ISBN 978-634-255-149-3

CISCO ROUTING AND SWITCHING

PENULIS :

- Hermila A
- Deddy Rudhistiar
- Miftah Fadhli As'ad
- Ali Impron
- Lut Faizal
- Octsa Khairus Praharsyarendra

CISCO ROUTING AND SWITCHING

Hermila A
Deddy Rudhistiar
Miftah Fadhli As'ad
Ali Impron
Lut Faizal
Octsa Khairus Praharsyarendra

GET PRESS INDONESIA

CISCO ROUTING AND SWITCHING

Penulis :
Hermila A
Deddy Rudhistiar
Miftah Fadhli As'ad
Ali Impron
Lut Faizal
Octsa Khairus Praharsyarendra

ISBN : 978-634-255-149-3

Editor : Hendra Nusa Putra,S.Kom, M. Kom
Penyunting : Tri Puti 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, November 2025

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 Cisco Routing And Switching ini.

Buku Ini Membahas *Cisco System Overview*, Perangkat Jaringan Cisco, Pengantar IP Address IPv4, Konsep Dasar Jaringan (*Basic Network*), Konsep Teknologi Switch, Routing Statis (*Static Routing)*.

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, Oktober 2025

Penulis

DAFTAR ISI

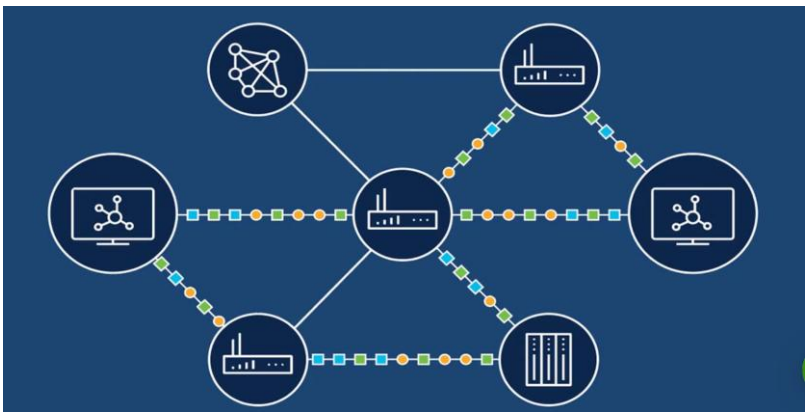
DAFTAR TABEL

DAFTAR GAMBAR

BAB 1
CISCO SYSTEM OVERVIEW

1.1 Pendahuluan

Di era digital, jaringan komputer bukan lagi sekadar "penghubung perangkat," melainkan tulang punggung seluruh proses bisnis, layanan publik, dan interaksi manusia–mesin. Dari layanan perbankan daring, komputasi awan, video konferensi, hingga *Internet of Things* (IoT) yang menggerakkan kota cerdas, semua bergantung pada jaringan yang andilnya simultan yakni andal, aman, elastis, dan dapat diamati (*observable*) (Gill *et al.*, 2024). Literatur jaringan klasik menegaskan bahwa jaringan modern harus dipahami dari dua kacamata sekaligus "*nuts-and-bolts*" (perangkat, taut fisik, protokol) dan "*services*" (layanan yang dihadirkan ke aplikasi). Keduanya tak terpisahkan dalam merancang dan mengoperasikan infrastruktur hari ini (Agus Wibowo, 2023; Baraka, 2023; Hafiz *et al.*, 2024).



Gambar 1.1. Cisco Routing
(Sumber :
https://www.cisco.com/site/us/en/learn/topics/networking/what-is-routing.html)

Secara teknis, inti dari routing dan switching memungkinkan paket data bergerak dengan efisien dari sumber ke tujuan. Sementara routing mengidentifikasi lintasan antardomain jaringan menggunakan protokol seperti OSPF (*Open Shortest Path First*) dan BGP (*Border Gateway Protocol*) yakni litasan antar domain interior dan eksterior, sementara switching berfungsi di lapisan data-link untuk membentuk domain broadcast yang efektif. Menurut Tanenbaum, routing/switching adalah "mekanisme inti" di lapisan jaringan yang berurusan dengan skala internet, pengendalian kemacetan, dan masalah kualitas layanan (TANENBAUM and WETHERALL, 2011). Sedangkan berdasarkan situs resmi Cisco, mendefinisikan routing sebagai proses pemilihan dan penetapan jalur untuk lalu lintas paket IP di dalam atau antara jaringan, serta proses pengelolaan lalu lintas jaringan secara keseluruhan. Pemahaman ini menjelaskan alasan pilihan desain pada tingkat perangkat. Jumlah konten memori yang dapat dialamatkan/TCAM pada switch dan pipeline forwarding pada router memengaruhi kinerja ujung-ke-ujung.

Melihat berdasarkan sudut pandang ekosistem, vendos perangkat lebih dari sekadar produsen hardware. Mereka memasok sistem operasi jaringan, rancangan arsitektur, perangkat manajemen dan pengawasan, set fitur (QoS, segmetasi, keamanan), *policy lifecycle* (dukungan suku cadang, pembaruan software), dan ekosistem pelatihan-sertifikasi, yang merupakan standar industri. Sejak lama, "interoperabilitas" telah ditetapkan sebagai kebutuhan utama menurut buku referensi (Tanenbaum and Wetherall, 2011; Kurose and Ross, 2013), dan vendor besar membantu dengan penerapan protokol terbuka yang konsisten lintas lini produk. Cisco Systems memiliki posisi khusus dalam konteks ini. Perusahaan ini, yang didirikan oleh Leonard Bosack dan Sandy Lerner di San Jose pada tahun 1984, tumbuh dari dasar universitas (Stanford) menjadi pemain global yang mempengaruhi cara internet dibangun, mulai dari awal internetworking, sistem operasi IOS, hingga praktik desain jaringan bisnis terbaik. Historiografi yang baik, baik dalam ensiklopedia maupun arsip newsroom, menceritakan sejarah awal Cisco: eksperimen internetworking kampus, perakitan router, dan

penggabungan kemampuan software-hardware yang akhirnya menjadi ciri khas perusahaan (cisco, 2025).

1.2 Sejarah dan Perkembangan Cisco System

Cisco didirikan pada Desember 1984 oleh Leonard Bosack dan Sandy Lerner, keduanya dari kalangan akademik di Stanford University. Mereka menghadapi tantangan praktis di Stanford. Jaringan komputer yang tersebar, sistem yang berbeda protokolnya, dan kesulitan dalam menghubungkan domain jaringan yang heterogen. Untuk itu, mereka mengembangkan konsep multiprotocol router sebuah perangkat yang mampu menjembatani jaringan dengan protokol berbeda agar bisa saling berkomunikasi. Cisco sendiri merupakan nama yang diambil dari kata "San Francisco" (EBSCO, 2023).

Cisco memulai pembangunan router pertamanya pada tahun 1986 dengan merekrut engineer pertama, Kirk Lougheed, yang sebelumnya bekerja di Stanford dan terlibat dalam pengembangan sistem. Dia bergabung dengan Cisco pada Juli 1986 dan bertanggung jawab untuk mengembangkan sistem operasi jaringan yang akhirnya menjadi IOS (*Internetworking Operating System*) Cisco. Pada awalnya, kantor Cisco di Atherton, California, memiliki ruang penyimpanan yang digunakan untuk pengembangan perangkat dan lab. Router pertama Cisco adalah seri AGS (*Advanced Gateway Server*), yang dirancang untuk menghubungkan jaringan lokal dengan jaringan yang lebih luas, mendukung multiprotocol forwarding (Leinwand and Pinsky, 1999; Carthern *et al.*, 2015; Carpenter and Lazonick, 2023). Berikut tabel ringkah sejarah perkembangan cisco berisi periode, peristiwa utama, dampak atau signifikansi teknologinya,

Tabel 1.1. Perkembangan Cisco

Periode / Tahun	Peristiwa Utama	Dampak / Signifikansi Teknologis
1984	Cisco Systems didirikan oleh *Leonard Bosack* dan *Sandy Lerner* di Stanford University. Nama "Cisco" diambil dari kata *San Francisco*.	Awal mula pengembangan *router multiprotocol* yang memungkinkan komunikasi lintas jaringan berbeda protokol.
1986–1989	Cisco merilis router komersial pertamanya: **Advanced Gateway Server (AGS)** dan memperkenalkan sistem operasi **Cisco IOS**.	IOS menjadi *de facto standard* dalam sistem operasi perangkat jaringan, mendukung berbagai protokol (IP, IPX, AppleTalk).
1990	Cisco melakukan **IPO** di NASDAQ (kode saham: CSCO).	Membuka akses modal besar, mempercepat ekspansi global, dan memperkuat posisi pasar enterprise networking.
1993–1996	Cisco mulai agresif melakukan akuisisi, termasuk **Crescendo Communications**, **Kalpana Inc.**, dan **Grand Junction Networks**.	Masuk ke segmen **LAN switching**, menjadikan Cisco penguasa pasar switching enterprise.
1997–2000	Era kepemimpinan **John Chambers** dimulai (CEO sejak 1995). Cisco memperkenalkan konsep **networking for the internet economy** dan menjadi perusahaan dengan valuasi tertinggi dunia (2000).	Cisco menjadi tulang punggung infrastruktur internet global dan simbol pertumbuhan ekonomi digital.

Periode / Tahun	Peristiwa Utama	Dampak / Signifikansi Teknologis
2001–2005	Setelah gelembung dot-com pecah, Cisco melakukan restrukturisasi dan efisiensi organisasi.	Fokus bergeser ke *services integration*, keamanan jaringan, dan kolaborasi (VoIP, WebEx).
2003–2010	Akuisisi besar seperti **Linksys (2003)**, **Scientific-Atlanta (2005)**, **WebEx (2007)**.	Cisco memperluas pasar ke jaringan rumah, video broadcasting, dan kolaborasi daring.
2011–2017	Fokus pada teknologi **Software Defined Networking (SDN)**, **Cloud**, dan **IoT**. Akuisisi seperti *Tail-f* (SDN), *AppDynamics* (analitik aplikasi), *Viptela* (SD-WAN).	Mengubah arah Cisco dari hardware-based menuju software-driven architecture.
2018–2021	Cisco memperkenalkan konsep **Intent-Based Networking** dan solusi keamanan terintegrasi **Zero Trust Security**.	Meningkatkan automasi jaringan, menggabungkan keamanan dan kebijakan jaringan dalam satu ekosistem.
2022–2024	Fokus strategi baru: **Networking + Security + Observability**, ditandai dengan akuisisi **Splunk (2023–2024)**.	Transformasi Cisco menjadi perusahaan data-driven network intelligence. Integrasi observabilitas dan keamanan berbasis AI.

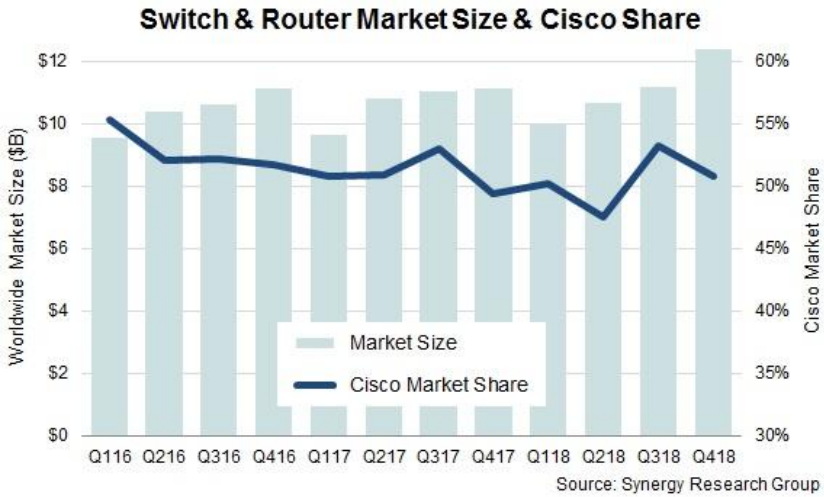
Sumber. Capenter 2023; Wikipedia; Cisco.com)

1.3 Posisi Cisco dalam Industri Jaringan

Cisco Systems telah lama menjadi pemimpin pasar dalam penyediaan perangkat jaringan, solusi bisnis, dan sistem infrastruktur digital dalam industri jaringan komputer global.

Sejak awal 1990-an, Cisco telah menciptakan standar industri, memperluas ekosistem pendidikan, dan beradaptasi dengan perubahan paradigma teknologi dari hardware-centric networking menuju software-defined dan cloud-based networking.

Secara konsisten, Cisco berada di posisi teratas dalam pasar router dan switch enterprise di seluruh dunia. Menurut laporan IDC dan Gartner selama dua puluh tahun terakhir, Cisco telah menempatkan dirinya sebagai pemimpin quadrant—atau pemimpin empat puluh-dalam segmen Enterprise Network Infrastructure. Pangsa pasarnya sering melampaui 40% di sektor switching enterprise dan 35% di sektor routing. Kualitas perangkat keras, sistem operasi jaringan yang stabil (IOS dan NX-OS), dan dukungan teknis yang luas di seluruh dunia memungkinkan dominasi ini (srgresearch, 2019). Penelitian Carpenter & Lazonick (2020), keberhasilan Cisco sebagai pemimpin pasar tidak hanya ditentukan oleh inovasi teknologinya, tetapi juga oleh model bisnis berbasis akuisisi strategis dan integrasi teknologi. Cisco mengakuisisi lebih dari 200 perusahaan sejak 1993, mulai dari perusahaan switching, keamanan, kolaborasi, hingga observability platform seperti Splunk pada 2024 menunjukkan kemampuan adaptasi jangka panjang terhadap perubahan pasar (Carpenter and Lazonick, 2023). Gambaran lengkap pasar router cisco dapat dilihat pada gambar 1.2 berikut.



Gambar 1.2. Switch & Router Market Size & Cisco Share (Sumber : Synergy Research Group, 2029)

Sistem operasi jaringan seperti Cisco IOS, IOS XE, dan NX-OS dirancang dengan filosofi modular, yang memungkinkan kompatibilitas lintas perangkat dan pembaruan berkelanjutan. Keunggulan utama Cisco terletak pada konsistensi arsitektur dan interoperabilitas lintas platform. Ini meningkatkan stabilitas dan kemudahan integrasi infrastruktur Cisco ke berbagai lingkungan jaringan, termasuk kampus, perusahaan besar, perusahaan kecil, dan pusat data. Beberapa riset menunjukkan bahwa penggunaan Cisco IOS secara luas dalam pelatihan dan implementasi jaringan meningkatkan reliabilitas dan keamanan sistem dibandingkan solusi dari vendor lain, terutama dalam konteks enterprise yang kompleks. Cisco juga mengembangkan intent-based networking (IBN), yaitu pendekatan otomatisasi jaringan yang memungkinkan sistem memahami kebijakan organisasi dan menerjemahkannya ke dalam konfigurasi otomatis (Feitosa *et al.*, 2021; Kabir *et al.*, 2021; Mwewa and Lubobya, 2022).

Cisco juga memberikan berkontribusi besar dalam pengembangan dan standarisasi protokol jaringan global. Melalui keterlibatan aktif di organisasi seperti IETF (*Internet Engineering Task Force*), IEEE, dan ITU-T, Cisco ikut merumuskan protokol utama seperti EIGRP (*Enhanced Interior Gateway Routing*

Protocol) yang dikembangkan oleh Cisco, kemudian dibuka sebagian spesifikasinya agar kompatibel dengan vendor lain. Ada juga NetFlow dan sFlow merupakan teknologi analitik lalu lintas jaringan yang kini menjadi dasar sistem pemantauan modern. SPAN / RSPAN / ERSPAN – mekanisme packet mirroring yang menjadi standar operasional di data center.

1.4 Peran Cisco dalam Pendidikan dan Sertifikasi

Sejak akhir dekade 1990-an, Cisco Systems telah memainkan peran strategis dalam dunia pendidikan melalui pendirian Cisco Networking Academy sebuah inisiatif global yang dirancang untuk membekali pelajar, mahasiswa, dan profesional dengan keterampilan jaringan, keamanan siber, dan teknologi informasi terkini. Melalui program ini, Cisco tidak hanya menyiapkan tenaga kerja siap industri, tetapi juga menumbuhkan ekosistem pembelajaran berbasis teknologi yang berkontribusi langsung terhadap pertumbuhan ekonomi digital.

Setelah diluncurkan secara resmi pada tahun 1997 sebagai kolaborasi dengan perguruan tinggi dan sekolah menengah di Amerika Serikat, *Cisco Networking Academy* berkembang menjadi program global yang beroperasi di lebih dari 190 negara. Tujuan awal adalah menyediakan kurikulum yang sesuai dengan standar industri jaringan komputer dan membantu lembaga pendidikan memberi siswa keterampilan kerja praktis. Laporan resmi Cisco Networking Academy Impact Report (2023) menyatakan bahwa, sejak didirikan, program ini telah menerima lebih dari 20 juta siswa, dan 4,7 juta siswa aktif setiap tahun. Lebih dari 250 lembaga pendidikan di Indonesia telah bekerja sama dengan program ini. Ini termasuk universitas negeri dan politeknik.

Peran *Cisco Networking Academy* telah menjadi model kolaborasi sukses antara industri dan akademia. López, Sánchez, dan Martín (2020) dalam penelitian mereka menjelaskan bahwa NetAcad menciptakan triple helix synergy — sinergi antara sektor industri, institusi pendidikan, dan pemerintah dalam mempersiapkan tenaga kerja digital masa depan. Model ini meningkatkan relevansi kurikulum pendidikan teknologi informasi terhadap kebutuhan lapangan kerja nyata (Kang and Lee, 2020). Selain berperan banyak

dalam akdemik. Cisco juga membantu menyediakan sarana untuk para profesional jaringan mendapatkan pengkuan keilmuan yang sering dikenal dengan sebutan sertifikasi. Program sertifikasi yang ditawarkanpun beragam sesuai levelnya. Berikut level sertifikasi pada cisco.

Tabel 1.2. Program sertifikasi cisco

Tingkat Sertifikasi	**Nama Sertifikasi**	**Fokus Kompetensi**
Entry Level	*Cisco Certified Technician (CCT)*	Dasar-dasar troubleshooting perangkat Cisco.
Associate Level	*Cisco Certified Network Associate (CCNA)*	Konsep dasar jaringan, IP addressing, routing & switching, dan keamanan dasar.
Professional Level	*Cisco Certified Network Professional (CCNP)*	Implementasi dan optimasi jaringan enterprise berskala besar, OSPF, BGP, VLAN, QoS, dan automasi.
Expert Level	*Cisco Certified Internetwork Expert (CCIE)*	Desain dan *troubleshooting* kompleks pada jaringan global.
Architect Level	*Cisco Certified Architect (CCAr)*	Perancangan arsitektur jaringan dan strategi transformasi digital tingkat perusahaan.

(sumber. Cisco.com)

Sertifikasi-sertifikasi ini bersifat vendor-based standard, yang artinya keterampilan teknis peserta diukur langsung berdasarkan kemampuan mengoperasikan dan mengonfigurasi perangkat Cisco. Namun demikian, karena perangkat Cisco digunakan luas di industri, kompetensi yang diperoleh bersifat transferrable dan relevan lintas vendor jaringan lain

1.5 Relevansi Cisco di Era Modern

Lanskap teknologi jaringan telah berubah secara signifikan dalam dua puluh tahun terakhir. Era jaringan cerdas, otomatis, dan berbasis data memasuki dunia digital yang sebelumnya bergantung pada infrastruktur fisik. *Cisco Systems* tetap relevan dan bahkan menjadi bagian penting dari evolusi jaringan modern ke arah yang lebih aman, adaptif, dan terotomasi, meskipun transformasi ini menuntut integrasi yang lebih dalam antara networking, keamanan, *cloud computing*, dan *artificial intelligence* (AI).

Cisco telah berevolusi dari perusahaan penyedia perangkat keras jaringan menjadi penyedia solusi digital terpadu yang mencakup perangkat keras, perangkat lunak, keamanan, dan layanan berbasis cloud. Pendekatan ini dikenal sebagai *Digital Network Architecture* (DNA), di mana jaringan tidak lagi dikelola secara manual tetapi dikontrol melalui *software-defined networking* (SDN) dan *intent-based networking* (IBN). Menurut Cisco Global Networking Trends Report (2024), lebih dari 70% perusahaan global kini menggunakan solusi berbasis SDN dan IBN untuk mengelola infrastruktur TI mereka, dan Cisco menjadi vendor utama dalam implementasi arsitektur tersebut. Laporan tersebut juga mencatat bahwa Cisco berfokus pada "secure, AI-driven, and cloud-managed networking" sebagai strategi utama menghadapi era digital (cisco, 2024).

Selain itu, dalam konteks global, keamanan menjadi dimensi penting dari relevansi Cisco. Dengan meningkatnya ancaman dunia maya, Cisco berinvestasi besar dalam *Zero Trust Security Framework* dan *Secure Access Service Edge* (SASE). Strategi ini memadukan keamanan berbasis cloud, identitas pengguna, dan kebijakan akses jaringan untuk membangun lapisan perlindungan adaptif. (Yamin and Katt, 2022) menegaskan bahwa solusi keamanan Cisco — seperti Cisco SecureX dan Cisco Umbrella — terbukti memperkuat postur keamanan perusahaan dalam menghadapi ancaman phishing, ransomware, dan DDoS. Cisco memosisikan keamanan bukan lagi sebagai fitur tambahan, tetapi sebagai fondasi utama arsitektur jaringan modern.

Terbaru cisco juga semakin eksis mengikuti perkembangan jaman dan kebutuhan teknologi di era sekarang yaitu kontribusi

dalam bidang Cloud dan *Internet of Things* (IoT). Relevansi Cisco juga diperkuat oleh posisinya dalam ekosistem Cloud Computing dan *Internet of Things* (IoT). Dengan semakin banyaknya perangkat dan sensor terhubung ke jaringan, Cisco mengembangkan solusi IoT Edge dan Fog Computing, yang memungkinkan pemrosesan data dilakukan di dekat sumbernya untuk mengurangi latensi dan beban jaringan pusat. Beberapa riset menyoroti bahwa arsitektur Cisco Fog Computing menjadi model utama dalam desain jaringan IoT industri (IIoT) karena kemampuannya menjaga keandalan, efisiensi bandwidth, dan keamanan di level edge (Sabireen and Neelanarayanan, 2021; Yacelga, Arevalo and Zambrano, 2023). Cisco juga memperluas solusi Meraki Cloud Platform, yang memudahkan organisasi dalam mengelola jaringan cabang, Wi-Fi, dan keamanan berbasis cloud melalui antarmuka web yang sederhana. Model ini menjadikan Cisco relevan bagi organisasi berskala kecil hingga multinasional yang memerlukan kontrol jaringan jarak jauh tanpa kompleksitas teknis tinggi.

Hal yang menarik, relevansi Cisco di era modern tidak hanya dari aspek teknologi, tetapi juga kontribusinya terhadap Tujuan Pembangunan Berkelanjutan (SDGs). Cisco mengimplementasikan inisiatif "*Cisco Purpose*", yaitu strategi global untuk mendorong pendidikan digital, inklusi sosial, dan energi berkelanjutan. Cisco berkomitmen mencapai net-zero emission pada tahun 2040, melalui pengembangan perangkat hemat energi dan sistem operasi yang efisien daya (cisco, 2024).

1.6 Aplikasi Cisco Secara Umum

Sebagai perusahaan global dalam bidang jaringan komputer, Cisco tidak hanya berfokus pada pengembangan perangkat keras seperti router dan switch, tetapi juga menyediakan berbagai aplikasi dan layanan digital yang mendukung kebutuhan pendidikan, bisnis, dan pemerintahan. Produk-produk Cisco mencakup beragam kategori: mulai dari infrastruktur jaringan dasar, layanan cloud, keamanan siber, hingga alat simulasi dan pendidikan seperti Cisco Packet Tracer. Tabel 1.3 berikut menampilkan ringkasan jenis-jenis produk dan aplikasi Cisco beserta fungsi, lingkup penggunaan, dan contoh penerapannya di dunia nyata.

