kom) di Universitas Gunadarma, Jakarta - Indonesia. Penulis menekuni bidang Robotika, IoT, Computer Vision, Kecerdasan Buatan, Remote Sensing dan Sistem Tertanam. Beberap keanggota penulis, diantarnya Ikatan Ahli Informatika Indonesia (IAII) dan Asosiasi Perguruan Tinggi Informatika dan Komputer (APTIKOM).

BIODATA PENULIS

Dr. Erick Fernando, S.Kom., M.S.I.
Dosen Program Studi Sistem Informasi
Fakultas Teknik dan Informatik
Universitas Multimedia Nusantara

Penulis saat ini merupakan dosen tetap pada Program Studi Sistem Informasi Fakultas Teknik dan Informatik, Universitas Multimedia Nusantara. Menyelesaikan pendidikan S1 pada Jurusan Teknik Informatika dan melanjutkan S2 pada Jurusan Magister Sistem Informasi. Serta Menyelesaikan S3 pada Doktor of Computer Science. Penulis menekuni bidang Basis data, Teknologi Blockchain, Adopsi Teknologi, Big Data, Sistem Informasi Geografis, *Emmbeded System* Dlll.