Tabel 1.3. Jenis dan aplikasi cisco

No.	Jenis / Produk Cisco	Fungsi Utama	Lingkup Penggunaan
1	Cisco Router	Mengarahkan lalu lintas data antarjaringan (routing), menghubungkan LAN ke WAN, serta mendukung protokol seperti OSPF, EIGRP, dan BGP.	Perusahaan, lembaga pemerintahan, ISP, dan pendidikan.
2	Cisco Switch	Menghubungkan perangkat dalam satu jaringan lokal (LAN) dan mengatur pembagian bandwidth serta VLAN.	Sekolah, kampus, perusahaan, dan pusat data.
3	Cisco Firewall (ASA / Firepower)	Melindungi jaringan dari ancaman eksternal dengan menerapkan kebijakan keamanan dan inspeksi paket.	Instansi pemerintahan, perbankan, industri, dan perusahaan besar.
4	Cisco Meraki Cloud Platform	Manajemen jaringan berbasis cloud untuk Wi-Fi, kamera, dan perangkat IoT melalui dashboard web.	Sekolah, bisnis ritel, dan lembaga pemerintahan.
5	Cisco Webex	Platform komunikasi dan kolaborasi daring (video meeting, chat, dan berbagi dokumen).	Dunia pendidikan, bisnis, dan lembaga internasional.

No.	Jenis / Produk Cisco	Fungsi Utama	Lingkup Penggunaan
6	Cisco SD-WAN	Menghubungkan cabang perusahaan melalui jaringan WAN yang terpusat, efisien, dan aman.	Perusahaan multinasional dan penyedia layanan jaringan.
7	Cisco SecureX / Umbrella	Solusi keamanan siber berbasis cloud untuk mendeteksi dan mencegah ancaman digital.	Korporasi, lembaga keuangan, dan pemerintahan.
8	Cisco Networking Academy (NetAcad)	Program pendidikan global yang menyediakan pelatihan jaringan dan sertifikasi profesional (CCNA, CCNP).	Sekolah, universitas, politeknik, dan pelatihan profesional.
9	Cisco Packet Tracer	Aplikasi simulasi jaringan yang memungkinkan pengguna mendesain, mengonfigurasi, dan menguji jaringan virtual.	Pendidikan, pelatihan, dan penelitian.
10	Cisco DNA Center	Platform otomasi dan analisis jaringan berbasis *intent-based networking (IBN)* untuk mengontrol kebijakan jaringan secara cerdas.	Perusahaan besar dan penyedia layanan jaringan.

DAFTAR PUSTAKA

Agus Wibowo (2023) *TEORI & PRAKTIK JARINGAN KOMPUTER*. Edited by J.T. Santoso. Semarang: Yayasan Prima Agus Teknik Bekerjasama dengan Universitas STEKOM.

Baraka (2023) *Menggali Lebih Dalam: Pengenalan Konsep Dasar Jaringan Komputer - Biro Perencanaan Sumber Daya Manusia dan Karir*. Available at: https://baraka.uma.ac.id/jaringan-komputer-adalah-struktur-interkoneksi/ (Accessed: October 4, 2025).

Carpenter, M. and Lazonick, W. (2023) "The Pursuit of Shareholder Value: Cisco's Transformation from Innovation to Financialization." Available at: https://papers.ssrn.com/abstract=4470282 (Accessed: October 7, 2025).

Carthern, C. *et al.* (2015) *Cisco Networks - Engineers' Handbook of Routing, Switching, and Security with IOS, NX-OS, and ASA*. Apress.

cisco (2024) "Global Networking Trends Report 2024," *https://www.cisco.com/c/dam/global/en_uk/solutions/enterprise-networks/2024-global-networking-trends.pdf*.

cisco (2025) *What Is Routing? - Cisco*. Available at: https://www.cisco.com/site/us/en/learn/topics/networking/what-is-routing.html (Accessed: October 4, 2025).

EBSCO (2023) *Cisco Systems Goes Public*. Available at: https://www.ebsco.com/research-starters/business-and-management/cisco-systems-goes-public (Accessed: October 4, 2025).

Feitosa, L. *et al.* (2021) "Performance Evaluation of Message Routing Strategies in the Internet of Robotic Things Using the D/M/c/K/FCFS Queuing Network," *Electronics 2021, Vol. 10, Page 2626*, 10(21), p. 2626. Available at: https://doi.org/10.3390/ELECTRONICS10212626.

Gill, S.S. *et al.* (2024) "Modern computing: Vision and challenges," *Telematics and Informatics Reports*, 13, p. 100116. Available at: https://doi.org/10.1016/J.TELER.2024.100116.

Hafiz, S. *et al.* (2024) "Pengantar Jaringan Komputer," *Penerbit Mifandi Mandiri Digital*, 1(01). Available at: https://jurnal.mifandimandiri.com/index.php/penerbitmmd/article/view/42 (Accessed: October 4, 2025).

Kabir, M.H. *et al.* (2021) "Performance Analysis of Mesh Based Enterprise Network Using RIP, EIGRP and OSPF Routing Protocols," *Engineering Proceedings 2021, Vol. 10, Page 47*, 10(1), p. 47. Available at: https://doi.org/10.3390/ECSA-8-11285.

Kang, Y. and Lee, K. (2020) "Designing technology entrepreneurship education using computational thinking," *Education and Information Technologies*, 25(6), pp. 5357–5377. Available at: https://doi.org/10.1007/S10639-020-10231-2/METRICS.

Kurose, J.F.. and Ross, K.W.. (2013) *Computer networking : a top-down approach*. Pearson. Available at: https://books.google.com/books/about/Computer_Networking.html?hl=id&id=gbAhngEACAAJ (Accessed: October 4, 2025).

Leinwand, A. and Pinsky, B. (1999) *Cisco Router Configuration (2nd Edition)*. 2nd ed. Cisco Press.

Mwewa, W. and Lubobya, S.C. (2022) "Performance Evaluation of Routing Protocols in Enterprise Networks," *American Journal of Computing and Engineering*, 5(1), pp. 24–35. Available at: https://doi.org/10.47672/AJCE.953.

Sabireen, H. and Neelanarayanan, V. (2021) "A Review on Fog Computing: Architecture, Fog with IoT, Algorithms and Research Challenges," *ICT Express*, 7(2), pp. 162–176. Available at: https://doi.org/10.1016/J.ICTE.2021.05.004.

srgresearch (2019) *Switch & Router Revenues Set a New Record; Cisco Market Share Still Over 50%*. Available at: https://www.srgresearch.com/articles/switch-router-revenues-set-new-record-cisco-market-share-still-over-50 (Accessed: October 7, 2025).

TANENBAUM, A.S. and WETHERALL, D.J. (2011) *COMPUTER NETWORKS*. 5th ed. Boston: Pearson Education, Inc.

Yacelga, A.L., Arevalo, N.B. and Zambrano, L.A. (2023) "Fog Computing in the Industrial Internet of Things: Challenges, Trends, and Strategies," *Fusion: Practice and Applications*, 13(2),

pp. 91–105. Available at: https://doi.org/10.54216/FPA.130208.
Yamin, M.M. and Katt, B. (2022) “Modeling and executing cyber security exercise scenarios in cyber ranges,” *Computers & Security*, 116, p. 102635. Available at: https://doi.org/10.1016/J.COSE.2022.102635.

BAB 2
PERANGKAT JARINGAN CISCO

2.1 Pendahuluan

Perangkat jaringan adalah tulang punggung infrastruktur komunikasi modern, memungkinkan data mengalir dengan cepat, efisien, dan aman di berbagai jenis jaringan, mulai dari lokal hingga global. Keberadaan perangkat ini sangat penting dalam mendukung operasional organisasi, baik untuk skala kecil seperti usaha mikro hingga skala besar seperti perusahaan multinasional dan penyedia layanan internet. Dalam ekosistem digital yang semakin kompleks, perangkat jaringan tidak hanya bertugas mentransfer data tetapi juga mengelola lalu lintas dengan cara yang cerdas, memastikan konektivitas yang konsisten, serta menjaga keamanan informasi dari berbagai ancaman siber yang terus berkembang. Kebutuhan akan perangkat jaringan menjadi semakin krusial seiring dengan meningkatnya ketergantungan pada teknologi digital dalam kehidupan sehari-hari. Misalnya, meningkatnya penggunaan aplikasi berbasis cloud, layanan video on demand, IoT (*Internet of Things*), serta transformasi bisnis ke model digital-first telah menghasilkan lonjakan eksponensial dalam lalu lintas data.

Di sisi lain, ancaman siber seperti serangan ransomware, malware, dan serangan *Distributed Denial of Service* (DDoS) semakin canggih dan meluas, menuntut perangkat jaringan untuk tidak hanya cepat dan andal tetapi juga dilengkapi dengan sistem keamanan yang kuat. Selain itu, keberagaman kebutuhan jaringan juga menjadi tantangan tersendiri. Organisasi menghadapi masalah skalabilitas saat harus mengintegrasikan perangkat jaringan baru ke infrastruktur yang sudah ada, sekaligus mempertahankan performa dan stabilitas jaringan. Di era transformasi digital ini, di mana teknologi seperti big data, *artificial intelligence* (AI), dan machine learning digunakan untuk analitik dan pengambilan keputusan, jaringan harus mampu mendukung aplikasi yang memerlukan latensi rendah dan bandwidth tinggi. Hal ini menuntut perangkat

jaringan untuk memiliki kemampuan yang lebih canggih, termasuk mendukung arsitektur jaringan modern seperti SDN (*Software-Defined Networking)* dan virtualisasi.

Cisco Systems, yang berdiri pada tahun 1984, memulai perjalanannya dengan menghadirkan solusi revolusioner berupa router multiprotokol pertama yang memungkinkan integrasi berbagai jenis jaringan. Sejak itu, Cisco berkembang menjadi pemimpin pasar perangkat jaringan dengan portofolio produk yang mencakup router, switch, firewall, access point, dan solusi jaringan berbasis perangkat lunak seperti SD-WAN dan DNA Center. Fokus Cisco tidak hanya pada inovasi teknologi, tetapi juga pada pengembangan ekosistem yang mendukung seperti pelatihan, sertifikasi, dan komunitas pengguna global. Di Indonesia, Cisco mulai hadir secara aktif sejak awal 2000-an, seiring dengan berkembangnya kebutuhan jaringan di sektor bisnis, pendidikan, dan pemerintahan. Kehadiran Cisco Indonesia membantu mendorong transformasi digital dengan menyediakan perangkat berkualitas tinggi dan mendukung implementasi teknologi di berbagai skala. Cisco menjadi mitra strategis bagi banyak institusi besar di Indonesia, termasuk bank, penyedia layanan telekomunikasi, universitas, dan perusahaan teknologi.

Sebagai pemimpin industri, Cisco tidak hanya menyediakan perangkat keras seperti router, switch, dan firewall, tetapi juga solusi yang terintegrasi dengan teknologi terkini seperti *Software-Defined Networking* (SDN), keamanan berbasis AI, dan arsitektur hybrid cloud. Reputasinya diperkuat oleh ekosistem dukungan yang luas, termasuk pelatihan dan sertifikasi seperti CCNA dan CCNP, yang membuat tenaga kerja TI di seluruh dunia mampu menggunakan teknologi Cisco dengan optimal. Salah satu tonggak penting Cisco di Indonesia adalah peluncuran program-program pelatihan seperti Cisco Networking Academy, yang telah melatih ribuan profesional IT di seluruh negeri. Program ini membantu meningkatkan keterampilan tenaga kerja lokal di bidang jaringan, memperkuat posisi Indonesia dalam menghadapi persaingan global di era digital. Selain itu, Cisco juga telah memainkan peran penting dalam memperluas infrastruktur internet di Indonesia, mendukung inisiatif

pemerintah untuk mempercepat adopsi teknologi di daerah terpencil.

2.2 Kategori dan Fungsi Perangkat Jaringan Cisco

Cisco menawarkan berbagai jenis perangkat jaringan yang dirancang untuk memenuhi kebutuhan beragam organisasi, mulai dari usaha kecil hingga perusahaan multinasional. Salah satu perangkat utama yang ditawarkan adalah router, sebuah perangkat esensial dalam arsitektur jaringan yang berfungsi untuk mengarahkan lalu lintas data antar jaringan dengan cara yang efisien dan aman. Router bertanggung jawab untuk memastikan data yang dikirimkan melalui jaringan sampai ke tujuan yang benar, baik di dalam jaringan internal maupun antar jaringan eksternal. Fungsinya tidak hanya sebatas menghubungkan jaringan lokal (LAN) dengan jaringan luas (WAN), tetapi juga mendukung berbagai teknologi jaringan modern seperti virtualisasi, enkripsi data, dan integrasi layanan berbasis cloud.

2.2.1 Router Cisco

Router Cisco digunakan untuk mengarahkan lalu lintas data antar jaringan. Seri populer seperti ISR (Integrated Services Routers) menawarkan fitur untuk jaringan enterprise, sedangkan ASR (Aggregation Services Routers) dirancang untuk data center dengan kebutuhan kapasitas tinggi.

Gambar 2.1. Router Cisco
(Sumber : https://www.cisco.com/c/en/us/support/routers/small-business-rv-series-routers/series.html)

2.2.2 Switch Cisco

Switch berfungsi untuk mengelola lalu lintas data dalam jaringan lokal (LAN). Cisco menyediakan Layer 2 Switch untuk switching sederhana dan Layer 3 Switch yang mendukung routing.

Seri populer termasuk Catalyst untuk jaringan enterprise dan Nexus untuk data center.

Gambar 2.2. Switch Cisco
(Sumber :
https://www.cisco.com/c/it_it/support/switches/catalyst-2960-xr-series-switches/series.html)

2.2.3 Firewall Cisco

Firewall seperti Cisco ASA dan Cisco Firepower memastikan keamanan jaringan dengan mencegah akses yang tidak sah. Firewall ini juga mendukung fitur seperti Intrusion Prevention System (IPS) dan analitik ancaman canggih.

Gambar 2.3. Firewall Cisco
(Sumber :
https://www.cisco.com/c/en_uk/products/security/firewalls/index-1b.html)

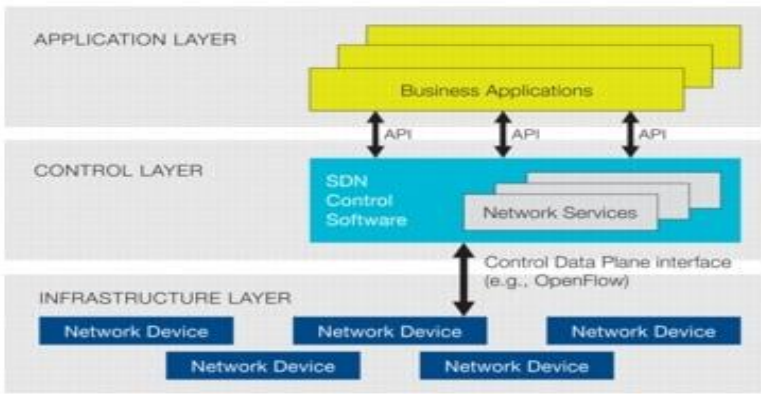
2.2.4 *Wireless Access Point* dan *Controller*

Access Point Cisco (seri Aironet dan Catalyst) memungkinkan koneksi nirkabel yang cepat dan aman. Pengelolaan terpusat dilakukan melalui Cisco Wireless Controller, yang mendukung fitur seperti seamless roaming dan manajemen frekuensi.

Gambar 2.4. Wireless Acces Point
(Sumber :
https://www.cisco.com/c/en/us/products/wireless/access-point-controller-selector.html)

2.2.5 *Software-Defined Networking* (SDN)

Produk seperti Cisco DNA Center memungkinkan manajemen jaringan berbasis perangkat lunak, mempermudah pengelolaan dan pengawasan jaringan secara efisien. Berikut Arsitektur Layer pada *Software-Defined Networking* yang dimana aplication layer saling berhubungan dengan control layer dan kedua hal tersebut digunakan untuk mengelola Infrastucture Layer yang didalamnya terdapat *Network Device*. Pada *Application layer* terdapat *Bussine Aplication* dan pada Control Layer terdapat *Network Service* untuk menjembatasi antara Aplication Layer terhadap *Network Device*.



Gambar 2.5. Arsitektur Layer SDN
(Sumber :
https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Data_Center/VMDC/SDN/SDN.html)

2.3 Spesifikasi dan Teknologi pada Perangkat Cisco

Perangkat jaringan Cisco dikenal dengan kualitas dan kinerjanya yang unggul, ditunjang oleh spesifikasi perangkat keras canggih, dukungan terhadap protokol jaringan standar, serta fitur tambahan yang dirancang untuk mendukung kebutuhan jaringan modern. Berikut adalah penjelasan rinci mengenai komponen utama yang menjadikan perangkat Cisco andal dan efisien dalam memenuhi kebutuhan organisasi.

2.3.1 Komponen Perangkat Keras

1. **Prosesor**

   Prosesor yang digunakan dalam perangkat Cisco dirancang khusus untuk menangani beban kerja jaringan yang intensif. Prosesor ini mampu mengelola lalu lintas data berkecepatan tinggi dengan latensi rendah, mendukung kebutuhan jaringan seperti routing, switching, dan keamanan secara real-time. Dalam perangkat kelas enterprise dan data center, Cisco menggunakan prosesor multi-core yang memungkinkan paralelisme tinggi, sehingga mampu menangani berbagai tugas secara bersamaan tanpa mengurangi performa.

2. **Memori**

   Perangkat Cisco dilengkapi dengan memori yang dapat diupgrade, termasuk memori utama (RAM) dan penyimpanan internal (*flash storage*). RAM digunakan untuk menyimpan tabel routing, informasi VLAN, dan konfigurasi sementara, yang esensial untuk menjaga performa jaringan dalam kondisi optimal. Sementara itu, flash storage digunakan untuk menyimpan sistem operasi Cisco IOS (*Internetwork Operating System*), konfigurasi startup, serta file lainnya. Dengan memori yang dapat diupgrade, perangkat dapat diadaptasi untuk memenuhi kebutuhan jaringan yang terus berkembang.

3. **Interface Port**

   Perangkat Cisco menyediakan berbagai jenis port untuk mendukung konektivitas jaringan yang fleksibel. Port Ethernet tersedia dalam berbagai kecepatan (1 Gbps, 10 Gbps, hingga 100 Gbps), sementara port SFP (*Small Form-Factor Pluggable*)

memungkinkan koneksi fiber optic yang ideal untuk jaringan jarak jauh. Selain itu, perangkat seperti switch Cisco juga mendukung *Power over Ethernet* (PoE), yang memungkinkan port Ethernet mengalirkan daya listrik untuk perangkat seperti access point, kamera CCTV, dan IP phone tanpa memerlukan kabel daya tambahan.

2.3.2 Dukungan Protokol Standar

1. **IPv4 dan IPv6**

   Perangkat Cisco mendukung dual stack untuk IPv4 dan IPv6, memungkinkan jaringan untuk beroperasi dengan kedua protokol secara bersamaan. Dukungan ini sangat penting dalam transisi dari IPv4 ke IPv6, yang menjadi standar baru di era modern karena kapasitas alamat IP-nya yang jauh lebih besar. Dengan dual stack, perangkat Cisco memastikan kompatibilitas dan interoperabilitas dalam jaringan global.

2. **MPLS (*Multiprotocol Label Switching*)**

   Cisco mendukung protokol MPLS, yang dirancang untuk meningkatkan efisiensi routing di jaringan WAN. Teknologi ini memungkinkan pengiriman data melalui jalur optimal berdasarkan label yang ditentukan, bukan berdasarkan alamat IP. MPLS sangat efektif untuk jaringan besar yang memerlukan kecepatan tinggi dan kemampuan untuk menangani banyak lalu lintas, seperti dalam skenario data center atau jaringan penyedia layanan.

3. **BGP (*Border Gateway Protocol*)**

   Perangkat Cisco mendukung BGP, protokol routing eksternal yang digunakan untuk pertukaran informasi routing antar jaringan besar, seperti penyedia layanan internet (ISP). BGP memungkinkan pengelolaan jalur lintas jaringan yang optimal berdasarkan kebijakan tertentu, menjadikannya protokol utama untuk jaringan global.

2.3.3 Fitur Tambahan

1. **QoS (*Quality of Service*)**

   QoS pada perangkat Cisco memastikan bahwa lalu lintas jaringan yang kritis, seperti data suara dan video, mendapatkan prioritas tinggi. Fitur ini membagi bandwidth secara dinamis, memastikan aplikasi penting tetap berjalan dengan latensi rendah dan tanpa gangguan, sementara aplikasi non-kritis diberikan prioritas lebih rendah. Teknologi ini sangat penting dalam skenario seperti konferensi video atau VoIP, di mana kualitas layanan memengaruhi pengalaman pengguna secara langsung.

2. **NetFlow**

   NetFlow adalah fitur monitoring yang dikembangkan oleh Cisco untuk menganalisis lalu lintas jaringan secara mendalam. Teknologi ini mencatat pola lalu lintas, sumber dan tujuan data, serta jenis protokol yang digunakan, memberikan wawasan real-time tentang performa jaringan. Dengan NetFlow, administrator jaringan dapat mengidentifikasi masalah, mengoptimalkan jalur lalu lintas, dan mendeteksi potensi ancaman keamanan, seperti anomali lalu lintas yang dapat menunjukkan adanya serangan DDoS.

3. **PoE (*Power over Ethernet*)**

   Cisco mendukung teknologi PoE, yang memungkinkan pengiriman daya listrik melalui kabel Ethernet standar. Fitur ini sangat bermanfaat dalam mengurangi kebutuhan kabel daya tambahan, menyederhanakan instalasi, dan meningkatkan fleksibilitas dalam penempatan perangkat seperti access point, kamera IP, dan perangkat IoT. Selain itu, Cisco juga menawarkan teknologi PoE+ dan UPOE (*Universal Power over Ethernet*) untuk mendukung perangkat yang membutuhkan daya lebih besar.

2.4 Arsitektur Sistem Operasi Cisco

Arsitektur sistem operasi pada perangkat Cisco merupakan komponen utama yang mendukung performa, fleksibilitas, dan keamanan jaringan. Cisco telah mengembangkan beberapa sistem operasi khusus, seperti Cisco IOS dan Cisco NX-OS, yang dirancang untuk memenuhi kebutuhan perangkat dan skenario jaringan yang

beragam. Setiap sistem operasi ini dibangun dengan fitur dan desain arsitektur yang disesuaikan untuk berbagai kebutuhan, mulai dari jaringan kecil hingga infrastruktur berskala besar. Berikut ini adalah penjelasan lebih mendalam mengenai sistem operasi yang digunakan pada perangkat Cisco.

2.4.1 Cisco IOS (*Internetwork Operating System*)

Cisco IOS adalah sistem operasi utama yang digunakan pada sebagian besar perangkat jaringan Cisco, seperti router dan switch. Sistem operasi ini dikenal karena kestabilan dan fleksibilitasnya dalam mendukung berbagai fungsi jaringan. Cisco IOS menggunakan antarmuka berbasis teks yang dikenal sebagai CLI untuk konfigurasi, pemantauan, dan manajemen perangkat jaringan. CLI memberikan kontrol penuh kepada administrator untuk mengatur parameter jaringan secara detail, seperti routing, keamanan, dan pengelolaan lalu lintas. Kemampuan ini memungkinkan administrator jaringan untuk mengoptimalkan perangkat sesuai kebutuhan spesifik mereka. Cisco IOS mendukung berbagai protokol routing dinamis, seperti OSPF (Open Shortest Path First), BGP (*Border Gateway Protocol*), dan EIGRP (*Enhanced Interior Gateway Routing Protocol*). Protokol ini memungkinkan perangkat secara otomatis menentukan jalur terbaik untuk mengirimkan data berdasarkan kondisi jaringan, seperti kepadatan lalu lintas atau kegagalan perangkat lain. Keamanan adalah fitur utama Cisco IOS, dengan dukungan untuk firewall, VPN (Virtual Private Network), dan kontrol akses berbasis peran (Role-Based Access Control). Fitur ini membantu melindungi jaringan dari ancaman internal dan eksternal dengan mengatur akses berdasarkan tingkat otorisasi pengguna. Cisco IOS juga dilengkapi dengan alat pemantauan seperti NetFlow, yang memungkinkan administrator untuk menganalisis lalu lintas jaringan secara real-time, mengidentifikasi anomali, dan memprediksi kebutuhan kapasitas di masa depan.

2.4.2 Cisco NX-OS

Cisco NX-OS adalah sistem operasi khusus yang dirancang untuk perangkat jaringan di data center, seperti seri Nexus. Sistem operasi ini memberikan kinerja tinggi, skalabilitas, dan keandalan

untuk memenuhi kebutuhan infrastruktur jaringan modern. Cisco NX-OS menggunakan arsitektur modular, yang berarti setiap fungsi dijalankan sebagai modul terpisah. Hal ini memungkinkan perangkat untuk tetap beroperasi bahkan jika salah satu modul mengalami kegagalan. Fitur ini mendukung ketersediaan tinggi (*high availability*), yang sangat penting dalam lingkungan data center di mana downtime dapat menyebabkan kerugian besar. NX-OS dirancang untuk bekerja secara optimal dengan perangkat Cisco Nexus, yang banyak digunakan dalam infrastruktur jaringan skala besar seperti data center. Sistem operasi ini mendukung virtualisasi jaringan, jaringan berbasis fabrik, dan integrasi dengan teknologi seperti SDN (*Software-Defined Networking*) untuk meningkatkan fleksibilitas dan efisiensi. Cisco NX-OS mendukung protokol jaringan yang dirancang khusus untuk kebutuhan data center, seperti FCoE (*Fibre Channel over Ethernet*) dan VXLAN (*Virtual Extensible LAN*). Protokol ini memungkinkan pengelolaan lalu lintas data dengan latensi rendah dan efisiensi tinggi, yang penting untuk aplikasi berbasis cloud dan virtualisasi.

Cisco memberikan perhatian besar terhadap keamanan sistem operasinya untuk melindungi jaringan dari ancaman yang terus berkembang. Beberapa langkah yang diambil oleh Cisco. Cisco secara rutin menyediakan pembaruan firmware untuk perangkatnya. Pembaruan ini tidak hanya memperbaiki bug atau kerentanan keamanan tetapi juga menambahkan fitur baru untuk meningkatkan kinerja perangkat. Sistem operasi Cisco dilengkapi dengan fitur keamanan bawaan seperti enkripsi data, pencegahan intrusi (IPS), dan kontrol akses berbasis identitas. Hal ini membantu melindungi perangkat dari ancaman siber seperti serangan DDoS atau akses tidak sah. Cisco IOS dan NX-OS telah mendapatkan berbagai sertifikasi keamanan dari lembaga independen, menunjukkan kepatuhannya terhadap standar keamanan global. Dengan arsitektur sistem operasi yang kuat dan fitur yang canggih, Cisco IOS dan NX-OS menjadi tulang punggung yang memungkinkan perangkat Cisco memberikan performa optimal, keamanan, dan keandalan di berbagai skenario jaringan, mulai dari jaringan kecil hingga data center besar.

2.6 Masa Depan Perangkat Cisco

Cisco terus berinovasi untuk memenuhi tuntutan jaringan modern yang semakin kompleks dan dinamis. Fokus utama masa depan perangkat Cisco adalah pengembangan teknologi baru yang memungkinkan efisiensi, fleksibilitas, dan keamanan jaringan, serta mendukung keberlanjutan lingkungan. Berikut adalah arah pengembangan utama perangkat Cisco.

2.6.1 Inovasi Teknologi

1. **SD-WAN (*Software-Defined Wide Area Network*)**

   Cisco telah memperkuat posisinya di pasar SD-WAN dengan menawarkan solusi yang mengintegrasikan jaringan tradisional dengan teknologi cloud. SD-WAN memungkinkan organisasi untuk menghubungkan berbagai lokasi dengan cara yang lebih efisien, mengurangi ketergantungan pada koneksi MPLS yang mahal, dan memberikan fleksibilitas dalam pengelolaan lalu lintas data. Teknologi ini memungkinkan aplikasi berbasis cloud untuk berjalan dengan performa optimal, sekaligus memastikan keamanan data melalui enkripsi dan kontrol akses berbasis kebijakan.

2. **AI dalam Jaringan**

   Cisco mulai mengintegrasikan kecerdasan buatan (AI) untuk mengelola dan mengoptimalkan jaringan secara lebih efisien. Dengan AI, perangkat Cisco dapat memprediksi masalah sebelum memengaruhi operasional, misalnya dengan menganalisis pola lalu lintas jaringan untuk mendeteksi potensi gangguan atau kerusakan perangkat. Mengotomatiskan pengelolaan jaringan, seperti menyesuaikan alokasi bandwidth berdasarkan kebutuhan aplikasi.

   Meningkatkan keamanan dengan mendeteksi anomali dalam lalu lintas data yang dapat menunjukkan potensi ancaman siber. Teknologi AI ini diintegrasikan melalui platform seperti Cisco DNA Center, yang memungkinkan analitik berbasis AI untuk pengelolaan jaringan yang lebih proaktif.

3. **IoT-Ready**

   Dengan meningkatnya adopsi perangkat Internet of Things (IoT) di berbagai sektor, perangkat Cisco kini dirancang untuk mendukung konektivitas IoT secara aman. Perangkat baru dilengkapi dengan protokol khusus dan kemampuan segmentasi jaringan, yang memisahkan lalu lintas IoT dari lalu lintas data utama untuk mencegah ancaman keamanan. Selain itu, perangkat ini dirancang untuk bekerja dalam lingkungan yang menantang, seperti pabrik atau lokasi terpencil, di mana perangkat IoT sering digunakan.

2.6.2 Fokus pada Sustainability

1. **Teknologi Hemat Energi**

   Dalam menghadapi tantangan perubahan iklim dan kebutuhan akan infrastruktur ramah lingkungan, Cisco berinvestasi dalam teknologi hemat energi. Misalnya, perangkat Cisco yang mendukung *Power over Ethernet* (PoE) dirancang untuk mengurangi konsumsi daya dengan mengalirkan energi hanya saat perangkat membutuhkannya. Selain itu, Cisco menggunakan komponen perangkat keras dengan efisiensi energi tinggi, seperti prosesor dan memori yang dirancang untuk mengurangi konsumsi daya tanpa mengorbankan performa.

2. **Desain Ramah Lingkungan**

   Cisco juga mengadopsi desain produk yang mendukung prinsip keberlanjutan. Misalnya, perangkat Cisco kini dibuat dari material yang dapat didaur ulang, dan proses produksi dioptimalkan untuk mengurangi jejak karbon. Selain itu, Cisco mendorong program pengelolaan siklus hidup perangkat, di mana perangkat yang sudah usang dapat dikembalikan untuk didaur ulang atau dimutakhirkan dengan komponen baru.

3. **Mendukung Infrastruktur Hijau**

   Cisco bekerja sama dengan berbagai organisasi untuk membangun infrastruktur jaringan yang mendukung inisiatif hijau. Perangkat Cisco dirancang untuk mendukung pusat data berkelanjutan, di mana efisiensi energi menjadi prioritas utama. Cisco juga menawarkan solusi manajemen energi berbasis IoT untuk membantu organisasi melacak dan mengoptimalkan penggunaan energi di seluruh jaringan mereka.

DAFTAR PUSTAKA

Cisco Systems (2023). Cisco IOS Software Overview. [Online] Available at: https://www.cisco.com [Accessed 8 December 2024].

Cisco Systems (2023). Cisco NX-OS Software Features and Benefits. [Online] Available at: https://www.cisco.com [Accessed 8 December 2024].

Cisco Systems (2023). What is SD-WAN? [Online] Available at: https://www.cisco.com [Accessed 8 December 2024].

Tanenbaum, A. S., and Wetherall, D. J. (2021). Computer Networks. 6th ed. Harlow: Pearson Education.

Stallings, W. (2020). Data and Computer Communications. 11th ed. Boston: Pearson.

Perkovic, I. (2020). Cisco Router Configuration Handbook. 2nd ed. Indianapolis: Cisco Press.

Odom, W. (2022). CCNA 200-301 Official Cert Guide, Volume 1 and 2. 6th ed. Indianapolis: Cisco Press.

Lammle, T. (2022). CCNA Certification Study Guide: Exam 200-301. 9th ed. Hoboken: Wiley.

Doyle, J. (2016). Routing TCP/IP, Volume I. 2nd ed. Indianapolis: Cisco Press.

Kumar, A. (2021). Introduction to Networking: Principles and Practices. 3rd ed. London: Springer.

Hucaby, D. (2022). Cisco ASA for Accidental Administrators: An Illustrated Step-by-Step ASA Learning and Configuration Guide. 3rd ed. CreateSpace Independent Publishing Platform.

Marschke, S., Moyer, J., and Diehl, C. (2019). SDN and NFV Simplified: A Visual Guide to Understanding Software Defined Networks and Network Function Virtualization. 1st ed. Indianapolis: Cisco Press.

Hucaby, D. (2020). Cisco Wireless LAN Security. 2nd ed. Indianapolis: Cisco Press.

Ramaswamy, K. (2020). IP Routing on Cisco IOS, IOS XE, and IOS XR: An Essential Guide to Understanding and Implementing IP Routing Protocols. 2nd ed. Indianapolis: Cisco Press.

BAB 3
PENGANTAR INTERNET PROTOCOL VERSI 4 (IPv4)

3.1 Pendahuluan

Pengalamatan IP adalah komponen fundamental dalam jaringan komputer yang memungkinkan perangkat-perangkat untuk saling berkomunikasi di internet maupun dalam jaringan lokal. IPv4 (*Internet Protocol version* 4) merupakan versi protokol internet yang paling banyak digunakan sejak pertama kali diperkenalkan. IPv4 menggunakan skema alamat 32-bit yang memungkinkan sekitar 4,3 miliar alamat IP unik. Meskipun jumlah ini terdengar besar, seiring waktu kebutuhan akan alamat IP semakin meningkat akibat pesatnya perkembangan teknologi, perangkat, dan pengguna internet.

Alamat IP diatur ke dalam beberapa kelas untuk memudahkan distribusi dan manajemen jaringan berdasarkan kebutuhan yang berbeda-beda. Klasifikasi ini membantu organisasi dalam menentukan skala jaringan yang dibutuhkan, baik itu untuk jaringan besar, menengah, atau kecil. Dalam klasifikasi ini, terdapat lima kelas utama: Kelas A, B, C, D, dan E, masing-masing dengan karakteristik unik yang sesuai dengan jumlah host dan pengguna jaringan. Memahami pengklasifikasian ini sangat penting bagi administrator jaringan untuk mengoptimalkan penggunaan alamat IP secara efisien dan memastikan bahwa jaringan berfungsi dengan baik. Selain itu, konsep seperti subnetting digunakan untuk membagi jaringan lebih lanjut, meningkatkan fleksibilitas dalam manajemen jaringan yang kompleks.

3.2 Apa itu IP Address ?

IP Address (*Internet Protocol Address*) adalah sebuah label numerik unik yang diberikan kepada setiap perangkat yang terhubung ke jaringan komputer berbasis protokol internet, seperti

komputer, server, printer, atau perangkat lain. Alamat ini digunakan untuk mengidentifikasi dan menghubungkan perangkat-perangkat tersebut, memungkinkan komunikasi antar mereka di dalam jaringan, baik lokal (LAN) maupun internet. Setiap perangkat yang terhubung ke internet membutuhkan alamat IP agar dapat saling bertukar informasi dan data.

IP Address terdiri dari serangkaian angka yang dibagi ke dalam beberapa bagian. Ada dua versi utama alamat IP yang digunakan di dunia saat ini: IPv4 dan IPv6.

1. IPv4 (*Internet Protocol version* 4) menggunakan skema alamat 32-bit yang terdiri dari empat bagian (oktet), di mana setiap bagian dipisahkan oleh titik dan diwakili oleh angka desimal (contoh: 192.168.0.1). IPv4 memungkinkan sekitar 4,3 miliar alamat unik.
2. IPv6 (Internet Protocol version 6) adalah pengembangan dari IPv4 dan menggunakan skema alamat 128-bit, yang terdiri dari delapan kelompok angka heksadesimal dipisahkan oleh titik dua (contoh: 2001:0db8:85a3:0000:0000:8a2e:0370:7334). IPv6 dikembangkan untuk menangani keterbatasan ruang alamat IPv4 yang semakin habis seiring meningkatnya jumlah perangkat yang terhubung ke internet.

Setiap alamat IP dibagi menjadi dua komponen: Network ID dan Host ID. Network ID digunakan untuk mengidentifikasi jaringan di mana perangkat tersebut berada, sedangkan Host ID mengidentifikasi perangkat tertentu di dalam jaringan tersebut.

Ada dua jenis alamat IP:

1. Alamat IP Publik, yang dapat diakses oleh perangkat lain melalui internet.
2. Alamat IP Privat, yang digunakan dalam jaringan lokal dan tidak dapat diakses langsung dari internet.

Secara umum, IP Address berfungsi sebagai "alamat rumah" bagi perangkat di jaringan, memungkinkan mereka untuk saling mengenali dan bertukar informasi. Tanpa IP Address, komunikasi data di internet tidak mungkin terjadi. IP Address ini sangat penting

untuk memastikan bahwa data yang dikirim dari satu perangkat sampai ke tujuan yang benar tanpa masalah.

3.2.1 Sejarah Pengembangan IPv4

IPv4 (Internet Protocol version 4) adalah protokol komunikasi yang dikembangkan pada awal 1980-an oleh DARPA (*Defense Advanced Research Projects Agency*) sebagai bagian dari proyek ARPANET, jaringan komputer pertama yang menjadi dasar perkembangan internet modern. IPv4 diperkenalkan sebagai bagian dari RFC 791 pada tahun 1981, menggantikan protokol sebelumnya yang kurang efisien dalam mengelola komunikasi antar jaringan.

Pada saat pengembangan IPv4, kebutuhan akan alamat IP global dianggap cukup terpenuhi dengan menggunakan skema alamat 32-bit, yang memungkinkan sekitar 4,3 miliar alamat unik. Pada masa itu, internet masih dalam tahap awal, dan hanya sebagian kecil organisasi, akademisi, dan lembaga pemerintah yang terhubung ke jaringan.

Seiring dengan pesatnya pertumbuhan internet pada akhir 1990-an dan awal 2000-an, jumlah perangkat yang terhubung melonjak drastis, menyebabkan ketidakcukupan alamat IPv4. Untuk mengatasi masalah ini, berbagai solusi sementara seperti NAT (*Network Address Translation*) dan CIDR (*Classless Inter-Domain Routing*) diperkenalkan guna memperpanjang masa pakai IPv4.

Namun, keterbatasan ruang alamat IPv4 tetap menjadi tantangan besar, yang akhirnya mendorong pengembangan IPv6, protokol pengganti dengan ruang alamat yang jauh lebih besar. Meski begitu, IPv4 masih menjadi protokol yang dominan hingga saat ini, dengan transisi ke IPv6 yang berlangsung secara bertahap.

3.2.2 Struktur Dasar IP Address

Dalam Cisco Routing and Switching, pada Bab 3 yang membahas Pengantar IP Address IPv4, dijelaskan bahwa IP Address adalah pengenal unik yang digunakan untuk menghubungkan perangkat dalam jaringan berbasis IP. Struktur dasar dari alamat IP versi 4 (IPv4) terdiri dari 32-bit angka biner yang dibagi menjadi empat bagian, atau disebut juga oktet, yang dipisahkan oleh titik.

Setiap oktet diwakili oleh angka desimal dalam rentang 0 hingga 255. Contoh alamat IP dalam format desimal adalah 192.168.1.1.

IPv4 terdiri dari dua bagian utama, yaitu Network ID dan Host ID. Network ID mengidentifikasi jaringan tempat perangkat berada, sementara Host ID mengidentifikasi perangkat spesifik dalam jaringan tersebut. Alamat IP juga dikategorikan ke dalam beberapa kelas (A, B, C, D, E) yang membedakan skala jaringan berdasarkan jumlah perangkat yang diakomodasi.

Subnet mask digunakan bersamaan dengan IP Address untuk memisahkan bagian jaringan dan host dalam sebuah alamat IP, membantu mengelola dan mengidentifikasi subnet di jaringan.

3.3 Pengklasifikasian IP Address

IP Address IPv4 dibagi menjadi beberapa kelas, yang membantu mengidentifikasi jaringan dan perangkat dalam skala besar hingga kecil. Setiap kelas memiliki rentang tertentu yang memungkinkan untuk mendukung berbagai ukuran jaringan.

3.3.1 Kelas-kelas IP Address

Dalam protokol IPv4, alamat IP diklasifikasikan ke dalam lima kelas utama: Kelas A, B, C, D, dan E, berdasarkan rentang alamat dan ukuran jaringan yang dapat didukung. Klasifikasi ini memudahkan pengalokasian alamat IP untuk berbagai ukuran jaringan, dari yang sangat besar hingga yang kecil. Setiap kelas memiliki karakteristik yang berbeda-beda dalam hal jumlah jaringan dan host.

1. **Kelas A** digunakan untuk jaringan berskala besar, seperti perusahaan internasional atau penyedia layanan internet. Alamat ini memungkinkan hingga 16 juta host dalam satu jaringan, tetapi jumlah jaringan yang didukung lebih sedikit.
2. **Kelas B** ditujukan untuk jaringan berskala menengah, seperti universitas atau organisasi besar. Setiap jaringan dapat memiliki hingga 65.000 host, dengan lebih banyak jumlah jaringan dibanding Kelas A.
3. **Kelas C** digunakan untuk jaringan kecil, seperti kantor atau perusahaan kecil. Jumlah host yang didukung hanya 254 per jaringan, tetapi jumlah jaringan yang didukung sangat banyak.

4. **Kelas D** digunakan untuk multicast, di mana data dikirim ke beberapa perangkat sekaligus.
5. **Kelas E** dicadangkan untuk tujuan eksperimental dan penelitian.

Berikut adalah tabel klasifikasi IP Address berdasarkan kelas:

Tabel 3.1. Klasifikasi Kelas IP Jaringan

Kelas IP	Rentang Alamat	Jumlah Jaringan	Jumlah Host per Jaringan
Kelas A	1.0.0.0 - 126.255.255.255	128 jaringan	16 juta host
Kelas B	128.0.0.0 - 191.255.255.255	16.384 jaringan	65.534 host
Kelas C	192.0.0.0 - 223.255.255.255	2.097.152 jaringan	254 host
Kelas D	224.0.0.0 - 239.255.255.255	Multicast	-
Kelas E	240.0.0.0 - 255.255.255.255	Eksperimen	-

Dengan memahami klasifikasi IP Address, administrator jaringan dapat menentukan jenis jaringan yang paling sesuai berdasarkan skala dan kebutuhan penggunaannya. Penggunaan yang tepat dari setiap kelas IP dapat membantu menghindari pemborosan alamat IP dan meningkatkan efisiensi jaringan. Meski IPv6 telah diperkenalkan untuk mengatasi keterbatasan IPv4, klasifikasi IP Address dalam IPv4 tetap relevan dan penting untuk dipelajari dalam dunia jaringan saat ini, Meski saat ini sudah ada IPv6, IPv4 masih digunakan secara luas di seluruh dunia.

3.3.2 Penggunaan Kelas IP Sesuai Kebutuhan

Dalam konteks **Cisco Routing and Switching**, memahami penggunaan kelas IP Address sesuai kebutuhan adalah penting untuk memastikan jaringan berfungsi optimal. Setiap kelas IP menawarkan skala dan cakupan yang berbeda, yang dirancang untuk memenuhi berbagai ukuran jaringan.

1. **Kelas A** cocok untuk organisasi besar atau penyedia layanan internet yang memiliki banyak perangkat, karena mendukung hingga jutaan host dalam satu jaringan.

2. **Kelas B** ideal untuk jaringan menengah, seperti universitas atau perusahaan besar, yang membutuhkan ruang untuk puluhan ribu host.
3. **Kelas C** paling sering digunakan untuk jaringan kecil, seperti kantor atau bisnis kecil, yang hanya memerlukan sedikit perangkat dengan dukungan hingga 254 host per jaringan.
4. Kelas **D** digunakan khusus untuk multicast, sedangkan **Kelas E** dicadangkan untuk penelitian dan pengembangan. Memilih kelas IP yang tepat memungkinkan pemanfaatan alamat IP secara efisien, meminimalkan pemborosan, dan mengoptimalkan kinerja jaringan sesuai dengan kebutuhan organisasi.

3.4 Struktur IPv4

Struktur dasar IPv4 yang terdiri dari 32-bit angka biner yang dibagi menjadi empat bagian, atau oktet. Setiap oktet dipisahkan oleh titik dan diwakili oleh angka desimal dalam rentang 0 hingga 255. Contoh representasi IPv4 adalah 192.168.1.1.

Setiap alamat IPv4 dibagi menjadi dua bagian utama: Network ID dan Host ID. Network ID digunakan untuk mengidentifikasi jaringan tempat perangkat berada, sementara Host ID mengidentifikasi perangkat tertentu dalam jaringan tersebut. Kombinasi dari keduanya memungkinkan perangkat saling berkomunikasi dalam jaringan yang sama maupun dengan jaringan lain.

IPv4 juga mendukung penggunaan Subnet Mask, yang membantu membagi jaringan besar menjadi beberapa subnet kecil. Subnet mask adalah serangkaian angka 32-bit yang juga ditulis dalam format desimal, seperti 255.255.255.0, yang berfungsi untuk memisahkan bagian alamat IP mana yang mewakili network dan host.

Selain itu, IPv4 mengimplementasikan berbagai mekanisme untuk mengelola ruang alamat yang terbatas, seperti CIDR (*Classless Inter-Domain Routing*), yang memungkinkan fleksibilitas lebih dalam alokasi alamat IP dan mengatasi keterbatasan klasifikasi berbasis kelas.

Struktur IPv4 ini memberikan kerangka kerja yang kuat untuk pengalamatan di internet, meskipun dengan pertumbuhan perangkat yang pesat, IPv6 dikembangkan sebagai solusi jangka panjang. Meski begitu, IPv4 masih mendominasi dalam banyak aplikasi jaringan dan tetap relevan hingga saat ini.

3.4.1 Network ID

Network ID adalah komponen kunci dalam pengalamatan IP yang berfungsi untuk mengidentifikasi jaringan tempat perangkat atau host berada. Dengan adanya Network ID, perangkat dalam jaringan yang sama dapat saling berkomunikasi secara efisien, sementara router dapat menentukan jalur yang tepat untuk mengirimkan data ke jaringan lain.

Struktur alamat IPv4 terdiri dari 32 bit, yang dibagi menjadi empat oktet. Jumlah bit yang dialokasikan untuk Network ID bervariasi tergantung pada klasifikasi alamat IP, yang terbagi menjadi beberapa kelas:

1. **Kelas A**: Dalam kelas ini, Network ID terdiri dari 8 bit pertama (oktet pertama), yang memungkinkan hingga 128 jaringan dan dapat mendukung hingga 16 juta host per jaringan. Format ini cocok untuk organisasi besar atau penyedia layanan internet.
2. **Kelas B**: Untuk kelas ini, Network ID terdiri dari 16 bit pertama (dua oktet pertama), mendukung hingga 16.384 jaringan dan hingga 65.534 host per jaringan. Kelas B ideal untuk jaringan menengah, seperti universitas atau perusahaan besar.
3. **Kelas C**: Pada kelas ini, Network ID mencakup 24 bit pertama (tiga oktet pertama), yang mendukung hingga 2.097.152 jaringan, tetapi hanya dapat menampung hingga 254 host per jaringan. Kelas C biasanya digunakan untuk jaringan kecil, seperti kantor atau bisnis kecil.

Pemahaman tentang Network ID dan jumlah bit yang dialokasikan untuk setiap kelas sangat penting dalam perancangan dan pengelolaan jaringan, memungkinkan penggunaan alamat IP yang efisien dan terstruktur.

3.4.2 Host ID

Host ID adalah bagian dari alamat IP yang digunakan untuk mengidentifikasi perangkat atau host tertentu dalam jaringan. Setiap perangkat yang terhubung ke jaringan, seperti komputer, printer, atau router, memerlukan Host ID yang unik agar dapat berkomunikasi dengan perangkat lain di dalam atau di luar jaringan tersebut.

Struktur alamat IPv4 terdiri dari 32 bit, yang dibagi menjadi dua bagian utama: Network ID dan Host ID. Jumlah bit yang digunakan untuk Host ID bervariasi berdasarkan klasifikasi alamat IP, yang terdiri dari Kelas A, B, dan C.

1. **Kelas A**: Dalam kelas ini, 24 bit terakhir (tiga oktet terakhir) digunakan untuk Host ID. Ini memungkinkan setiap jaringan Kelas A untuk memiliki hingga 16 juta host. Alamat ini sangat cocok untuk organisasi besar yang memerlukan banyak perangkat dalam satu jaringan.
2. **Kelas B**: Untuk alamat Kelas B, 16 bit terakhir (dua oktet terakhir) dialokasikan untuk Host ID. Dengan demikian, setiap jaringan Kelas B dapat mendukung hingga 65.534 host. Kelas ini dirancang untuk jaringan menengah, seperti universitas atau perusahaan besar.
3. **Kelas C**: Di kelas ini, 8 bit terakhir (satu oktet terakhir) digunakan untuk Host ID, yang hanya memungkinkan hingga 254 host per jaringan. Kelas C umumnya digunakan untuk jaringan kecil, seperti kantor atau bisnis kecil.

Selain itu, penting untuk memahami bahwa beberapa alamat IP dari setiap kelas dialokasikan untuk tujuan khusus, seperti alamat siaran (*broadcast*) dan alamat jaringan itu sendiri, yang mengurangi jumlah Host ID yang tersedia. Pemahaman yang mendalam tentang Host ID dan jumlah bit yang dialokasikan untuk setiap kelas sangat penting untuk perancangan dan pengelolaan jaringan yang efisien. Hal ini memungkinkan administrator jaringan untuk mengoptimalkan penggunaan alamat IP dan memastikan komunikasi yang efektif di dalam jaringan.

3.5 Subnetting Pada IPv4

Subnetting adalah proses membagi jaringan IP besar menjadi subnet-subnet yang lebih kecil. Subnetting memungkinkan efisiensi yang lebih tinggi dalam pengalokasian alamat IP dan meningkatkan keamanan serta kinerja jaringan. Dengan menggunakan subnetting, administrator jaringan dapat mengelompokkan perangkat berdasarkan lokasi, fungsi, atau kebutuhan lainnya, sehingga memudahkan dalam pengelolaan dan pemantauan lalu lintas data. Subnetting menjadi sangat penting dalam jaringan yang memiliki banyak perangkat dan memerlukan pengaturan yang kompleks.

Pada implementasinya, subnetting memungkinkan pembagian jaringan untuk memaksimalkan pemanfaatan alamat IP yang tersedia, terutama ketika jumlah perangkat dalam setiap subnet jauh lebih kecil daripada kapasitas jaringan utuh. Misalnya, dalam jaringan dengan alamat IP kelas B, administrator dapat membagi jaringan menjadi beberapa subnet yang lebih kecil menggunakan CIDR (*Classless Inter-Domain Routing*). CIDR menghilangkan keterbatasan klasifikasi IP tradisional, memungkinkan fleksibilitas dalam alokasi alamat dan pengelolaan subnet. Dengan menggunakan teknik ini, pengaturan IP lebih fleksibel dan dapat disesuaikan dengan kebutuhan organisasi yang dinamis.

3.5.1 Konsep Dasar Subnetting

Dalam struktur alamat IPv4, yang terdiri dari 32 bit, subnetting memanfaatkan **Subnet Mask** untuk menentukan jumlah bit yang dialokasikan pada Network ID dan Host ID. Misalnya, jika alamat IP memiliki subnet mask **/24** atau **255.255.255.0,** maka 24 bit pertama digunakan untuk Network ID, dan 8 bit sisanya untuk Host ID. Dengan mengubah subnet mask, jumlah bit yang dialokasikan untuk Network ID dan Host ID dapat diatur ulang sesuai kebutuhan jaringan.

Dengan subnetting, kita dapat mengisolasi lalu lintas broadcast dalam setiap subnet, yang mengurangi beban pada jaringan utama dan memungkinkan komunikasi yang lebih efisien. Subnetting juga membantu meningkatkan keamanan, karena setiap subnet dapat dikonfigurasi dengan aturan akses dan keamanan yang

berbeda. Teknik ini sangat berguna dalam jaringan besar atau perusahaan yang memerlukan pengelolaan alamat IP yang lebih fleksibel dan terstruktur, sehingga semua perangkat dapat dikelola dengan optimal sesuai fungsinya dalam jaringan.

3.5.2 Manfaat Subnetting

Dengan subnetting, administrator jaringan dapat memisahkan jaringan besar menjadi bagian yang lebih kecil dan lebih terkelola. Ini memudahkan kontrol lalu lintas data, menambah keamanan, dan mengurangi konflik IP.

Salah satu manfaat utama subnetting adalah efisiensi penggunaan alamat IP. Dengan membagi satu jaringan besar menjadi subnet-subnet yang lebih kecil, alamat IP dapat dioptimalkan sehingga tidak ada pemborosan. Ini sangat penting dalam mengatasi keterbatasan alamat IPv4.

Selain itu, subnetting juga meningkatkan kinerja jaringan. Dengan membatasi lalu lintas broadcast hanya dalam subnet tertentu, beban pada jaringan utama berkurang, sehingga koneksi menjadi lebih cepat dan stabil. Keamanan jaringan juga meningkat melalui subnetting, karena setiap subnet dapat memiliki aturan akses dan konfigurasi keamanan yang berbeda, mencegah ancaman atau akses yang tidak diinginkan dari luar subnet tersebut.

Keuntungan utama dari subnetting adalah kemampuan untuk mengontrol lalu lintas jaringan. Karena setiap subnet berfungsi sebagai jaringan terpisah, broadcast atau pengiriman data yang bersifat menyebar hanya terbatas dalam subnet tersebut, sehingga mengurangi beban lalu lintas dan menghindari potensi konflik. Hal ini sangat berguna di jaringan yang luas dan padat, seperti pada perusahaan atau universitas, di mana subnet-subnet kecil dapat dikonfigurasi berdasarkan departemen atau divisi untuk memfasilitasi kontrol akses dan keamanan data.

Misalkan kita memiliki alamat IP 192.168.10.0/24 yang termasuk dalam Kelas C, di mana subnet mask default adalah 255.255.255.0. Dalam konfigurasi ini, /24 menunjukkan bahwa 24 bit pertama (atau tiga oktet pertama) digunakan untuk Network ID, sementara 8 bit terakhir digunakan untuk Host ID. Ini berarti kita memiliki satu jaringan yang mendukung hingga 254 host (karena ada

2 bit khusus untuk alamat jaringan dan alamat broadcast yang tidak bisa digunakan sebagai Host ID).

Namun, jika kita ingin membagi jaringan ini menjadi beberapa subnet yang lebih kecil, kita dapat memodifikasi subnet mask dengan mengambil bit tambahan dari Host ID dan menambahkannya ke Network ID. Misalnya, dengan mengubah subnet mask menjadi /26 (atau 255.255.255.192), kita akan menambahkan dua bit tambahan untuk Network ID. Ini memungkinkan kita untuk membuat empat subnet dalam jaringan tersebut.

Contoh Penghitungan Subnet:

1. Alamat Jaringan Awal: 192.168.10.0/24
2. Subnet Mask Baru: /26 atau 255.255.255.192
3. Jumlah Subnet yang Dihasilkan: Dengan dua bit tambahan, kita memiliki $2^2 = 4$ subnet.

Setiap subnet akan mendukung 64 alamat total, tetapi hanya 62 alamat host yang dapat digunakan karena dua alamat dikhususkan untuk jaringan dan broadcast.

Tabel 3.2. Range IP berdasarkan Subnet

Subnet	Network ID	Range Host	Broadcast Address
Subnet 1	192.168.10.0/26	192.168.10.1 - 192.168.10.62	192.168.10.63
Subnet 2	192.168.10.64/26	192.168.10.65 - 192.168.10.126	192.168.10.127
Subnet 3	192.168.10.128/26	192.168.10.129 - 192.168.10.190	192.168.10.191
Subnet 4	192.168.10.192/26	192.168.10.193 - 192.168.10.254	192.168.10.255

Dengan demikian, jaringan awal 192.168.10.0/24 berhasil dipecah menjadi empat subnet terpisah, masing-masing dengan 62 host yang dapat digunakan. Teknik ini membuat pengelolaan jaringan lebih fleksibel dan meningkatkan keamanan serta efisiensi komunikasi antar subnet.

3.6 Pembagian Alamat IP: Public dan Private

Dalam jaringan komputer, alamat IP terbagi menjadi Public IP dan Private IP. Pembagian ini memungkinkan penggunaan alamat IP yang lebih efisien dan memastikan koneksi yang aman antarjaringan. Public IP adalah alamat yang digunakan untuk mengidentifikasi

perangkat pada jaringan publik, seperti internet, sehingga perangkat dengan alamat Public IP dapat diakses oleh perangkat lain di seluruh dunia. Penyedia Layanan Internet (ISP) menyediakan dan mengelola alokasi Public IP ini, yang unik dan tidak boleh digunakan secara berulang untuk menghindari konflik alamat. Contoh dari rentang Public IP adalah 8.8.8.8 dan 142.250.190.78.

Sebaliknya, Private IP digunakan di dalam jaringan lokal atau *Local Area Network* (LAN), seperti di rumah atau kantor, dan tidak dapat diakses secara langsung dari internet. Alamat Private IP digunakan untuk mengidentifikasi perangkat di dalam jaringan internal, memisahkannya dari jaringan eksternal. Contoh rentang Private IP mencakup alamat-alamat di kelas A (10.0.0.0 - 10.255.255.255), kelas B (172.16.0.0 - 172.31.255.255), dan kelas C (192.168.0.0 - 192.168.255.255).

Penggunaan Private IP dalam jaringan lokal memberikan keamanan tambahan karena perangkat di jaringan eksternal tidak dapat mengakses perangkat dengan Private IP tanpa perantara, seperti NAT (*Network Address Translation*). NAT mengonversi alamat Private IP menjadi Public IP saat perangkat di jaringan internal memerlukan akses ke internet. Dengan memisahkan Public dan Private IP, subnetting membantu meningkatkan keamanan, efisiensi, dan pemanfaatan sumber daya jaringan yang lebih baik dalam skala lokal maupun global.

Berikut adalah contoh tabel pembagian alamat **Public IP** dan **Private IP** beserta rentangnya:

Tabel 3.3. Pembagian Alamat Public IP dan Private IP

Jenis Alamat	Rentang Alamat IP	Contoh Penggunaan
Public IP	Semua alamat IP di luar rentang Private IP	Digunakan oleh perangkat di internet untuk dapat diakses secara global. Contoh: 8.8.8.8 (Google DNS) atau 142.250.190.78 (Google).
Private IP (Kelas A)	10.0.0.0 - 10.255.255.255	Digunakan untuk jaringan internal perusahaan besar. Contoh: 10.0.0.1 atau 10.255.255.254

Jenis Alamat	Rentang Alamat IP	Contoh Penggunaan
Private IP (Kelas B)	172.16.0.0 - 172.31.255.255	Umumnya digunakan dalam jaringan internal menengah. Contoh: 172.16.0.1 atau 172.31.255.254
Private IP (Kelas C)	192.168.0.0 - 192.168.255.255	Sering digunakan di jaringan rumah atau kantor kecil. Contoh: 192.168.0.1 atau 192.168.255.254

Tabel ini menunjukkan rentang alamat IP yang dapat digunakan sesuai dengan jenisnya. Public IP unik dan global, sedangkan Private IP digunakan di dalam jaringan lokal untuk identifikasi perangkat dan pengaturan keamanan tambahan.

3.7 Kekurangan IPv4

IPv4, sebagai versi protokol Internet yang pertama kali diterapkan secara luas, memiliki beberapa keterbatasan yang semakin terlihat seiring perkembangan teknologi dan meningkatnya jumlah perangkat yang terhubung ke internet. Salah satu kekurangan terbesar IPv4 adalah terbatasnya jumlah alamat IP. IPv4 menggunakan format 32 bit yang hanya dapat menghasilkan sekitar 4,3 miliar alamat unik. Pada awalnya, jumlah ini diperkirakan sudah mencukupi, tetapi dengan pesatnya pertumbuhan perangkat digital, terutama di era Internet of Things (IoT), kebutuhan akan alamat IP jauh melebihi kapasitas IPv4. Alhasil, distribusi alamat IP menjadi tidak merata, menyebabkan kelangkaan di banyak wilayah.

Keterbatasan IPv4 juga mempengaruhi efisiensi pengelolaan jaringan. Sebagai solusi, teknik seperti *Network Address Translation* (NAT) banyak digunakan untuk memungkinkan perangkat dengan alamat Private IP berkomunikasi melalui satu alamat Public IP. Namun, NAT sering kali memperumit konfigurasi jaringan dan membuat penerapan protokol tertentu lebih sulit karena adanya lapisan tambahan dalam aliran data.

Dari sisi keamanan, IPv4 juga memiliki kelemahan. IPv4 tidak dirancang dengan keamanan sebagai prioritas utama, sehingga protokol ini rentan terhadap berbagai serangan siber. Meskipun

teknologi enkripsi dan firewall dapat diterapkan, hal ini sering memerlukan konfigurasi tambahan dan solusi di luar protokol itu sendiri. *Internet Protocol Security* (IPsec), misalnya, tidak secara native terintegrasi dengan IPv4, berbeda dengan IPv6 yang sudah mendukung keamanan lebih baik secara bawaan.

Selain itu, fragmentasi alamat adalah kelemahan lain dari IPv4. Karena keterbatasan dalam klasifikasi alamat IP, blok alamat sering kali tidak teralokasikan secara optimal, menciptakan jaringan dengan alamat yang tidak sepenuhnya digunakan. Ini memperburuk masalah ketersediaan dan menyebabkan inefisiensi dalam distribusi alamat IP.

Secara keseluruhan, IPv4 mulai menunjukkan batasannya seiring dengan perkembangan internet modern. Untuk mengatasi kekurangan ini, IPv6 dikembangkan sebagai penerus dengan ruang alamat yang jauh lebih besar dan fitur-fitur tambahan untuk mendukung efisiensi, keamanan, dan fleksibilitas jaringan. Akan tetapi, meskipun IPv6 menawarkan berbagai keunggulan, migrasi penuh ke IPv6 masih berjalan lambat, dan IPv4 tetap digunakan secara luas dalam infrastruktur internet di seluruh dunia.

3.8 IPv4 dan Transisi ke IPv6

Pv4 adalah versi keempat dari protokol Internet yang pertama kali diperkenalkan pada tahun 1981 dan telah menjadi standar utama untuk mengidentifikasi perangkat dalam jaringan. Dengan panjang alamat 32 bit, IPv4 mampu menyediakan sekitar 4,3 miliar alamat unik, yang pada awalnya diperkirakan mencukupi kebutuhan global. Namun, pesatnya pertumbuhan perangkat digital, termasuk komputer, smartphone, dan perangkat *Internet of Things* (IoT), menyebabkan keterbatasan jumlah alamat IP menjadi semakin kritis. Akibatnya, sistem yang mengandalkan IPv4 menghadapi tantangan dalam mengakomodasi jumlah perangkat yang terus meningkat.

Untuk mengatasi kekurangan tersebut, IPv6 dikembangkan dengan ruang alamat yang jauh lebih luas, menggunakan format 128 bit yang memungkinkan sekitar 340 triliun-triliun-triliun alamat. Hal ini tidak hanya memperluas kapasitas, tetapi juga menyediakan ruang yang cukup untuk ekspansi masa depan tanpa batasan yang

signifikan. IPv6 juga membawa berbagai perbaikan lainnya, termasuk dukungan bawaan untuk *Internet Protocol Security* (IPsec), yang meningkatkan keamanan jaringan dengan menyediakan enkripsi dan autentikasi data.

Transisi dari IPv4 ke IPv6, meskipun diperlukan, tidaklah mudah. IPv4 dan IPv6 tidak kompatibel secara langsung, sehingga berbagai teknik transisi perlu diterapkan untuk memungkinkan keduanya berfungsi bersama. Beberapa teknik transisi umum meliputi Dual Stack, Tunneling, dan Translation. Dual Stack memungkinkan perangkat untuk menggunakan alamat IPv4 dan IPv6 secara bersamaan, sehingga perangkat dapat berkomunikasi di kedua jaringan. Tunneling adalah metode di mana paket IPv6 "diterowongkan" melalui jaringan IPv4, memungkinkan data IPv6 melewati infrastruktur IPv4. Sedangkan Translation menggunakan penerjemah protokol untuk mengonversi alamat dan data IPv4 ke dalam format IPv6 dan sebaliknya.

Penerapan IPv6 menghadapi hambatan, terutama dalam infrastruktur lama yang hanya mendukung IPv4. Banyak perangkat jaringan, aplikasi, dan sistem operasi perlu diperbarui atau diganti untuk mendukung IPv6, yang dapat memakan biaya dan waktu. Meski demikian, sebagian besar penyedia layanan internet (ISP) dan perusahaan besar kini mulai mengadopsi IPv6 secara bertahap untuk memenuhi kebutuhan modern.

Secara keseluruhan, transisi ke IPv6 sangat penting dalam memastikan keberlanjutan dan perluasan jaringan internet. IPv6 tidak hanya menyediakan solusi atas keterbatasan alamat, tetapi juga meningkatkan efisiensi, keamanan, dan kemampuan jaringan. Walaupun transisi penuh masih berlangsung, IPv6 diharapkan menjadi fondasi utama infrastruktur jaringan di masa depan, mendukung perkembangan internet yang semakin luas dan kompleks.

DAFTAR PUSTAKA

Afrizal and Fitriani (no date) 'Penerapan IPV4 dan IPV6pada Jaringanyang Terhubung.pdf'.

Ashraf, S., Muhammad, D. and Aslam, Z. (2020) 'Analyzing challenging aspects of IPv6 over IPv4', *Jurnal Ilmiah Teknik Elektro Komputer dan Informatika*, 6(1), p. 54. Available at: https://doi.org/10.26555/jiteki.v16i1.17105.

Comer, D.E. (2018) *Internetworking with TCP/IP Volume One: Principles, Protocols, and Architecture*. 6th edn. Pearson: Pearson.

Hossain, M.A. *et al.* (2016) 'Performance Analysis of Three Transition Mechanisms between IPv6 Network and IPv4 Network: Dual Stack, Tunneling and Translation', *International Journal of Computer*, 20(1), pp. 217–228. Available at: http://ijcjournal.org/.

Ip, T. *et al.* (1981) 'Chapter 3 INTERNET PROTOCOL VERSIONS 4 (IPV4)', 4, pp. 3–4.

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

Sisat, S.N., Bhopale, P.S. and Barbudhe, V.K. (2016) 'IP Subnetting', *International Journal of Electronics, Communication & Soft Computing Science and Engineering*, 2(5), pp. 3–8.

Stallings, W. (2020) *Data and Computer Communications*. 11th edn. Pearson: Pearson.

Syafrizal, M., Qamar, S. and Aji, D.B. (2013) 'IMPLEMENTASI MIGRASI IPV4 KE IPV6 Hasil Penelitian dan Pembahasan', *Jurnal Dasi*, 14(1), pp. 44–50.

Tanenbaum, A.S. and Wetherall, D.J. (2013) *Computer Networks*. 5th edn. Pearson: Pearson.

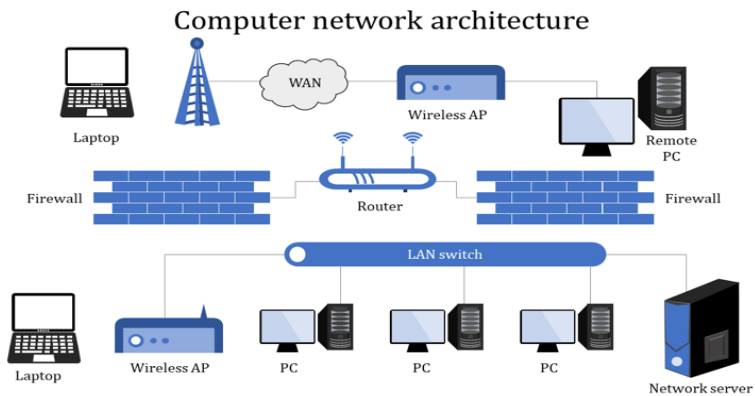
Tiwari, M.K. *et al.* (2024) 'The Comprehensive Review: Internet Protocol (IP) Address a Primer for Digital Connectivity', *Asian Journal of Research in Computer Science*, 17(8), pp. 34–45. Available at: https://doi.org/10.9734/ajrcos/2024/v17i7488.

BAB 4
KONSEP DASAR JARINGAN (BASIC NETWORK)

4.1 Pengertian Jaringan Komputer

Jaringan komputer adalah sekumpulan perangkat yang saling terhubung untuk berbagi sumber daya dan informasi (Mary Jeya Jothi, 2015; Jain and Pateriya, 2019; Najath, Herath and Rajapakse, 2022). Jaringan ini memungkinkan perangkat-perangkat seperti komputer, server, printer, dan perangkat lain untuk saling berkomunikasi dan bertukar data . Dalam dunia yang semakin terhubung ini, jaringan komputer menjadi komponen yang sangat vital dalam berbagai aspek kehidupan sehari-hari, mulai dari komunikasi pribadi hingga operasi bisnis besar.

Pada dasarnya, jaringan komputer terdiri dari dua komponen utama, yaitu *hardware* dan *software*. Perangkat keras atau *hardware* meliputi komponen fisik yang digunakan untuk menghubungkan perangkat, seperti kabel, router, switch, dan perangkat penghantar lainnya. Sedangkan perangkat lunak atau *software* mencakup sistem operasi jaringan dan protokol yang memungkinkan perangkat-perangkat tersebut berinteraksi satu sama lain.



Gambar 4.1. Arsitektur Jaringan Komputer (Sumber: slideegg.com)

Komponen Dasar dalam Jaringan Komputer

1. **Perangkat Penghantar (*End Devices*)**
   Perangkat penghantar adalah perangkat yang digunakan oleh pengguna untuk mengakses jaringan, seperti komputer, laptop, smartphone, dan perangkat lainnya. Perangkat penghantar ini dapat berfungsi sebagai sumber atau tujuan data dalam komunikasi jaringan. Misalnya, komputer klien yang mengirimkan permintaan ke server untuk mendapatkan data atau file, atau perangkat penyimpanan yang berbagi file di dalam jaringan local (Jain and Daniyal, 2022).
2. **Perangkat Penghubung (*Networking Devices*)**
   Perangkat penghubung berfungsi untuk mengatur dan menghubungkan perangkat-perangkat dalam jaringan. Beberapa perangkat penghubung yang umum digunakan dalam jaringan komputer adalah:
   a. **Hub**: Merupakan perangkat yang menghubungkan beberapa perangkat dalam satu jaringan, tetapi tidak mengelola lalu lintas data dengan efisien. Semua data yang dikirimkan ke hub akan disebarkan ke semua perangkat yang terhubung (Wu and Irwin, 2016).
   b. **Switch**: Switch lebih efisien dibandingkan hub, karena hanya mengirimkan data ke perangkat yang dituju berdasarkan alamat MAC (*Media Access Control*), sehingga mengurangi kemacetan dalam jaringan (Jain and Daniyal, 2022).
   c. **Router**: Router digunakan untuk menghubungkan beberapa jaringan, baik jaringan lokal (LAN) dengan jaringan yang lebih luas (WAN) atau menghubungkan jaringan ke internet. Router berfungsi untuk menentukan jalur terbaik bagi data untuk sampai ke tujuan berdasarkan alamat IP (Tran, Nguyen and Thai, 2024).
   d. **Gateway**: Gateway digunakan untuk menghubungkan dua jaringan yang berbeda yang menggunakan protokol yang berbeda pula.

3. **Media Transmisi**
   Media transmisi adalah saluran fisik yang digunakan untuk mengirimkan data dalam jaringan. Ada beberapa jenis media transmisi, termasuk kabel tembaga (seperti twisted pair dan coaxial), kabel serat optik (fiber optic), dan media nirkabel (seperti Wi-Fi dan Bluetooth) (Hofmann and Kasseckert, 2020).
4. **Protokol Jaringan**
   Protokol jaringan adalah aturan dan standar yang digunakan untuk mengatur komunikasi antara perangkat dalam jaringan. Protokol ini mengatur berbagai aspek komunikasi, mulai dari bagaimana data dikemas, dikirim, hingga diterima oleh perangkat yang lain (Fuchs, 2008; Kuzlu and Popescu, 2020). Beberapa protokol yang paling umum digunakan adalah TCP/IP, yaitu protokol utama yang digunakan untuk komunikasi data di internet, HTTP , dan FTP

Jenis-Jenis Jaringan Komputer

Beberapa jenis jaringan komputer yang dibedakan berdasarkan ukuran dan area geografisnya antara lain:

1. **LAN (*Local Area Network*)**
   LAN adalah jaringan komputer yang terbatas pada area geografis yang kecil, seperti dalam satu gedung atau kampus (Page, 2005). LAN memungkinkan perangkat-perangkat di dalamnya untuk berbagi data dan sumber daya, seperti printer atau server file, dengan kecepatan tinggi.
2. **WAN (*Wide Area Network*)**
   WAN merupakan jaringan yang mencakup area geografis yang lebih luas, seperti antar kota atau negara. WAN menghubungkan beberapa LAN yang terpisah dan memungkinkan komunikasi data jarak jauh. Internet adalah contoh dari WAN terbesar di dunia (Page, 2005).
3. **MAN (*Metropolitan Area Network*)**
   MAN adalah jaringan yang lebih besar dari LAN tetapi lebih kecil dari WAN, mencakup area yang lebih luas, seperti beberapa gedung atau kampus dalam satu kota atau wilayah metropolitan.

4. **PAN (*Personal Area Network*)**
   PAN adalah jaringan yang sangat terbatas, biasanya digunakan untuk menghubungkan perangkat pribadi dalam jarak dekat, seperti antara ponsel dan perangkat wearable atau headset Bluetooth.

Fungsi Utama Jaringan Komputer

1. **Berbagi Sumber Daya**
   Salah satu fungsi utama dari jaringan komputer adalah memungkinkan perangkat untuk berbagi sumber daya. Misalnya, pengguna di dalam jaringan dapat berbagi printer, hard disk, atau aplikasi tanpa perlu memiliki perangkat masing-masing.
2. **Komunikasi**
   Jaringan komputer memungkinkan perangkat untuk saling berkomunikasi. Misalnya, dalam dunia bisnis, karyawan dapat saling mengirimkan email, melakukan video konferensi, atau berbagi file.
3. **Pengamanan dan Pemulihan**
   Pengamanan data sangat penting dalam jaringan komputer, terutama karena data yang dikirimkan melalui jaringan bisa rentan terhadap serangan atau kehilangan. Oleh karena itu, jaringan modern dilengkapi dengan berbagai mekanisme keamanan, seperti enkripsi data, firewall, dan sistem deteksi intrusi.
4. **Pengelolaan Terpusat**
   Dalam jaringan, pengelolaan perangkat dan sumber daya bisa dilakukan secara terpusat. Administrator jaringan dapat mengelola akses pengguna, memonitor kinerja, dan memastikan ketersediaan sumber daya dengan lebih mudah melalui server pusat.

Jaringan komputer telah menjadi bagian tak terpisahkan dari kehidupan modern. Dengan adanya jaringan, orang dapat berkomunikasi dengan mudah, mengakses informasi kapan saja dan di mana saja, serta berbagi sumber daya dengan lebih efisien. Dalam dunia bisnis, jaringan memungkinkan perusahaan untuk

menghubungkan kantor cabang yang terpisah, meningkatkan efisiensi, dan mendukung kerja sama tim yang lebih baik.

4.2 Topologi Jaringan

Topologi jaringan adalah cara perangkat-perangkat dalam jaringan saling terhubung satu sama lain. Topologi ini mendefinisikan struktur atau desain fisik serta logis dari jaringan. Pemilihan topologi yang tepat sangat penting karena akan memengaruhi kinerja, pemeliharaan, serta biaya dari jaringan itu sendiri.

Jenis-Jenis Topologi Jaringan

1. **Topologi Bus**

   Topologi bus adalah jenis topologi jaringan yang paling sederhana. Pada topologi ini, semua perangkat dalam jaringan terhubung ke satu kabel utama yang disebut backbone atau bus. Data yang dikirim oleh perangkat di dalam jaringan akan ditransmisikan melalui bus dan diterima oleh semua perangkat yang terhubung. Namun, hanya perangkat yang dituju yang akan memproses data tersebut, sementara perangkat lainnya akan mengabaikan paket data tersebut.

   a. **Keuntungan**:
      1) Mudah dipasang dan lebih murah dibandingkan dengan topologi lainnya.
      2) Penggunaan kabel yang efisien karena hanya memerlukan satu kabel utama.

   b. **Kekurangan**:
      1) Jika kabel utama (*backbone*) rusak, seluruh jaringan akan terputus.
      2) Dapat mengalami kemacetan atau degradasi kinerja ketika jumlah perangkat dalam jaringan bertambah banyak.

2. **Topologi Star**

   Pada topologi star, semua perangkat dalam jaringan terhubung ke perangkat pusat yang disebut switch atau hub. Perangkat ini berfungsi sebagai pengatur lalu lintas data antar perangkat. Data yang dikirim oleh perangkat satu akan diteruskan oleh switch atau hub ke perangkat tujuan. Topologi star sangat populer di

lingkungan kantor dan kampus karena kemudahan pengelolaan dan pemeliharaan.

a. **Keuntungan**:
    1) Jika satu perangkat atau kabel gagal, hanya perangkat tersebut yang akan terpengaruh, bukan seluruh jaringan.
    2) Pengelolaan lalu lintas data lebih mudah karena perangkat pusat mengontrol data yang dikirim.
    3) Skalabilitas lebih baik, karena perangkat baru dapat ditambahkan dengan mudah.
b. **Kekurangan**:
    1) Jika perangkat pusat (seperti switch atau hub) gagal, seluruh jaringan akan terputus.
    2) Memerlukan lebih banyak kabel untuk menghubungkan setiap perangkat ke pusat.

3. **Topologi Ring**

Pada topologi ring, setiap perangkat dalam jaringan terhubung dengan perangkat lainnya dalam bentuk cincin. Data bergerak dalam satu arah atau dua arah melalui jaringan, mengelilingi cincin hingga sampai ke perangkat yang dituju. Setiap perangkat dalam topologi ini bertindak sebagai pengulang untuk data yang melintasi jaringan.

a. **Keuntungan**:
    1) Dapat mengelola lalu lintas data secara lebih terorganisir, terutama dalam jaringan yang memiliki trafik tinggi.
    2) Tidak ada kolisi data, karena data bergerak dalam satu arah (untuk topologi ring satu arah).
b. **Kekurangan**:
    1) Jika satu perangkat atau kabel gagal, seluruh jaringan akan terputus.
    2) Pengelolaan dan pemeliharaan jaringan bisa lebih sulit dibandingkan dengan topologi lainnya.

4. **Topologi Mesh**

Pada topologi mesh, setiap perangkat dalam jaringan terhubung langsung ke semua perangkat lainnya. Ini menciptakan redundansi yang sangat tinggi, karena data dapat mengambil

jalur alternatif jika salah satu jalur gagal. Topologi mesh sering digunakan pada jaringan yang memerlukan tingkat keandalan yang sangat tinggi, seperti pada jaringan telekomunikasi atau pusat data.

a. Keuntungan:

1) Keandalan yang sangat tinggi karena ada banyak jalur alternatif untuk data.
2) Jika satu jalur atau perangkat gagal, data masih dapat dikirim melalui jalur lain.

b. Kekurangan:

1) Memerlukan kabel yang sangat banyak dan konfigurasi yang lebih kompleks.
2) Biaya instalasi dan pemeliharaan sangat tinggi karena banyaknya koneksi yang diperlukan.

5. Topologi Hybrid

Topologi hybrid merupakan gabungan dari dua atau lebih topologi jaringan yang berbeda, yang digabungkan untuk mengatasi kekurangan dari masing-masing topologi. Misalnya, sebuah jaringan dapat menggabungkan topologi star dan bus untuk menghubungkan beberapa area dalam jaringan besar. Keuntungan dari topologi hybrid adalah fleksibilitasnya untuk memenuhi kebutuhan spesifik jaringan.

a. Keuntungan:

1) Fleksibel dan dapat disesuaikan dengan kebutuhan jaringan yang lebih kompleks.
2) Dapat menggabungkan keunggulan berbagai topologi.

b. Kekurangan:

1) Desain dan implementasi lebih rumit.
2) Biaya dapat lebih tinggi dibandingkan dengan menggunakan satu jenis topologi.

Pemilihan topologi jaringan yang tepat bergantung pada beberapa faktor, seperti ukuran jaringan, anggaran, kebutuhan kinerja, dan tingkat keandalan yang dibutuhkan. Misalnya, dalam lingkungan kecil dengan anggaran terbatas, topologi bus atau star mungkin lebih cocok, sementara dalam jaringan besar yang

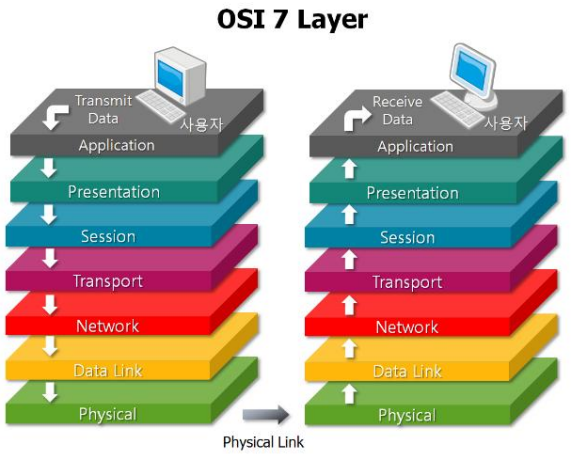
membutuhkan redundansi tinggi, topologi mesh atau hybrid lebih sesuai.

4.3 Model Referensi OSI dan TCP/IP

Model referensi OSI (*Open Systems Interconnection*) dan TCP/IP (*Transmission Control Protocol/Internet Protocol*) adalah dua model yang digunakan untuk menggambarkan bagaimana perangkat-perangkat dalam jaringan berkomunikasi satu sama lain (Kuzlu and Popescu, 2020). Kedua model ini memberikan struktur yang jelas tentang bagaimana data dikirim, diterima, dan diproses dalam jaringan komputer. Meskipun keduanya memiliki tujuan yang sama, yaitu untuk memfasilitasi komunikasi antar sistem, ada perbedaan dalam jumlah lapisan serta cara mereka mendekati masalah komunikasi.

Model OSI (*Open Systems Interconnection*)

Model OSI adalah model referensi jaringan yang paling terkenal dan terdiri dari tujuh lapisan, masing-masing dengan fungsi yang spesifik. Model ini dikembangkan oleh *International Organization for Standardization* (ISO) untuk memberikan standar yang jelas tentang cara perangkat keras dan perangkat lunak jaringan berinteraksi. Model OSI membagi proses komunikasi menjadi tujuh lapisan, yang diurutkan dari lapisan fisik hingga aplikasi.



Gambar 4.2. OSI Layer (Sumber : blogspot.com)

Lapisan-lapisan OSI:

1. **Lapisan Fisik (*Physical Layer*)**
   Lapisan fisik adalah lapisan terendah dalam model OSI yang bertanggung jawab untuk transmisi data secara fisik melalui media transmisi. Ini mencakup segala hal yang berkaitan dengan perangkat keras seperti kabel, konektor, dan sinyal yang digunakan untuk mentransmisikan data. Lapisan ini juga mengatur kecepatan transmisi dan pengkodean sinyal.
   Contoh: Kabel Ethernet, fiber optic, sinyal nirkabel, serta perangkat keras lainnya yang digunakan untuk pengiriman data.
2. **Lapisan Data Link (*Data Link Layer*)**
   Lapisan data link bertanggung jawab untuk menyediakan pengalamatan perangkat dalam jaringan lokal dan untuk memastikan bahwa data dapat ditransmisikan tanpa kesalahan. Lapisan ini mengatur pengalamatan perangkat dengan alamat MAC (*Media Access Control*), serta menangani pengendalian aliran dan deteksi kesalahan.
   Contoh: Switch, bridge, dan protokol Ethernet.
3. **Lapisan Jaringan (*Network Layer*)**
   Lapisan ini bertanggung jawab untuk pengalamatan logis dan routing data antar jaringan. Lapisan jaringan memastikan data dapat dikirimkan dari perangkat asal ke perangkat tujuan meskipun perangkat tersebut terhubung melalui berbagai jaringan yang berbeda. Pengalamatan IP (*Internet Protocol*) adalah bagian dari lapisan ini.
   Contoh: Router dan protokol IP (IPv4 dan IPv6).
4. **Lapisan Transportasi (*Transport Layer*)**
   Lapisan transportasi bertanggung jawab untuk mengatur komunikasi antar sistem di dua perangkat yang berbeda. Lapisan ini mengatur bagaimana data dibagi menjadi segmen, serta menyediakan pengendalian aliran dan pengendalian kesalahan. Dua protokol utama yang bekerja pada lapisan ini adalah TCP (*Transmission Control Protocol*) dan UDP (*User Datagram Protocol*).
   Contoh: Protokol TCP, UDP.

5. **Lapisan Sesi (*Session Layer*)**
   Lapisan sesi mengatur komunikasi antar aplikasi yang berjalan di dua perangkat berbeda. Lapisan ini menyediakan mekanisme untuk membuka, mengelola, dan menutup sesi komunikasi. Selain itu, lapisan sesi juga mengatur sinkronisasi data antar perangkat yang terhubung.
   Contoh: Protokol SMB (Server Message Block), NetBIOS.
6. **Lapisan Presentasi (*Presentation Layer*)**
   Lapisan presentasi bertanggung jawab untuk penerjemahan, pengkodean, dan kompresi data agar dapat dipahami oleh aplikasi yang menerima data tersebut. Lapisan ini memastikan bahwa data yang dikirimkan dalam bentuk yang dapat diproses oleh perangkat tujuan, baik itu dalam format teks, gambar, atau suara.
   Contoh: Protokol SSL/TLS (untuk enkripsi), JPEG (untuk pengkodean gambar).
7. **Lapisan Aplikasi (*Application Layer*)**
   Lapisan aplikasi adalah lapisan tertinggi dalam model OSI yang menyediakan layanan jaringan langsung kepada aplikasi pengguna. Lapisan ini berfungsi sebagai antarmuka antara aplikasi pengguna dan jaringan. Berbagai protokol aplikasi seperti HTTP, FTP, SMTP, dan DNS beroperasi di lapisan ini.
   Contoh: Protokol HTTP (untuk web), FTP (untuk transfer file), SMTP (untuk email).

Model TCP/IP (*Transmission Control Protocol / Internet Protocol*)

Model TCP/IP adalah model referensi yang lebih sederhana dan lebih praktikal dibandingkan dengan OSI. Model ini dikembangkan oleh Departemen Pertahanan Amerika Serikat pada tahun 1970-an untuk memastikan komunikasi antara perangkat dalam jaringan komputer yang berbeda dapat berjalan lancar. TCP/IP terdiri dari empat lapisan yang lebih luas, yang berfungsi untuk menyederhanakan proses komunikasi di internet dan jaringan komputer lainnya.

Lapisan-lapisan TCP/IP:

1. **Lapisan Akses Jaringan (*Network Access Layer*)**
   Lapisan ini mencakup fungsi yang setara dengan lapisan fisik dan data link pada model OSI. Lapisan akses jaringan bertanggung jawab untuk pengiriman data secara fisik melalui media transmisi dan pengalamatan perangkat dalam jaringan lokal.
   Contoh: Ethernet, Wi-Fi, frame relay.
2. **Lapisan Internet (*Internet Layer*)**
   Lapisan ini setara dengan lapisan jaringan pada model OSI. Fungsi utamanya adalah pengalamatan dan routing data antara perangkat yang terhubung melalui berbagai jaringan. Protokol utama di lapisan ini adalah IP (*Internet Protocol*), yang bertanggung jawab untuk pengalamatan dan pengiriman paket data.
   Contoh: Protokol IP (IPv4, IPv6), router.
3. **Lapisan Transportasi (*Transport Layer*)**
   Seperti pada model OSI, lapisan transportasi pada TCP/IP bertanggung jawab untuk memastikan data dikirimkan dengan benar antar perangkat yang terhubung. Protokol TCP dan UDP bekerja pada lapisan ini. TCP memastikan pengiriman data yang andal dan dalam urutan yang benar, sementara UDP digunakan untuk aplikasi yang membutuhkan kecepatan lebih tinggi meskipun dengan risiko kehilangan data.
   Contoh: Protokol TCP, UDP.
4. **Lapisan Aplikasi (*Application Layer*)**
   Lapisan aplikasi dalam TCP/IP bertanggung jawab untuk menyediakan layanan jaringan yang langsung berinteraksi dengan aplikasi pengguna. Protokol yang beroperasi pada lapisan ini digunakan oleh aplikasi seperti web, email, dan transfer file.
   Contoh: HTTP, FTP, SMTP, DNS.

Perbandingan Model OSI dan TCP/IP

Meskipun model OSI dan TCP/IP memiliki tujuan yang sama, yaitu untuk memfasilitasi komunikasi data antar perangkat dalam jaringan, ada beberapa perbedaan yang perlu dipahami:

1. **Jumlah Lapisan**
   OSI memiliki tujuh lapisan, sementara TCP/IP hanya memiliki empat lapisan. Hal ini membuat TCP/IP lebih sederhana dan lebih praktikal untuk implementasi dalam dunia nyata.
2. **Pendekatan Top-Down vs. Bottom-Up**
   OSI dikembangkan dengan pendekatan top-down, dimana tiap lapisan dimaksudkan untuk melakukan fungsi spesifik yang terpisah, sementara TCP/IP lebih fokus pada implementasi praktis dan memiliki lebih sedikit lapisan.
3. **Kepopuleran dan Penerapan**
   TCP/IP adalah model yang lebih banyak diterapkan dalam dunia nyata, terutama karena ia merupakan dasar dari internet. Sebagian besar protokol yang digunakan dalam komunikasi internet seperti HTTP, FTP, dan IP beroperasi berdasarkan model TCP/IP. Sedangkan OSI lebih sering digunakan untuk tujuan pendidikan dan sebagai acuan untuk pemahaman dasar mengenai bagaimana jaringan bekerja.

Model OSI dan TCP/IP keduanya sangat penting dalam memahami cara kerja komunikasi data dalam jaringan. Meskipun model OSI memberikan kerangka yang lebih rinci dan terstruktur, model TCP/IP lebih praktikal dan banyak digunakan dalam implementasi jaringan yang sebenarnya.

4.4 Media Transmisi dalam Jaringan

Media transmisi adalah saluran fisik atau logis yang digunakan untuk mentransfer data antar perangkat dalam jaringan komputer. Media ini berfungsi sebagai penghubung untuk mentransmisikan sinyal data dari satu perangkat ke perangkat lainnya. Pemilihan media transmisi yang tepat sangat krusial dalam merancang jaringan yang efisien, karena jenis media yang digunakan akan memengaruhi kecepatan, kualitas, dan keandalan komunikasi data.

Terdapat dua kategori utama media transmisi dalam jaringan komputer: media transmisi kabel dan media transmisi nirkabel. Setiap jenis media memiliki karakteristik, kelebihan, dan kekurangan

yang harus dipertimbangkan sesuai dengan kebutuhan spesifik jaringan.

Media Transmisi Kabel

1. **Kabel Tembaga (*Copper Cable*)**

   Kabel tembaga merupakan salah satu media transmisi yang paling banyak digunakan dalam jaringan komputer. Dua jenis kabel tembaga yang paling sering digunakan adalah Twisted Pair dan Coaxial Cable.

   a. Twisted Pair* (TP) *Cable

   Kabel twisted pair terdiri dari dua buah kawat tembaga yang dipilin bersama membentuk pasangan. Ada dua jenis twisted pair yang umum digunakan dalam jaringan:

   1) ***Unshielded Twisted Pair* (UTP)** adalah jenis kabel yang umum digunakan dalam jaringan Ethernet. Kabel ini terdiri dari empat pasangan kawat yang dipilin bersama tanpa pelindung tambahan. UTP tersedia dalam berbagai kategori, seperti Cat 5e, Cat 6, dan Cat 6a, yang masing-masing menawarkan kecepatan dan jangkauan yang berbeda.
   2) **Shielded Twisted Pair (STP)**: STP memiliki pelindung tambahan yang mengurangi interferensi elektromagnetik (EMI), sehingga lebih tahan terhadap gangguan sinyal dibandingkan dengan UTP.
   3) **Keuntungan**:
      a) Relatif murah dan mudah dipasang.
      b) UTP banyak digunakan dalam jaringan LAN karena harganya yang terjangkau dan kecepatan yang memadai untuk sebagian besar aplikasi.
   4) **Kekurangan**:
      a) Rentan terhadap gangguan elektromagnetik (EMI), terutama pada jarak yang lebih jauh.
      b) Jangkauan terbatas untuk transmisi data dalam kecepatan tinggi.

   b. Coaxial Cable

   Coaxial cable atau kabel koaksial adalah kabel tembaga yang memiliki lapisan pelindung logam di sekitarnya, yang

berfungsi untuk melindungi sinyal dari interferensi eksternal.

1) **Keuntungan**:
   a) Lebih tahan terhadap interferensi dibandingkan dengan twisted pair.
   b) Memiliki bandwidth yang lebih tinggi daripada twisted pair.
2) **Kekurangan**:
   a) Cenderung lebih mahal dan lebih sulit dipasang dibandingkan dengan twisted pair.
   b) Terbatas pada jarak transmisi dan dapat mempengaruhi kualitas sinyal pada panjang kabel yang lebih jauh.

2. Kabel Serat Optik (*Fiber Optic Cable*)

Kabel serat optik adalah media transmisi yang memanfaatkan cahaya untuk mentransfer data melalui serat kaca atau plastik. Kabel ini terdiri dari serat optik yang dilindungi oleh lapisan pelindung. Data dikirim dalam bentuk pulsa cahaya melalui serat optik, memungkinkan transmisi dengan kecepatan tinggi dan jarak yang sangat jauh.

Gambar 4.3. Kabel Serat Optik (Sumber: rfindustries.com)

a. Keuntungan:

1) Kecepatan tinggi dan bandwidth sangat besar.
2) Tidak rentan terhadap interferensi elektromagnetik karena sinyal dikirimkan dalam bentuk cahaya.

3) Jarak transmisi yang jauh tanpa kehilangan sinyal yang signifikan.
4) Keamanan lebih baik, karena sulit untuk mengakses sinyal dalam kabel serat optik tanpa merusak kabel.

b. Kekurangan:

1) Biaya instalasi dan perawatan yang lebih tinggi.
2) Instalasi kabel serat optik lebih rumit dan memerlukan peralatan khusus untuk pemotongan dan penyambungan kabel.

Kabel serat optik sangat cocok digunakan untuk jaringan yang memerlukan kecepatan tinggi dan jangkauan jauh, seperti jaringan backbone antar gedung atau komunikasi antar kota.

Media Transmisi Nirkabel

Media transmisi nirkabel menggunakan gelombang radio, mikro, atau sinyal inframerah untuk mentransmisikan data tanpa memerlukan kabel fisik. Jenis media ini sangat populer dalam jaringan LAN dan WAN karena kemudahan instalasi dan fleksibilitasnya.

1. Wi-Fi (*Wireless Fidelity*)

Wi-Fi adalah teknologi nirkabel yang populer untuk menghubungkan perangkat dalam jaringan lokal (LAN). Teknologi ini memanfaatkan gelombang radio untuk mentransfer data antara perangkat dan *access point* (AP).

a. Keuntungan:

1) Instalasi yang lebih cepat dan fleksibel karena tidak memerlukan kabel fisik.
2) Memungkinkan koneksi mobile pada perangkat seperti laptop, smartphone, dan perangkat IoT.

b. Kekurangan:

1) Rentan terhadap interferensi elektromagnetik (EMI) dan gangguan dari perangkat lain yang menggunakan frekuensi yang sama.
2) Jangkauan terbatas dan dapat dipengaruhi oleh hambatan fisik seperti dinding atau objek besar.

Wi-Fi banyak digunakan di rumah, kantor, dan tempat umum untuk menyediakan koneksi internet nirkabel bagi berbagai perangkat.

2. **Bluetooth**
   Bluetooth merupakan teknologi nirkabel untuk komunikasi jarak dekat yang memungkinkan perangkat, seperti smartphone, headset, dan perangkat wearable, untuk saling terhubung dalam jangkauan yang terbatas.
   a. **Keuntungan**:
      1) Hemat energi dan dapat digunakan untuk komunikasi antar perangkat pribadi (PAN).
      2) Ideal untuk komunikasi jarak dekat antara perangkat seperti smartphone dan headset, speaker, atau keyboard.
   b. **Kekurangan**:
      1) Jangkauan terbatas, biasanya hanya beberapa meter.
      2) Kecepatan transfer data lebih rendah dibandingkan dengan Wi-Fi atau kabel tembaga.
3. **Gelombang Mikro (*Microwave*) dan Satelit**
   Media transmisi gelombang mikro digunakan untuk komunikasi jarak jauh, seperti komunikasi antara dua lokasi yang terpisah oleh jarak jauh. Gelombang mikro dapat mentransmisikan data dalam frekuensi yang lebih tinggi dibandingkan dengan radio.
   a. **Keuntungan**:
      1) Dapat digunakan untuk komunikasi antara lokasi yang jauh tanpa membutuhkan kabel fisik.
      2) Ideal untuk jaringan WAN yang menghubungkan beberapa lokasi yang terpisah jauh.
   b. **Kekurangan**:
      1) Rentan terhadap gangguan cuaca seperti hujan atau badai yang dapat mempengaruhi kualitas sinyal.
      2) Memerlukan jalur pandang langsung (line of sight) antara pengirim dan penerima, yang dapat membatasi penerapannya di beberapa kondisi geografis.

Pemilihan media transmisi yang tepat sangat bergantung pada berbagai faktor, seperti kebutuhan kecepatan, jarak transmisi,

anggaran, dan tingkat gangguan yang diharapkan dalam lingkungan jaringan. Untuk jaringan lokal (LAN), kabel tembaga (terutama twisted pair) sering kali cukup efektif dan murah. Namun, untuk jaringan yang memerlukan kecepatan tinggi dan jarak jauh, kabel serat optik adalah pilihan terbaik. Sementara itu, media transmisi nirkabel seperti Wi-Fi sangat berguna untuk fleksibilitas dan konektivitas perangkat mobile, meskipun terbatas dalam hal jangkauan dan kecepatan transfer data.

4.5 Protokol Jaringan

Protokol jaringan merujuk pada sekumpulan pedoman atau spesifikasi yang dirancang untuk mengatur interaksi antara perangkat dalam jaringan komputer. Protokol ini menjamin bahwa data dikirim, diterima, dan diproses secara akurat dan optimal. Setiap protokol jaringan beroperasi pada berbagai lapisan model OSI dan TCP/IP, dengan setiap lapisan memiliki peran tertentu dalam pengelolaan aliran data dan pemrosesan informasi.

Jenis-Jenis Protokol Jaringan

1. **Protokol Internet (IP)**
   Protokol Internet (IP) adalah salah satu protokol paling fundamental dalam jaringan komputer. IP bertanggung jawab untuk pengalamatan dan routing paket data antara perangkat yang terhubung melalui jaringan. Protokol ini menentukan cara data dibungkus menjadi paket dan dikirimkan ke alamat tujuan. Ada dua versi utama dari protokol IP: IPv4 dan IPv6.
   a. **IPv4 (*Internet Protocol Version* 4)**
      Internet Protocol version 4 (IPv4) adalah protokol jaringan yang paling luas digunakan hingga saat ini. IPv4 mengandalkan sistem pengalamatan 32-bit, yang menghasilkan sekitar 4,3 miliar alamat IP unik. Meski awalnya dianggap mencukupi, pertumbuhan eksponensial perangkat yang terhubung ke internet menyebabkan keterbatasan ketersediaan alamat, sehingga mendorong pengembangan dan adopsi IPv6 sebagai solusi jangka panjang.

b. IPv6 (*Internet Protocol Version* 6)

Internet Protocol version 6 (IPv6) merupakan generasi lanjutan dari protokol IP yang dikembangkan untuk mengatasi keterbatasan ruang alamat pada IPv4. Dengan panjang alamat 128-bit, IPv6 menyediakan ruang alamat yang sangat luas, mendukung sekitar 3.4×10^{38} alamat unik. Selain kapasitasnya yang besar, IPv6 juga membawa peningkatan efisiensi routing, dukungan autokonfigurasi (stateless address autoconfiguration), dan keamanan yang lebih baik melalui integrasi IPsec.

2. *Transmission Control Protocol* (TCP)

Transmission Control Protocol (TCP) adalah protokol komunikasi pada Layer 4 (Transport Layer) dalam model TCP/IP yang menyediakan layanan pengiriman data yang andal dan berurutan. TCP menggunakan mekanisme three-way handshake untuk membentuk koneksi, serta menerapkan kontrol kesalahan, pengurutan paket, dan retransmisi terhadap data yang hilang atau korup, guna memastikan integritas dan keakuratan pengiriman antar host dalam jaringan.

a. Keandalan: TCP memastikan pengiriman data yang andal melalui penggunaan mekanisme verifikasi, urutan data, dan pengendalian aliran.

b. Segmentasi: TCP membagi data yang lebih besar menjadi segmen-segmen yang lebih kecil untuk menghindari pengiriman data dalam ukuran yang terlalu besar, yang dapat mengakibatkan masalah di jaringan.

c. Contoh Penggunaan: TCP digunakan dalam aplikasi yang membutuhkan keandalan tinggi, seperti pengiriman email (SMTP), transfer file (FTP), dan browsing web (HTTP).

Contoh: Ketika Anda mengakses situs web, browser Anda menggunakan TCP untuk memastikan data halaman web yang Anda lihat sampai ke perangkat Anda dengan benar dan dalam urutan yang benar.

3. *User Datagram Protocol* (UDP)

User Datagram Protocol (UDP) merupakan protokol Layer 4 (*Transport Layer*) dalam model OSI yang menyediakan komunikasi tanpa koneksi (*connectionless*) dan tanpa jaminan

reliabilitas. Tidak seperti TCP, UDP tidak melakukan mekanisme pengendalian aliran, pengurutan, atau retransmisi data yang hilang, sehingga cocok digunakan pada aplikasi real-time seperti streaming audio/video atau layanan DNS, di mana latensi rendah lebih diutamakan dibanding keakuratan pengiriman.

Contoh Penggunaan: Dalam konferensi video atau streaming langsung, seperti YouTube atau Skype, UDP digunakan untuk mengirimkan data secara cepat, meskipun beberapa paket data mungkin hilang di jalan.

4. ***Hypertext Transfer Protocol*** **(HTTP) dan HTTPS**

   HTTP adalah protokol aplikasi yang digunakan untuk mengakses dan mentransfer halaman web melalui internet. HTTP bekerja di lapisan aplikasi pada model OSI dan menggunakan TCP sebagai protokol transportasi. HTTPS adalah versi aman dari HTTP yang mengenkripsi data yang dikirimkan untuk melindungi informasi sensitif.

   Contoh Penggunaan: Ketika Anda mengakses sebuah website, browser Anda menggunakan HTTP atau HTTPS untuk mengirimkan permintaan ke server dan menerima respons berupa halaman web.

5. ***File Transfer Protocol*** **(FTP)**

   FTP adalah protokol aplikasi yang digunakan untuk mentransfer file antar perangkat dalam jaringan. FTP memungkinkan pengguna untuk mengunduh dan mengunggah file dari server atau antara perangkat di jaringan lokal.

   FTP digunakan untuk mengelola file di server web, mengunduh file dari situs web, dan mengunggah file ke server.

6. ***Domain Name System*** **(DNS)**

   DNS adalah protokol aplikasi yang berfungsi untuk menerjemahkan nama domain yang mudah diingat (seperti www.google.com) menjadi alamat IP numerik yang digunakan untuk mengidentifikasi perangkat di jaringan. DNS bekerja di lapisan aplikasi dan sangat penting dalam penggunaan internet sehari-hari.

   Ketika Anda mengetik alamat website di browser, DNS akan menerjemahkan nama domain menjadi alamat IP yang dapat dipahami oleh perangkat jaringan.

Contohnya ketika Anda mengunjungi situs web, seperti www.amazon.com, DNS menerjemahkan nama domain tersebut ke dalam alamat IP server Amazon untuk memuat halaman web.

7. ***Address Resolution Protocol* (ARP)**
   ARP adalah protokol yang digunakan untuk memetakan alamat IP ke alamat MAC (*Media Access Control*) yang digunakan di lapisan data link. ARP memungkinkan perangkat dalam jaringan lokal untuk mengetahui alamat fisik perangkat lain berdasarkan alamat IP.
   Ketika perangkat ingin mengirimkan data ke perangkat lain di jaringan yang sama, ARP digunakan untuk mencari tahu alamat MAC dari alamat IP yang diberikan.
8. **Simple Mail Transfer Protocol (SMTP)**
   SMTP adalah protokol aplikasi yang digunakan untuk mengirimkan email antar server. SMTP bekerja di lapisan aplikasi dan menggunakan TCP untuk komunikasi antar server email. Protokol ini memungkinkan pengiriman email dari pengirim ke server email penerima.

4.6 Perangkat Jaringan Dasar

Perangkat jaringan adalah komponen penting yang memungkinkan berbagai perangkat dalam jaringan untuk saling berkomunikasi dan berbagi data. Tanpa perangkat jaringan yang tepat, jaringan komputer tidak akan berfungsi dengan baik.

1. **Hub**
   Hub adalah perangkat jaringan yang beroperasi pada Layer 1 (*Physical Layer*) dalam model OSI dan digunakan sebagai titik koneksi untuk mengintegrasikan beberapa perangkat dalam satu jaringan lokal (LAN). Perangkat ini mentransmisikan sinyal yang diterima ke semua port tanpa memproses atau menyaring data, sehingga semua perangkat yang terhubung menerima informasi yang sama, yang dapat menyebabkan collision jika lalu lintas tinggi.
   Hub menerima data dari satu perangkat dan mendistribusikannya ke semua perangkat yang terhubung ke dalam jaringan, tanpa mempedulikan perangkat mana yang seharusnya menerima data tersebut. Ini dapat menyebabkan

kemacetan dalam jaringan, karena data dikirim ke setiap perangkat, meskipun hanya satu perangkat yang memerlukannya.

Hub umumnya digunakan dalam jaringan kecil atau jaringan dengan beban lalu lintas rendah, meskipun saat ini hub mulai digantikan oleh switch yang lebih efisien.

2. Switch

Switch merupakan perangkat jaringan Layer 2 dalam model OSI yang berfungsi sebagai pengontrol lalu lintas data antar perangkat dalam satu segmen jaringan lokal. Berbeda dengan hub, switch mampu melakukan pengalihan frame secara selektif ke port tujuan berdasarkan tabel MAC address yang dibangunnya, sehingga meningkatkan efisiensi dan mengurangi collision dalam jaringan.

Switch mempelajari alamat MAC perangkat yang terhubung ke dalam port-portnya dan membuat tabel yang berisi informasi mengenai perangkat-perangkat tersebut. Ketika data diterima, switch akan memeriksa alamat MAC tujuan dan mengirimkan data hanya ke perangkat yang sesuai, bukan ke semua perangkat dalam jaringan. Ini mengurangi kemacetan dan meningkatkan efisiensi jaringan.

Switch digunakan di hampir semua jaringan LAN modern karena efisiensinya dalam mengelola lalu lintas data.

3. Router

Router adalah perangkat jaringan Layer 3 (Network Layer) dalam model OSI yang bertugas mengarahkan paket data antar jaringan yang memiliki skema alamat IP berbeda, seperti menghubungkan LAN dengan WAN atau antar beberapa LAN yang terpisah. Router menentukan jalur terbaik untuk pengiriman data menggunakan protokol routing, sehingga memungkinkan komunikasi lintas jaringan secara efisien.

Router bekerja di lapisan jaringan (Layer 3) dalam model OSI dan berperan dalam pengiriman data antar jaringan menggunakan alamat IP.

Router menerima data dari satu jaringan dan memutuskan rute terbaik untuk mengirimkan data ke tujuan menggunakan protokol routing (seperti RIP, OSPF, atau EIGRP). Router

menggunakan tabel routing untuk menentukan jalur yang optimal berdasarkan alamat IP tujuan.

4. **Bridge**

   Bridge merupakan perangkat Layer 2 dalam arsitektur OSI yang digunakan untuk menghubungkan dua segmen jaringan lokal (LAN) yang berbeda, sehingga perangkat di masing-masing segmen dapat berkomunikasi secara transparan. Bridge melakukan forwarding frame berdasarkan alamat MAC dan berfungsi untuk memperluas cakupan jaringan sekaligus mengisolasi lalu lintas guna mengurangi terjadinya collision atau kemacetan lalu lintas data.

   Bridge mempelajari alamat MAC perangkat yang terhubung di kedua sisi jaringan dan kemudian memutuskan apakah data yang diterima dari satu segmen harus diteruskan ke segmen lainnya. Dengan cara ini, bridge mengurangi jumlah perangkat yang terlibat dalam setiap segmen jaringan, mengurangi kemacetan dan meningkatkan efisiensi.

5. **Gateway**

   Gateway adalah perangkat jaringan yang berfungsi sebagai penghubung antara dua jaringan yang berbeda, baik itu dalam hal protokol atau teknologi jaringan. Gateway bekerja di berbagai lapisan OSI, sering kali di lapisan aplikasi (Layer 7), dan digunakan untuk menghubungkan jaringan yang menggunakan protokol yang berbeda.

   Gateway digunakan dalam situasi di mana dua jaringan dengan protokol yang berbeda perlu berkomunikasi, seperti di dalam organisasi besar yang memiliki beberapa sistem atau aplikasi yang menggunakan protokol berbeda.

6. **Modem**

   Modem adalah perangkat komunikasi yang berfungsi sebagai konverter sinyal antara jaringan digital dan saluran transmisi analog, seperti PSTN atau kabel coaxial. Perangkat ini melakukan modulasi terhadap sinyal digital dari host menjadi sinyal analog untuk transmisi, serta demodulasi sinyal analog yang diterima menjadi sinyal digital yang dapat dikenali oleh sistem jaringan lokal. Modem memungkinkan pertukaran data antara perangkat digital dan infrastruktur komunikasi berbasis analog.

DAFTAR PUSTAKA

Fuchs, U. (2008) 'A short introduction to computer networks introduction to computer networks', *NATO Science for Peace and Security Series B: Physics and Biophysics*, pp. 175–188. Available at: https://doi.org/10.1007/978-1-4020-8752-3_10.

Hofmann, S. and Kasseckert, R. (2020) 'Safeguards for the internal communication of IP-based transmission and cross-connect systems', in *Photonische Netze - 12. ITG-Fachtagung*, pp. 216–223. Available at: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85091435901&partnerID=40&md5=e16c09f889add9513011c245c097e1aa.

Jain, A. and Pateriya, R.K. (2019) 'An authentication method based on visual cryptography using lu factorization for cloud environment', *International Journal on Emerging Technologies*, 10(3), pp. 444–453. Available at: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85077680543&partnerID=40&md5=7b58022b593c1331dbb4511646ab0ada.

Jain, S. and Daniyal, M.D. (2022) 'The smart indication model that calculates amount of electromagnetic radiation absorbed by the human body when using a mobile device', in *International Interdisciplinary Humanitarian Conference for Sustainability, IIHC 2022 - Proceedings*, pp. 215–219. Available at: https://doi.org/10.1109/IIHC55949.2022.10060070.

Kuzlu, M. and Popescu, O. (2020) 'Upgrading of a data communication and computer networks course in engineering technology program', in *ASEE Annual Conference and Exposition, Conference Proceedings*. Available at: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85095732273&partnerID=40&md5=38c0fb39c5df306009e5b6708d8f9051.

Mary Jeya Jothi, R. (2015) 'A discussion on SSP structure of pan, helm and crown graphs', *ARPN Journal of Engineering and Applied Sciences*, 10(9), pp. 4115–4121. Available at:

https://www.scopus.com/inward/record.uri?eid=2-s2.0-84930171733&partnerID=40&md5=82901bcec01c585c9153f700a5610580.

Najath, M.N.M., Herath, H.M.D.S. and Rajapakse, A. (2022) 'Design and Testing of an Arduino-based Network Jammer Device', in *7th International Conference on Information Technology Research: Digital Resilience and Reinvention, ICITR 2022 - Proceedings*. Available at: https://doi.org/10.1109/ICITR57877.2022.9993285.

Page, T. (2005) 'Where is the future for networking and data communication technologies?', in *Technical Paper - Society of Manufacturing Engineers*. Available at: https://www.scopus.com/inward/record.uri?eid=2-s2.0-77956433448&partnerID=40&md5=97861a623af3577bce4a5514dfa55dd0.

Tran, N.Q., Nguyen, K.D.L. and Thai, C.D.T. (2024) 'Implementation and Evaluation of IPSec in an NFV-Based Network', in *Lecture Notes in Networks and Systems*, pp. 53–65. Available at: https://doi.org/10.1007/978-981-97-2053-8_4.

Wu, C.-H. and Irwin, J.D. (2016) *Introduction to Computer Networks and Cybersecurity*, *Introduction to Computer Networks and Cybersecurity*. Available at: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85018962814&partnerID=40&md5=727c56e8e92773b21a20b0492a092834.

BAB 5
KONSEP TEKNOLOGI SWITCH

5.1 Pendahuluan

Dalam dunia jaringan komputer, switch adalah perangkat yang sangat penting dalam memastikan efisiensi komunikasi antar perangkat di dalam suatu jaringan. Kehadirannya memungkinkan lalu lintas data mengalir secara optimal, mengurangi terjadinya kolisi, dan memastikan data dikirimkan ke tujuan yang tepat. Namun, sebelum teknologi switch berkembang menjadi salah satu elemen utama dalam jaringan, perangkat lain seperti hub dan bridge mendominasi infrastruktur jaringan, terutama di Local Area Network (LAN).

5.1.1 Sejarah Singkat Perkembangan Switch dalam Jaringan Komputer

Switch berkembang dari teknologi jaringan sederhana seperti hub dan bridge yang digunakan untuk menghubungkan beberapa perangkat dalam sebuah jaringan. Pada awalnya, hub adalah perangkat paling umum dalam jaringan, berfungsi untuk meneruskan sinyal listrik ke semua perangkat yang terhubung tanpa mempertimbangkan alamat tujuan. Hal ini mengakibatkan seringnya terjadi kolisi data, terutama ketika banyak perangkat yang mengirim data secara bersamaan.

Kemudian, hadir bridge, perangkat yang sedikit lebih cerdas daripada hub. Bridge mampu membedakan segmen-segmen jaringan dan mencegah terjadinya kolisi antar segmen. Namun, bridge masih memiliki keterbatasan dalam hal kecepatan dan skalabilitas, karena hanya dapat menangani lalu lintas pada tingkat yang sangat terbatas.

Pada pertengahan 1980-an, switch mulai dikembangkan untuk mengatasi masalah-masalah yang ada pada hub dan bridge. Switch pertama kali diperkenalkan oleh Kalpana pada tahun 1990-an, yang memulai revolusi dalam cara jaringan komputer dirancang dan

dikelola. Switch bekerja pada lapisan data link (layer 2) dari model OSI, tetapi kemudian berkembang hingga mampu beroperasi pada lapisan jaringan (layer 3). Teknologi ini segera menjadi andalan dalam jaringan modern karena kemampuannya untuk mempelajari alamat MAC dan melakukan switching berdasarkan alamat fisik perangkat.

Pada awal perkembangannya, switch hanya digunakan dalam jaringan skala besar dan pusat data, namun seiring dengan penurunan harga dan peningkatan kinerja, switch mulai digunakan secara luas di berbagai lingkungan jaringan, mulai dari rumah hingga perusahaan.

5.1.2 Pentingnya Perangkat Switch dalam Infrastruktur Jaringan Modern

Seiring berkembangnya kebutuhan jaringan komputer, terutama dengan munculnya aplikasi-aplikasi yang memerlukan bandwidth besar seperti video streaming, konferensi video, *cloud computing*, dan *Internet of Things* (IoT), peran switch dalam jaringan menjadi semakin penting. Beberapa alasan penting mengapa switch merupakan komponen esensial dalam infrastruktur jaringan modern adalah:

1. Efisiensi Jaringan: Tidak seperti hub yang hanya meneruskan data ke semua port, switch mampu mempelajari perangkat yang terhubung dan hanya mengirimkan data ke perangkat yang dituju. Ini mengurangi lalu lintas yang tidak perlu dan meningkatkan efisiensi penggunaan bandwidth.
2. Skalabilitas: Switch memungkinkan jaringan berkembang secara fleksibel. Dalam infrastruktur modern, jaringan perusahaan dapat terdiri dari ribuan perangkat yang terhubung, dan switch memungkinkan jaringan tersebut tetap efisien meskipun ukurannya besar.
3. Keamanan: Banyak switch managed yang mendukung fitur keamanan seperti VLAN (*Virtual Local Area Network*), *Access Control Lists* (ACL), dan fitur enkripsi yang membantu mengamankan lalu lintas data antar perangkat di dalam jaringan. Dengan VLAN, perangkat dapat diisolasi secara

logis meskipun berada dalam jaringan fisik yang sama, sehingga meningkatkan keamanan.

4. Pengelolaan Lalu Lintas: Switch modern mendukung fitur seperti *Quality of Service* (QoS) yang memungkinkan prioritisasi jenis lalu lintas tertentu (misalnya, lalu lintas video atau suara) untuk memastikan kinerja optimal dalam aplikasi-aplikasi penting.

5.1.3 Peran Switch dalam Era Jaringan yang Semakin Kompleks

Dalam jaringan modern, terutama di lingkungan perusahaan besar dan pusat data (data center), switch memegang peranan vital dalam memastikan ketersediaan jaringan yang cepat, andal, dan aman. Di era ini, infrastruktur jaringan tidak lagi sesederhana LAN kecil dengan beberapa perangkat yang saling terhubung. Perusahaan besar memiliki jaringan yang kompleks, terdiri dari ribuan perangkat, server, dan pusat data yang tersebar di berbagai lokasi geografis. Teknologi switch memungkinkan manajemen dan pengaturan lalu lintas data yang efisien dalam lingkungan seperti:

1. Perusahaan Besar: Dalam lingkungan perusahaan besar, switch digunakan untuk menghubungkan jaringan yang kompleks dan memberikan segmentasi yang diperlukan untuk memisahkan departemen-departemen atau fungsi-fungsi yang berbeda dalam perusahaan. Switch berfungsi untuk memastikan bahwa setiap perangkat dapat berkomunikasi dengan cepat dan efisien tanpa menyebabkan penurunan kinerja jaringan keseluruhan.
2. Pusat Data: Di pusat data, switch bekerja sebagai tulang punggung infrastruktur jaringan yang menghubungkan server, storage, dan perangkat lain dalam skala besar. Kecepatan, kapasitas, dan reliabilitas switch sangat penting dalam menjaga kinerja pusat data, terutama karena pusat data modern sering kali melayani aplikasi yang bersifat mission critical. Peran switch dalam pusat data semakin meningkat dengan hadirnya konsep *Software-Defined Networking* (SDN), di mana pengelolaan jaringan dapat dilakukan melalui perangkat lunak yang terpisah dari perangkat keras. Dalam SDN, switch berfungsi sebagai

perangkat yang meneruskan paket data berdasarkan instruksi dari kontroler jaringan, yang memberikan fleksibilitas lebih besar dalam mengelola dan mengoptimalkan jaringan.

3. *Internet of Things* (IoT): Dengan semakin banyaknya perangkat IoT yang terhubung ke jaringan, switch berperan dalam mengelola lalu lintas yang semakin padat dan kompleks. Switch modern dirancang untuk mendukung skala besar perangkat IoT, yang dapat mencapai ribuan perangkat terhubung dalam satu jaringan.

Secara keseluruhan, switch adalah perangkat yang krusial dalam memastikan jaringan berfungsi dengan lancar di era digital yang serba terkoneksi ini. Baik dalam jaringan perusahaan, pusat data, maupun dalam aplikasi IoT, switch memberikan performa, keandalan, dan keamanan yang dibutuhkan oleh infrastruktur jaringan yang semakin kompleks.

5.2 Definisi dan Fungsi Switch

5.2.1 Definisi Switch

Switch adalah perangkat jaringan yang bekerja pada lapisan Data Link Layer (Layer 2) dari model OSI. Perangkat ini bertanggung jawab untuk menghubungkan berbagai perangkat dalam suatu jaringan lokal (*Local Area Network*/LAN), memungkinkan mereka berkomunikasi satu sama lain dengan efisien. Fungsi utama switch adalah meneruskan paket data (*frame*) hanya ke perangkat tujuan yang tepat, menggunakan *Media Access Control* (MAC) address sebagai dasar untuk proses ini.

Dalam jaringan modern, switch berfungsi sebagai tulang punggung untuk memindahkan data secara cepat di antara perangkat seperti komputer, printer, server, dan perangkat lain dalam jaringan LAN. Tidak seperti hub, yang hanya menyalurkan data ke semua perangkat yang terhubung, switch memiliki kecerdasan untuk mempelajari MAC address perangkat yang terhubung dan memastikan bahwa data hanya dikirimkan ke perangkat yang dituju, mengurangi lalu lintas jaringan yang tidak perlu.

5.2.2 Perbandingan Antara Switch, Hub, dan Router

Sebelum teknologi switch berkembang, perangkat seperti hub digunakan untuk menghubungkan beberapa perangkat dalam satu jaringan. Meskipun fungsinya serupa dengan switch, terdapat perbedaan mendasar antara keduanya, serta dengan perangkat router.

1. Hub adalah perangkat jaringan yang bekerja dengan cara mentransmisikan data yang diterimanya ke semua perangkat yang terhubung ke jaringan, tanpa mempedulikan siapa penerima data sebenarnya. Hub bekerja di lapisan fisik (Layer 1) dari model OSI. Dalam jaringan yang menggunakan hub, semua perangkat berbagi bandwidth yang sama. Ini sering menyebabkan collision atau tabrakan data, yang dapat memperlambat kinerja jaringan secara keseluruhan. Karena semua perangkat menerima data yang dikirim, keamanan dan efisiensi jaringan cenderung lebih rendah.
2. Switch: Switch berfungsi lebih cerdas dibandingkan hub. Saat switch menerima frame data, ia memeriksa MAC address tujuan yang terdapat dalam frame tersebut dan hanya meneruskan data ke port yang terhubung dengan perangkat tujuan. Dengan cara ini, switch secara efektif mengisolasi lalu lintas antar perangkat, yang berarti satu perangkat tidak menerima data yang bukan miliknya, mengurangi collision, dan meningkatkan efisiensi bandwidth. Switch juga mempelajari MAC address dari perangkat yang terhubung dan menyimpan informasi ini di dalam MAC Address Table, sehingga setiap kali data dikirim, switch tahu perangkat mana yang harus menerima data tersebut.
3. Router: Router bekerja pada lapisan jaringan (Layer 3) dari model OSI. Fungsinya berbeda dari switch dan hub, yaitu menghubungkan beberapa jaringan dan menentukan jalur terbaik untuk data untuk mencapai tujuan akhir di luar jaringan lokal. Router mempelajari alamat IP perangkat di jaringan dan bekerja berdasarkan protokol routing untuk mengarahkan data antara jaringan yang berbeda, seperti LAN, *Wide Area Network* (WAN), dan Internet.

5.2.3 Cara Kerja Table MAC

Pada dasarnya, switch bekerja dengan mempelajari *Media Access Control* (MAC) address dari setiap perangkat yang terhubung ke jaringan melalui port-portnya. Setiap perangkat yang terhubung ke switch memiliki alamat MAC unik yang ditentukan pada saat pembuatan perangkat kerasnya. Ketika switch menerima paket data dari suatu perangkat, switch memeriksa frame header untuk mengetahui MAC address asal dan tujuan dari frame tersebut. Berikut cara kerja tabel MAC:

1. Pembelajaran MAC

   Saat sebuah perangkat baru mengirimkan data, switch akan membaca alamat MAC sumber dari frame yang masuk dan mencatatnya di MAC Address Table bersama dengan port fisik tempat perangkat tersebut terhubung. Dengan demikian, switch "mempelajari" di mana perangkat tersebut berada.

2. Pencarian MAC Address

   Saat switch menerima frame, ia juga memeriksa alamat MAC tujuan. Jika alamat MAC tujuan ada di tabel, switch meneruskan frame tersebut langsung ke port yang sesuai. Jika alamat MAC tujuan belum tercatat dalam tabel (misalnya perangkat baru yang belum pernah mengirim/terima data), switch akan meneruskan frame tersebut ke semua port, kecuali port tempat frame diterima. Ini dikenal sebagai flooding.

3. Pembaharuan Tabel MAC

   Tabel MAC secara dinamis diperbarui setiap kali perangkat baru mengirimkan data atau jika ada perubahan topologi jaringan. Switch juga memiliki mekanisme untuk menghapus entri lama dalam tabel MAC setelah periode waktu tertentu, menjaga efisiensi jaringan.

   Contoh Praktis: Misalkan terdapat tiga perangkat yang terhubung ke switch:

   PC A dengan MAC address **AA:BB:CC:DD:EE**

   PC B dengan MAC address **11:22:33:44:55:66**

   PC C dengan MAC address **77:88:99:00:AA**

   Saat PC A mengirim data ke PC B, switch menerima frame dari PC A melalui port 1 dan mempelajari bahwa MAC address **AA:BB:CC:DD:EE** terhubung ke port 1. Switch kemudian

memeriksa tabel MAC untuk mengetahui di mana **11:22:33:44:55:66** berada. Jika MAC address PC B sudah ada di tabel MAC (misalnya pada port 2), switch akan langsung mengirimkan frame tersebut ke port 2. Jika belum, switch akan melakukan flooding ke semua port kecuali port 1 hingga switch mengetahui posisi PC B. Setelah PC B mengirimkan balasan, switch akan memperbarui tabel MAC untuk mencatat bahwa **11:22:33:44:55:66** terhubung ke port 2, sehingga pada komunikasi selanjutnya antara PC A dan PC B, data akan dikirim secara langsung tanpa flooding.

5.2.4 Keuntungan Penggunaan Switch Dibandingkan Hub dan Router

1. **Efisiensi Lalu Lintas**
   Tidak seperti hub yang mengirimkan data ke semua perangkat, switch hanya mengirim data ke perangkat tujuan, mengurangi lalu lintas yang tidak perlu dan meningkatkan efisiensi penggunaan bandwidth.
2. **Mengurangi Collision**
   Switch mengelola collision domain dengan baik. Setiap perangkat yang terhubung ke switch memiliki collision domain tersendiri, sehingga mengurangi kemungkinan tabrakan data.
3. **Kecepatan yang Lebih Tinggi**
   Switch modern mendukung kecepatan tinggi, mulai dari 1 Gbps hingga 100 Gbps, yang sangat berguna dalam jaringan yang memiliki lalu lintas data tinggi, seperti pusat data atau jaringan perusahaan besar.
4. **Pengelolaan Lebih Baik**
   Switch managed memungkinkan administrator jaringan untuk memonitor, mengelola, dan mengontrol lalu lintas jaringan melalui fitur-fitur seperti **VLAN**, **Link Aggregation**, dan **QoS**.

5.3 Cara Kerja Switch

Cara kerjanya didasarkan pada penggunaan MAC address dan frame switching, di mana switch memutuskan ke mana data harus

diarahkan berdasarkan alamat tujuan di dalam frame. Pada bagian ini, kita akan membahas lebih mendalam bagaimana switch bekerja, termasuk protokol-protokol yang digunakan untuk menghindari masalah jaringan seperti loop, serta bagaimana switch mengelola berbagai jenis lalu lintas jaringan.

5.3.1 *Protokol Switching* dan *Spanning Tree Protocol* (STP)

Salah satu masalah utama yang bisa terjadi dalam jaringan yang menggunakan switch adalah loop. Loop terjadi ketika ada lebih dari satu jalur yang menghubungkan perangkat di jaringan, yang menyebabkan frame data berputar tanpa henti. Dalam kondisi ini, frame broadcast bisa terus berputar di jaringan, menyebabkan broadcast storm yang akan memperlambat, bahkan menghentikan operasi jaringan. Untuk menghindari masalah ini, digunakan protokol *Spanning Tree Protocol* (STP).

Spanning Tree Protocol (STP) adalah protokol yang digunakan untuk memastikan bahwa tidak ada loop dalam jaringan dengan multiple switch. STP beroperasi dengan membuat topologi logis yang disebut spanning tree di dalam jaringan fisik. Protokol ini secara dinamis menonaktifkan jalur yang redundan di antara switch, menciptakan jalur tunggal untuk menghindari loop. Namun, jika jalur aktif mengalami kegagalan, STP secara otomatis akan mengaktifkan jalur cadangan yang sebelumnya dinonaktifkan, menjaga jaringan tetap berjalan. Berikut adalah langkah-langkah dasar yang dilakukan STP:

1. Pemilihan Root Bridge, STP memilih satu switch sebagai root bridge, yaitu pusat dari spanning tree. Switch dengan Bridge ID terendah akan dipilih sebagai root bridge. Bridge ID terdiri dari prioritas switch dan MAC address-nya.
2. Menentukan Jalur Terbaik, setelah root bridge dipilih setiap switch di jaringan akan menentukan jalur terpendek menuju root bridge. Ini dilakukan dengan menghitung path cost, yang didasarkan pada kecepatan link antara switch.
3. Memblokir Jalur Redundan, STP kemudian memblokir semua jalur lain yang dapat menyebabkan loop, kecuali jalur terbaik menuju root bridge. Jalur yang diblokir tetap tersedia sebagai jalur cadangan jika jalur utama mengalami kegagalan.

4. Pemulihan Otomatis, jika jalur utama gagal STP secara otomatis akan mengaktifkan jalur cadangan untuk memastikan jaringan tetap aktif tanpa loop.

5.3.2 Pengelolaan Jenis Lalu Lintas: Broadcast, Unicast, dan Multicast

Switch modern mampu mengelola berbagai jenis lalu lintas data, termasuk broadcast, unicast, dan multicast. Masing-masing jenis lalu lintas ini memiliki cara pengelolaan yang berbeda di dalam switch.

1. Broadcast Traffic

   Broadcast traffic adalah data yang dikirimkan oleh satu perangkat untuk diterima oleh semua perangkat dalam jaringan. Saat sebuah perangkat mengirimkan paket broadcast, switch meneruskannya ke semua port kecuali port asal, karena broadcast tidak memiliki alamat tujuan yang spesifik. Contoh umum dari broadcast traffic adalah paket ARP (*Address Resolution Protocol*).
2. Unicast Traffic

   Unicast traffic adalah data yang dikirimkan oleh satu perangkat ke satu perangkat lain secara spesifik. Switch menggunakan tabel MAC address untuk memastikan bahwa data unicast hanya dikirim ke port yang terhubung ke perangkat tujuan. Ini adalah mode lalu lintas paling umum dalam jaringan modern.
3. Multicast Traffic

   Multicast traffic digunakan ketika satu perangkat ingin mengirimkan data ke sekelompok perangkat yang terpilih, bukan ke semua perangkat seperti pada broadcast. Switch menangani multicast menggunakan IGMP (*Internet Group Management Protocol*) untuk melacak perangkat mana yang termasuk dalam grup multicast, sehingga data hanya dikirim ke perangkat yang benar-benar memintanya, mengurangi lalu lintas yang tidak perlu.

5.3.3 Tabel MAC dan Alur Kerja Switching

Tabel MAC Address atau Forwarding Table adalah inti dari cara kerja switch dalam mengelola unicast traffic. Setiap kali switch menerima frame, ia mempelajari alamat MAC sumber dari frame tersebut dan mencatatnya di dalam tabel MAC. Kemudian, switch memeriksa MAC address tujuan untuk mengetahui ke port mana frame harus dikirim.

Berikut alur kerja switching yang menggunakan tabel MAC:

1. Mempelajari MAC Address
   Ketika frame diterima di sebuah port, switch akan memeriksa MAC address sumber dari frame tersebut. Jika MAC address tersebut belum ada di tabel MAC, switch akan menambahkannya dan mengaitkannya dengan port tempat frame tersebut diterima.
2. Pencocokan MAC Address
   Switch kemudian memeriksa MAC address tujuan dari frame. Jika MAC address tersebut ada di tabel MAC, switch akan langsung meneruskan frame ke port yang sesuai.
3. Flooding untuk Alamat Tidak Dikenal
   Jika MAC address tujuan belum ada di tabel, switch melakukan flooding dengan mengirim frame ke semua port kecuali port asal. Ketika perangkat yang sesuai menerima frame dan membalas, switch akan mempelajari MAC address-nya dan memperbarui tabel MAC.
4. Penghapusan MAC Address Lama
   Untuk menjaga efisiensi, tabel MAC memiliki mekanisme untuk menghapus entri lama setelah periode waktu tertentu jika perangkat tidak aktif, memungkinkan tabel MAC untuk diperbarui secara dinamis.

5.3.4 Masalah Umum pada Switch dan Solusinya

Meski switch merupakan perangkat jaringan yang canggih, beberapa masalah bisa muncul dalam jaringan yang menggunakan switch. Dua masalah utama adalah *congestion* (kemacetan) dan *latency* (keterlambatan).

1. *Congestion* (Kemacetan)

   Congestion terjadi ketika terlalu banyak lalu lintas yang harus ditangani oleh switch atau ketika ada lebih banyak perangkat yang mencoba mengirim data melalui port yang sama. Ini bisa mengakibatkan penurunan kinerja jaringan, dengan frame yang tertunda atau bahkan hilang. Solusi yang dapat digunakan yaitu:

   a. Switch berkecepatan tinggi, menggunakan switch dengan kapasitas bandwidth yang lebih tinggi, seperti 10 Gbps atau 40 Gbps, untuk menangani lalu lintas yang padat.
   b. *Quality of Service* (QoS), mengimplementasikan QoS untuk memprioritaskan jenis lalu lintas tertentu, seperti suara dan video, sehingga lalu lintas penting tidak terpengaruh oleh congestion.

2. *Latency* (Keterlambatan)

   Latency adalah waktu yang dibutuhkan untuk data mencapai tujuan. *Latency* yang tinggi bisa terjadi karena switch harus memproses banyak frame atau karena konfigurasi jaringan yang tidak optimal. Solusi untuk mengatasi permasalahan tersebut:

   a. Switch dengan low-latency, menggunakan switch yang dirancang khusus untuk latency rendah, terutama untuk aplikasi seperti pusat data dan jaringan kecepatan tinggi.
   b. Memperbaiki Topologi Jaringan, mengurangi jumlah hop yang harus dilalui data dalam perjalanan dari sumber ke tujuan dengan mengoptimalkan rute.

Switch modern dilengkapi dengan teknologi seperti *store-and-forward switching, cut-through switching*, dan *buffering* untuk membantu mengurangi latency dan meningkatkan kinerja keseluruhan jaringan. Dengan kemampuan untuk mengelola lalu lintas yang kompleks, mencegah loop melalui STP, dan mengatasi masalah seperti *congestion* dan *latency, switch* menjadi perangkat jaringan yang sangat penting dalam infrastruktur modern, terutama di lingkungan yang padat seperti perusahaan besar dan pusat data.

5.4 Jenis-jenis Switch

Switch hadir dalam berbagai jenis berdasarkan fungsionalitas, lapisan jaringan, dan kebutuhan pengguna. Pada bagian ini, kita akan membahas lebih rinci perbedaan antara switch layer 2 dan layer 3, pengenalan *switch Software-Defined Networking* (SDN), dan jenis-jenis switch lain seperti *core switch, distribution switch,* dan *access switch*. Terakhir, tabel perbandingan fitur switch unmanaged dan managed akan membantu memudahkan pemahaman mengenai pilihan perangkat yang tersedia.

5.4.1 Switch Layer 2 vs Layer 3

Switch Layer 2 beroperasi pada Data Link Layer dari model OSI dan bertanggung jawab untuk meneruskan frame berdasarkan MAC address. Switch layer 2 tidak memerlukan konfigurasi khusus untuk berfungsi di dalam jaringan dan biasanya digunakan untuk switching antar perangkat di dalam satu subnet. Switch Layer 3, di sisi lain, beroperasi pada Network Layer dan mampu meneruskan paket data berdasarkan IP address, sehingga tidak hanya mendukung switching tetapi juga routing. Ini berarti switch layer 3 dapat digunakan untuk komunikasi antar subnet atau VLAN (Virtual Local Area Network), menggantikan beberapa fungsi dari router. Switch Layer 2 biasanya digunakan di level Access di jaringan perusahaan atau kampus, di mana switch ini berfungsi untuk menghubungkan perangkat endpoint seperti komputer dan printer. Switch Layer 3 umumnya digunakan di level Distribution atau Core, di mana lalu lintas antar VLAN atau subnet perlu dirutekan.

Tabel 5.1. Perbandingan Switch Layer 2 dan Switch Layer 3

Fitur	Switch Layer 2	Switch Layer 3
Operasi pada Layer	Layer 2 (Data Link)	Layer 3 (Network)
Metode Forwarding	Berdasarkan MAC Address	Berdasarkan IP Address
Fungsi Routing	Tidak mendukung routing	Mendukung routing antar subnet/VLAN

Fitur	Switch Layer 2	Switch Layer 3
Contoh Penggunaan	Access Switch	Core/Distribution Switch
Biaya	Lebih murah	Relatif lebih mahal
Kompleksitas Konfigurasi	Sederhana	Lebih kompleks, mendukung pengaturan IP

5.4.2 Switch Berbasis Perangkat Lunak (*Software-Defined Networking*/SDN)

Switch berbasis *Software-Defined Networking* (SDN) adalah *switch* yang pengelolaannya dilakukan secara terpusat melalui perangkat lunak. Berbeda dengan *switch* tradisional yang menggunakan kontrol terdistribusi, SDN memungkinkan administrator jaringan untuk mengontrol semua switch dari satu titik kontrol. Ini memberikan fleksibilitas yang lebih besar dalam mengelola dan mengoptimalkan jaringan. Beberapa manfaat switch SDN:

1. Fleksibilitas: SDN memungkinkan perubahan topologi jaringan dengan cepat dan efisien, tanpa perlu mengubah perangkat keras.
2. Pengelolaan Terpusat: Semua perangkat switch dapat dikonfigurasi dan dipantau dari satu platform pusat, memudahkan administrasi jaringan besar.
3. Penggunaan yang Lebih Optimal: SDN memungkinkan pengelolaan lalu lintas jaringan yang lebih dinamis dan adaptif, yang sangat bermanfaat dalam jaringan pusat data (data center) atau perusahaan besar.

5.4.3 Jenis-jenis Switch: Core, Distribution, dan Access Switch

Dalam topologi jaringan perusahaan, switch dapat dibagi menjadi tiga jenis berdasarkan fungsi dan posisi mereka dalam hierarki jaringan:

1. Core Switch
   Core switch berada di inti jaringan dan berfungsi sebagai backbone dari seluruh infrastruktur jaringan. Switch ini memiliki kapasitas tinggi dan digunakan untuk menghubungkan semua distribution switch atau server

utama. Core switch biasanya berada di pusat data atau pusat jaringan perusahaan besar.

2. Distribution Switch
   Distribution switch berfungsi sebagai perantara antara access switch dan core switch. Distribusi lalu lintas yang berasal dari beberapa access switch diteruskan ke core switch melalui distribution switch. Pada lapisan ini, fitur seperti routing antar VLAN dan pengelolaan policy QoS diterapkan.
3. Access Switch
   Access switch digunakan untuk menghubungkan perangkat endpoint seperti komputer, printer, dan perangkat IoT. Switch ini berada di lapisan terdepan dari jaringan dan umumnya berfungsi sebagai layer 2 switch.

5.4.4 Perbandingan Managed vs Unmanaged Switch

Managed switch memberikan kontrol lebih besar terhadap lalu lintas jaringan dibandingkan unmanaged switch. Berikut tabel perbandingannya.

Tabel 5.2. Perbandingan Managed vs Unmanaged switch

Fitur	**Managed Switch**	**Unmanaged Switch**
Pengelolaan	Mendukung pengelolaan melalui CLI, SNMP, atau GUI	Tidak mendukung pengelolaan
Keamanan	Mendukung pengaturan keamanan tingkat lanjut	Hanya fitur keamanan dasar
Fitur VLAN	Mendukung VLAN	Tidak mendukung VLAN
Harga	Lebih mahal	Lebih murah
Kompleksitas Penggunaan	Lebih kompleks	Sangat sederhana, plug-and-play

5.5 Keuntungan Penggunaan Switch

Penggunaan switch dalam jaringan modern memberikan banyak keuntungan dibandingkan perangkat jaringan sebelumnya seperti hub atau bridge. Pada bagian ini, kita akan membahas beberapa keuntungan tersebut serta memberikan contoh studi kasus penggunaannya dalam jaringan perusahaan besar.

5.5.1 Studi Kasus: Implementasi Switch di Perusahaan Besar

Perusahaan besar dengan ribuan perangkat endpoint menggunakan switch untuk mengelola lalu lintas jaringan yang padat. Misalnya, sebuah perusahaan multinasional yang memiliki beberapa departemen dan gedung membutuhkan switch layer 3 untuk mengelola komunikasi antar subnet dan VLAN. Switch modern mampu mengelola lalu lintas ini dengan efektif, memisahkan segmen-segmen jaringan untuk meningkatkan keamanan dan kinerja. Keuntungan dari penggunaan switch di lingkungan seperti ini meliputi:

1. Peningkatan Bandwidth, dengan teknologi seperti link aggregation beberapa port fisik pada switch dapat digabungkan untuk menyediakan jalur dengan bandwidth lebih besar, sangat berguna di pusat data dan backbone jaringan.
2. Keamanan yang Lebih Baik, switch managed memungkinkan administrator untuk memisahkan lalu lintas jaringan ke dalam VLAN yang terisolasi, meningkatkan keamanan jaringan.
3. Pengelolaan yang Efisien, switch modern dilengkapi dengan fitur *Quality of Service* (QoS) untuk memprioritaskan lalu lintas kritis seperti *voice over* IP (VoIP) dan video conferencing, meningkatkan kualitas layanan secara keseluruhan.

5.2.2 Efisiensi Jaringan dalam Jaringan Padat

Dalam jaringan kampus atau perusahaan besar, switch memainkan peran penting dalam menjaga efisiensi jaringan. Kemampuan switch untuk melakukan unicast, multicast, dan broadcast filtering sangat penting untuk mengurangi beban lalu

lintas yang tidak perlu. Penggunaan VLAN juga memungkinkan administrator untuk membagi jaringan fisik menjadi beberapa jaringan virtual, mengurangi konflik alamat IP dan meningkatkan fleksibilitas pengelolaan jaringan. Switch modern, terutama yang digunakan di level distribution dan core, juga mendukung load balancing dan link redundancy untuk memastikan kelancaran operasional bahkan ketika ada link yang gagal.

DAFTAR PUSTAKA

Cisco Networking Academy (Ed.). (2020). *Introduction to networks companion guide (ccnav7)* (1 ed.). Cisco Press.

Cisco Systems, Inc. (2019). *Understanding Spanning Tree Protocol (STP)*. Cisco Systems.

Forouzan, B. A. (2013). *Data communications and networking* (5. ed). McGraw-Hill.

Held, G. (2000). *Understanding data communications: From fundamentals to networking* (3. ed). Wiley.

Indarwati, I., Muttakin, A., & Bantala, A. P. (2023). *Dasar-Dasar Teknik Jaringan Komputer Dan Telekomunikasi*.

McQuerry, S., Jansen, D., & Hucaby, D. (2009). *Cisco LAN switching configuration handbook* (2nd ed). Cisco Press.

Spurgeon, C. (2000). *Ethernet: The definitive guide*. O'Reilly.

Suprapto, A. (2020). *Pengantar Jaringan Komputer Pendekatan Praktis untuk Pemula*. IAIN SALATIGA.

Tanenbaum, A. S., & Wetherall, D. (2011). *Computer networks* (5. ed). Prentice Hall.

BAB 6
STATIC ROUTING

6.1 Pendahuluan

Pesatnya perkembangan teknologi digital telah menjadikan jaringan komputer sebagai infrastruktur vital dalam berbagai sektor, mulai dari pendidikan, pemerintahan, hingga industri (Kurniawan, 2021; Wahyudi et al., 2019). Di tengah pertumbuhan user dan perangkat yang saling terhubung, muncul tantangan pengelolaan lalu lintas data agar setiap informasi dapat sampai tujuan secara efisien serta aman (Zenhadi, 2022). Salah satu elemen kritis dalam arsitektur jaringan adalah proses routing, di mana router harus menentukan jalan terbaik bagi paket data melintasi berbagai segmen—proses ini ibarat jantung transportasi informasi di dunia maya.

Static routing masih menjadi pilihan utama pada jaringan yang cenderung stabil, segmentasi terbatas, serta kebutuhan kontrol jalur secara manual (Analisis PNL, 2022; ITU Online, 2024). Studi terbaru mengungkapkan, routing statik menawarkan keunggulan pada prediktabilitas, keamanan, dan minim risiko pengambilalihan rute otomatis oleh pihak tidak bertanggung jawab (JTI-UB, 2021; Uninets, 2025). Hal ini selaras dengan hasil riset di berbagai laboratorium dan case study instansi pendidikan, di mana static routing kerap diterapkan untuk skenario jaringan laboratorium, kantor cabang, maupun backup jalur utama (Prosiding Unram, 2024; DigiTech, 2022).

Namun, pendekatan statik memiliki tantangan khusus, terutama dalam hal adaptasi topologi yang dinamis. Pada jaringan berskala besar dan sering berubah, administrator harus melakukan konfigurasi manual pada setiap perangkat ketika terjadi perubahan rute. Ketelitian dan dokumentasi menjadi aspek penting untuk mencegah terjadinya unreachable network dan downtime layanan (Jurnal PNL, 2022; Static Routing Lab Report, 2025). Inilah yang juga menjadi pembeda utama dibandingkan pendekatan dynamic routing

seperti OSPF atau BGP, yang lebih adaptif melalui pembaruan otomatis (TAU, 2021).

Studi-studi mutakhir menganalisis bahwa keunggulan static routing dinilai sangat penting untuk penerapan pada jaringan dengan segmentasi khusus, layanan vital, serta sebagai backup jalur utama untuk menghadapi failure pada jalur dinamis (Uninets, 2025; CN Case Study, 2025). Tidak heran, implementasi static route tetap menjadi materi utama dalam pelatihan profesional dan sertifikasi bidang jaringan di seluruh dunia (Routing Configuration Cisco, 2022).

Bab ini akan membahas secara terstruktur konsep, prinsip kerja, praktik konfigurasi, dan studi kasus static routing di jaringan komputer modern. Selain tinjauan teori, setiap penjelasan akan diperkaya temuan terbaru dan best-practice hasil riset 2021–2025, sehingga menjadi referensi aktual bagi pembaca yang ingin memahami ataupun mengimplementasikan static routing di lingkungan riil.(Hamalik, 2020).

6.2 Dasar Teori *Static Routing*

Static routing adalah teknik pengaturan jalur data di jaringan komputer di mana administrator secara manual menentukan dan mencatat rute di setiap perangkat router (Wahyudi et al., 2019; JTIK UB, 2021). Berbeda dengan *dynamic routing* yang beradaptasi otomatis terhadap perubahan topologi, *static routing* tetap pada instruksi manual hingga terjadi pembaruan oleh operator. Setiap entry di tabel routing statis terdiri atas destination network, subnet mask, next-hop atau exit interface.

Studi laboratorium dan simulasi mutakhir membuktikan, static route sangat efisien digunakan pada jaringan dengan struktur tetap atau kebutuhan segmentasi khusus, seperti laboratorium, jaringan cabang, dan segment backup. Hal ini tercermin pada penelitian Analisis PNL (2022), yang menunjukkan bahwa rute statis unggul dalam delay minimal dan stabilitas throughput dibanding dynamic route, selaras dengan hasil percobaan ITU Online (2024) pada network router Cisco dan Juniper.

Contoh entry pada tabel routing statis

Destination	Netmask	Gateway	Interface
192.168.10.0	255.255.255.0	192.168.1.1	FastEthernet0/1

Konsep ini juga didukung pada implementasi sistem pendidikan: Prosiding Unram (2024) menemukan static routing sangat tepat untuk praktikum jaringan komputer dan troubleshooting segment isolasi karena administrator dapat memantau dan memodifikasi tiap rute secara presisi. Praktikum desain jaringan dengan static routing memperlihatkan keterkaitan yang kuat antara dokumentasi, pemahaman struktur topologi, serta pengelolaan jalur data (Static Routing Lab Report, 2025).
Keunggulan utama static routing meliputi:

1. Prediktabilitas dan kontrol penuh jalur data,
2. Zero overhead trafik pembaruan,
3. Minim risiko pembajakan rute oleh protokol traffic luar,
4. Diagnostik dan troubleshooting lebih sederhana.

Namun, kekurangan static routing mulai tampak pada skala besar atau jaringan yang sering berubah. Setiap kali penambahan atau pengurangan segmen, administrator harus memperbarui tabel routing di banyak perangkat (Jurnal DigiTech, 2022; Uninets, 2025). Kesalahan pencatatan rute dapat berujung pada unreachable segment dan memerlukan analisis manual pada setiap node jaringan (CN Case Study, 2025).

Pada era hybrid, static routing juga sering menjadi backup via floating static route, yang hanya aktif bila jalur dynamic gagal, sehingga pelayanan tetap berjalan di jaringan vital (Routing Configuration Cisco, 2022).

Prinsip teori static routing menjadi dasar utama sebelum administrator melangkah ke pengelolaan dynamic routing yang lebih kompleks, karena seluruh troubleshooting dan desain yang efisien bermula dari pemahaman manual tentang pemetaan jalur data di jaringan komputer.

6.3 Prinsip Kerja *Static Routing*

Pada prinsipnya, *static routing* mengandalkan aturan eksplisit yang dimasukkan administrator ke tabel routing setiap router. Setiap kali sebuah paket masuk ke router, perangkat akan memeriksa destination address pada header paket dan mencari rute yang sesuai di tabel routing (ITU Online, 2024). Jika ditemukan, paket akan diteruskan ke next-hop atau keluar melalui antarmuka yang ditentukan pada entri static route tersebut.

Alur Forwarding Data

1. Pembacaan Destination: Router menerima paket dan membaca destination IP.
2. Pencocokan Tabel Routing: Router mencocokkan jaringan tujuan dengan entri static routing yang telah diinput secara manual.
3. Forwarding Paket: Jika ada kecocokan, paket dikirim ke IP *next-hop* (gateway) atau keluar lewat interface yang diset. Jika tidak, paket bisa dibuang atau dilempar ke default gateway jika tersedia.
4. Replikasi di Setiap Hop: Setiap router berikutnya mengulangi proses yang sama hingga paket sampai tujuan akhir.

Konsep next-hop menjadi inti: jika perintah ip route 10.10.10.0 255.255.255.0 192.168.1.2 dimasukkan, maka semua trafik ke 10.10.10.0/24 akan dilempar ke router dengan alamat 192.168.1.2. Model forwarding ini konsisten di setiap device, menciptakan prediktabilitas jalur data (Static Routing Lab Report, 2025(Asrul, dkk. 2014).

Studi Kasus dan Simulasi

Dalam proyek laboratorium atau implementasi kantor cabang, biasanya diterapkan topologi linear atau ring dengan tiga hingga empat router. Setiap perangkat dikonfigurasi *static routing* satu per satu berdasarkan segmentasi jaringan (Prosiding Unram, 2024; CN Case Study, 2025). Jika salah satu route hilang, segmentasi tersebut menjadi *unreachable—a clear demonstration of strict dependency* pada entry statis.

Tabel simulasi static route:

Router	Destination	Netmask	Next-Hop	Interface
R1	192.168.3.0	255.255.255.0	192.168.2.2	Fa0/1
R2	192.168.1.0	255.255.255.0	192.168.2.1	Fa0/0
R3	192.168.1.0	255.255.255.0	192.168.3.1	Fa0/0

Keunggulan dan Batasan

Keuntungan prinsip kerja static routing:

1. Posisi jalur tetap dan mudah diprediksi,
2. Tidak ada update berkala yang membebani jaringan,
3. Troubleshooting lebih sederhana, sangat tepat untuk jaringan kecil atau kebutuhan jalur khusus.

Kekurangannya tampak bila terjadi perubahan atau penambahan jaringan—setiap update harus dikonfigurasi manual oleh admin di setiap router, sehingga rentan human error dan tidak fleksibel pada skala besar (Uninets, 2025; JTIK UB, 2021).

Penggunaan Hybrid dan Backup

Penelitian terbaru juga menyoroti praktik penggunaan floating *static route*, yakni jalur statis dengan administrative distance lebih tinggi yang hanya aktif jika dynamic routing gagal, guna menjamin redundansi dan ketersediaan layanan vital (Cisco Config Guide, 2022).

Studi Kasus dan Implementasi Static Routing

Implementasi static routing dalam jaringan komputer telah diuji dalam berbagai skenario, baik di lingkungan laboratorium pendidikan, enterprise, maupun case study pada public network (Uninets, 2025; Juniper, 2024). Studi mutakhir menyoroti bagaimana konfigurasi static routing secara manual memungkinkan administrator mengontrol penuh jalur data—mulai dari jaringan kecil, stub, kantor cabang, hingga deployment hybrid untuk failover/dedicated route backup (Cisco, 2022).

Studi Kasus 1: Jaringan Dua Router (LAN–LAN)

GeeksforGeeks (2022) memperlihatkan contoh implementasi paling dasar: dua router yang menghubungkan dua network berbeda. Static routing diatur agar paket data dari Network 1 (10.1.1.0/24) bisa sampai ke Network 2 (10.2.2.0/24), dan sebaliknya.

Konfigurasi:
Router R1:
ip route 10.2.2.0 255.255.255.0 10.1.1.2
Router R2:
ip route 10.1.1.0 255.255.255.0 10.2.2.2

Dengan konfigurasi ini, komunikasi dua arah dapat terjadi tanpa memerlukan dynamic routing protocol apa pun.
Tabel ilustrasi:

Router	Destination	Netmask	Next-Hop
R1	10.2.2.0	255.255.255.0	10.1.1.2
R2	10.1.1.0	255.255.255.0	10.2.2.2

Studi Kasus 2: Backbone Kampus dan Simulasi EVE-NG

Network backbone kampus UIN Sunan Kalijaga disimulasikan dengan EVE-NG untuk membandingkan *static routing* dan OSPF pada pengembangan jaringan antar gedung (Gatra, 2021). Hasil pengujian throughput dan delay dalam kondisi normal maupun ramai menunjukkan performa static routing sedikit lebih stabil, dengan average delay sekitar 59,5 ms dan throughput ±596 Bps. Packet loss rata-rata 0%, membuktikan keandalan static routing pada trafik yang tidak fluktuatif.

Studi Kasus 3: Enterprise & Network Planner

Juniper NorthStar Planner (2024) menggarisbawahi importance static route pada perencanaan jalur traffic penting, misalnya untuk permintaan layanan backup, VPN, atau rute khusus ke node tertentu. Static route digunakan agar traffic ke node vital selalu menempuh path yang sudah didefinisikan. Hal ini juga mempermudah troubleshooting dan pengendalian kebijakan routing di datacenter.

Studi Kasus 4: *Hybrid Static–Dynamic* (Backup)

Panduan Cisco NCS6000 (2022) dan Uninets (2025) juga menyorot teknik floating static route, yakni static route dengan administrative distance lebih tinggi, yang disiapkan untuk mengambil alih ketika primary (dynamic) route gagal.

1. Contoh praktik:
2. Primary dynamic route: OSPF
3. Static backup:
4. ip route 0.0.0.0 0.0.0.0 [next-hop] 250
5. Floating static route ini hanya aktif ketika jalur OSPF down, menjaga agar layanan tetap berjalan (*failover seamless*).

Tabel Perbandingan

Aspek	Static Routing	Dynamic Routing
Konfigurasi	Manual tiap node	Otomatis via protokol
Overhead	Minim	Ada update otomatis
Keamanan	Tinggi (tidak advertise)	Potensi expose
Skalabilitas	Rendah (manual)	Tinggi (adaptif)
Troubleshooting	Lebih mudah	Butuh analisis log
Contoh Kasus	Stub, backup, datacenter	Campus, WAN, ISP

Insight Praktis

Pengalaman lapangan dan simulasi mutakhir menegaskan keandalan static routing pada skala kecil–menengah serta pada critical segment, namun pada jaringan besar dengan kebutuhan skalabilitas dan automatisasi, dynamic routing tetap lebih efisien (Gatra, 2021; Uninets, 2025; Cisco, 2022).

Studi Kasus 5: Topologi "Fish" dalam Perencanaan Traffic (Juniper, 2024)

Pada skenario perencanaan traffic jaringan MPLS antarkota (studi Juniper NorthStar 2024), static route dimanfaatkan untuk mengarahkan permintaan bandwidth tinggi dengan jalur tertentu

demi mencegah kemacetan dan menjaga SLA layanan penting. Misalkan, permintaan traffic ke node NYC (IP: 10.10.10.11) dapat diarahkan secara eksplisit oleh admin dengan *static route* yang memaksa demand melewati jalur "CHI–DET–BOS"—menghindari rute default melalui node PHI.
Langkah konfigurasi:

1. Tetapkan IP tujuan pada node,
2. Tambahkan static route di source node (misal: dari WDC via tunnel RWDCBOS),
3. Verifikasi jalur traffic benar-benar mengikuti rute yang didefinisikan (bukan shortest path otomatis).
4. Insight penting: Static route memudahkan enforce traffic policy spesifik, terutama pada jaringan backbone, datacenter, maupun segment pelayanan kritikal yang tidak boleh terkena load balancing otomatis.

Studi Kasus 6: Uji IPv4 vs IPv6 pada Static Routing

1. Mahasiswa Universitas Bina Darma (Ulfa, 2017) melakukan benchmarking performa static routing pada topologi dual-stack:
   a. **Parameter diuji:** throughput, delay, packet loss saat melakukan transfer file 5MB dan 10MB dengan IPv4 vs IPv6.
   b. **Hasil:**
      - **Average throughput IPv6 (file 5MB):** 0.37 Mbps
      - **Average throughput IPv4 (file 5MB):** 0.3276 Mbps
      - **Packet loss static routing:** IPv6 = 0.036%, IPv4 = 0.042%
      - **Average delay static routing:** sekitar 0.03–0.04 detik (masih kategori sangat baik TIPHON).
   c. **Kesimpulan:** Static routing pada IPv6 cenderung sedikit lebih baik daripada IPv4 dari segi throughput, delay, dan packet loss dalam skenario file transfer laboratorium.

Tabel data performa:

Param	IPv4 (5MB)	IPv4 (10MB)	IPv6 (5MB)	IPv6 (10MB)
Throughput	0.3276	0.291	0.37	0.3748
Packet Loss%	0.042	0.034	0.036	0.024
Delay (detik)	0.0307	0.04	0.036	0.024

2. **(Data: Ulfa, 2017, Jurnal Matrik Binadarma).**
   Temuan Praktis & Rekomendasi
   a. **Pengujian kampus dan project enterprise** pada backbone UIN 2021 menunjukkan delay statis stabil sekitar 59,5 ms dan packet loss ~0% ketika topologi tidak berubah, reinforcing bahwa *static routing* masih sangat andal untuk core-to-edge segment *mission critical*.
   b. **Static route** paling efektif sebagai *policy path enforcement* dan backup failover pada skenario hybrid, di mana protokol dinamis (seperti OSPF/BGP) aktif sebagai jalur utama, static route level administrasi tinggi sebagai jalur cadangan (Cisco, 2022).

   Ringkasan Studi Kasus
   a. Implementasi static routing mudah dan powerful pada jaringan kecil sampai menengah serta traffic policy kritikal.
   b. Selalu dokumentasikan rute statis dan gunakan monitoring tools untuk mencegah error.
   c. Untuk jaringan besar/dinamis pertimbangkan dynamic/mix hybrid routing demi maintainabilitas dan skalabilitas.

Troubleshooting, Best Practice, dan Tips Static Routing

Strategi Dasar *Troubleshooting Static Routing*

Troubleshooting static routing dilakukan dengan pendekatan sistematis yang fokus pada identifikasi error dalam pengaturan jalur statis (Uninets, 2025). Prosesnya meliputi:

Memeriksa konfigurasi route yang hilang, salah penulisan next-hop, kesalahan netmask, atau ada rute yang belum dibuat.

Menggunakan perintah ping dan traceroute untuk memastikan keterjangkauan jaringan (*reachability*) serta mengidentifikasi pada hop mana masalah terjadi (MindmapAI, 2025).

Mengecek tabel routing dengan *show ip route* (Cisco) atau *ip route show* (Linux), pastikan entry static sudah benar dan aktif di router tujuan.

Kasus Praktis & Solusi Cepat

Link Failure: Jika link utama gagal, static route (atau floating static route dengan administrative distance lebih tinggi) bisa menswitch jalur ke backup.

Contoh:
ip route 0.0.0.0 0.0.0.0 [next-hop-backup] 250
Jalur ini hanya aktif jika OSPF/BGP down.

Recursion Depth & Outbound Interface:

Pada perangkat multivendor, seperti Huawei, gunakan outbound interface diparameter agar routing tidak recursion berlebihan; hal ini membantu performa dan efektivitas switchover.

Suboptimal Path: Static route bisa memaksa trafik melewati jalur tercepat atau segment tertentu jika protokol dinamis memilih path yang tidak optimal.

Network Segmentation: Untuk troubleshooting subnet tertentu tanpa mengganggu produksi, static route dapat diarahkan secara presisi ke subnet sasaran.

***Best Practice* Administratif**

Dokumentasi Konfigurasi: Selalu catat dan update seluruh static route setiap perubahan. Dokumentasi yang baik kritikal untuk troubleshooting dan konsistensi after action review pada jaringan berkembang.

Rutin Review & Backup Konfigurasi: Lakukan verifikasi berkala terhadap seluruh entry static pada jaringan, serta simpan *backup router config* untuk *recovery* cepat.

Monitoring & Redundansi: Gunakan tools monitoring seperti SNMP, NetFlow, atau Wireshark untuk deteksi dini anomali jalur. Terapkan backup/failover mechanism agar tidak ada single point of failure.

Sederhanakan Topologi: Jangan menerapkan static routing pada jaringan besar yang sering berubah; lebih baik gunakan dynamic routing untuk scalability.

Verifikasi *Gateway & Interface*: Pastikan tidak ada salah penempatan *default gateway* atau *interface down* (gunakan show ip interface brief atau setara).

Prosedur Troubleshooting

Cek status *interface* (*show ip interface brief* / ip addr show).
Verifikasi tabel routing (*show ip route* / *route print* / *netstat -nr*).
Lakukan *ping antarsegment* dan *traceroute* untuk mencari titik kegagalan.
Review konfigurasi static route pada setiap router yang terlibat.
Hapus atau update rute yang salah, lalu tes ulang konektivitas.
Jika menggunakan dual link/backup, cek administrasi distance dan implementasi failover.

Penutup & Saran Praktis

Static routing menawarkan troubleshooting yang straightforward, kontrol kuat atas jalur data, serta cepat diterapkan untuk bypass error atau isolasi trafik (ShapeHost, 2024). Namun, skalabilitas lemah dan rawan human error bila tidak didokumentasi, sehingga pemeliharaan dan pengecekan berkala jadi kunci sukses jaringan statis modern.

DAFTAR PUSTAKA

Analysis of Backbone UIN Sunan Kalijaga Network using EVE-NG. (2021). Atlantis Press. https://www.atlantis-press.com/proceedings/icse-uin-suka-21/125966896

Analisis Perbandingan Kinerja Routing Statis dan Dinamis. (2022). DigiTech. https://jtiik.ub.ac.id/index.php/jtiik/article/view/2983

Analisis Perbandingan Kinerja Static Routing Protocol dan Dynamic Routing Protocol. (2022). E-Jurnal PNL. https://e-jurnal.pnl.ac.id/eProTIK/article/download/5803/pdf

Cisco. (2022). Implementing Static Routes (NCS6000). https://www.cisco.com/c/en/us/td/docs/routers/ncs6000/software/ncs6k-7-6/routing/configuration/guide/b-routing-cg-ncs6000-76x/m-implementing-static-routing.pdf

Cisco. (2025). Best Practice Static Route Point-to-Point Link = Use Exit Interface Not IP. https://learningnetwork.cisco.com/s/question/0D53i00000Kt6ikCAB/best-practice-static-route-pointtopoint-link-use-exit-interface-not-ip

CNCase Study. (2025). Scribd. https://www.scribd.com/document/738427754/Cn-Case-Study

GeeksforGeeks. (2022). Implementation of Static Routing in Cisco - 2 Router Connections. https://www.geeksforgeeks.org/computer-networks/implementation-of-static-routing-in-cisco-2-router-connections/

Huawei. (2025). Troubleshooting Cases for IPv4 Static Routes. https://support.huawei.com/enterprise/en/doc/EDOC1100372040/108f915d/troubleshooting-cases-for-ipv4-static-routes

JumpCloud. (2025). What Is Static Routing? https://jumpcloud.com/it-index/what-is-static-routing

Juniper Networks. (2024). Static Routes Case Study. https://www.juniper.net/documentation/us/en/software/northstar6.2.3/northstar-planner-user-

guide/topics/task/ipmpls-router-static-routes-case-study.html
MindmapAI. (2025). Static Routing: A Comprehensive Guide. https://mindmapai.app/mind-mapping/static-routing
Palo Alto Networks. (2025). Configure a Static Route. https://docs.paloaltonetworks.com/ngfw/networking/static-routes/configure-a-static-route
ShapeHost. (2024). Unlock the Power of Static Routing to Troubleshoot Networks. https://shape.host/resources/static-routing-for-network-troubleshooting
Static Routing Lab Report. (2025). Scribd. https://www.scribd.com/document/857555484/Static-Routing-Lab-Report
Uninets. (2025). What is Static Routing? [2025 Guide]. https://www.uninets.com/blog/what-is-static-routing
Wahyudi, M., Purnama, R. A., & Firmansyah. (2019). Cisco Routing and Switching. Graha Ilmu. https://elibrary.bsi.ac.id/readbook/211571/cisco-routing-and-switching
Webasha. (2025). What is the difference between static and dynamic routing and how can you configure them. https://www.webasha.com/blog/what-is-the-difference-between-static-and-dynamic-routing-and-how-can-you-configure-them
Webasha. (2025). Routing - Injecting a Static Route. https://notes.networklessons.com/routing-injecting-a-static-route
ITUOnline. (2025). Troubleshooting A Routed Network. https://www.ituonline.com/blogs/troubleshooting-a-routed-network/

BIODATA PENULIS

Hermila A. S.SI., M.Pd.
Dosen Program Studi Pendidikan Teknologi Informasi
Fakultas Teknik Universitas Negeri Gorontalo

Penulis lahir di Polewali Mandar tanggal 25 Juli 1993. Penulis adalah dosen tetap pada Program Studi Pendidikan Teknologi Informasi Fakultas Teknik, Universitas Negeri Gorontalo. Menyelesaikan pendidikan S1 pada Jurusan Sistem Informasi STMIK Profesional Makassar dan melanjutkan S2 pada Jurusan Pendidikan Teknologi Kejuruan Kekhususan Pendidikan Teknik Informatika dan Komputer Universita Negeri Makassar. Penulis sekarang mulai menekuni bidang Menulis.

BIODATA PENULIS

Deddy Rudhistiar, S.Kom., M.Cs.
Dosen Program Studi S1 Teknik Informatika
Fakultas Teknologi Industri Institut Teknologi Nasional Malang

Penulis lahir di Pasuruan tanggal 28 Desember 1989. Penulis adalah dosen tetap pada Program Studi S1 Teknik Informatika Fakultas Teknologi Industri Institut Teknologi Nasional Malang. Menyelesaikan pendidikan S1 pada Jurusan Teknik Informatika dan melanjutkan S2 pada Jurusan Ilmu Komputer. Penulis menekuni bidang Jaringan Komputer, Kemanan Jaringan, Kriptografi dan Teknologi yang berhubungan dengan Cloud Computing.

BIODATA PENULIS

Miftah Fadhli As'ad, S.Kom., M.Kom
Dosen Program Studi Sistem dan Teknologi Informasi
Fakultas Teknik
Universitas Muhammadiyah Sinjai

Penulis lahir di Kab. Kolaka pada tanggal 30 November 1993. Penulis adalah Dosen pada Program Studi Sistem dan Teknologi Informasi Fakultas Teknik di Universitas Muhammadiyah Sinjai, pada tanggal 21 Juni 2004 penulis menyelesaikan studi di SDN 1 Tosiba Kab. Kolaka, tanggal 13 Agustus 2007 penulis menyelesaikan studi di SMPN 1 Samaturu Kab. Kolaka, kemudian menyelesaikan studi di SMK Mutiara Ilmu Makassar pada Tanggal 26 April 2010, Kemudian melanjutkan studi ke jenjang Stratas Satu (S1) Pada Perguruan Tinggi Universitas Muslim Indonesia pada Fakultas Ilmu Komputer Program Studi Teknik Informatika lulus pada tanggal 29 Oktober 2014, dan selanjutnya menyelesaikan Pendidikan Strata dua (S2) di STMIK Handayani Makassar pada tanggal 20 Juni 2022 pada program studi Sistem Komputer.

Saat ini, penulis aktif sebagai dosen tetap di Universitas Muhammadiyah Sinjai. berkontribusi dalam membentuk generasi penerus yang berkompeten. Sebagai seorang penulis, ia memanfaatkan keahliannya dalam bidang informatika untuk menginspirasi dan memberikan wawasan baru bagi para pembaca. Melalui karya-karyanya, penulis berharap dapat terus berkontribusi pada perkembangan ilmu pengetahuan dan pendidikan di Indonesia.

BIODATA PENULIS

Ir. Ali Impron, S.Kom., M.Kom.
Dosen Program Studi Informatika
Fakultas Teknik dan Pertanian
Universitas Muhammadiyah Sampit

Penulis lahir di Grobogan, Jawa Tengah, pada tahun 1983. Penulis adalah seorang dosen dan profesional IT dengan pengalaman lebih dari 17 tahun dalam mengelola layanan IT, internet service provider, dan industri pertambangan. Penulis memiliki keahlian dalam infrastruktur IT, IoT, Data Center, dan Bussiness Intelligence. Saat ini, penulis menjabat sebagai Head of Information Technology di PT. Darma Henwa Tbk, di mana penulis bertanggung jawab untuk mengelola tim IT dan memastikan layanan IT berkualitas tinggi.

Penulis menyelesaikan gelar Sarjana Komputer Prodi Teknik Informatika dari STMIK AKAKOM Yogyakarta, gelar Insinyur dari Prodi Program Profesi Insinyur Institut Teknologi Indonesia dan gelar Magister Teknologi Informasi dari Universitas Teknologi Digital Indonesia, Yogyakarta. Saat ini, penulis sedang menempuh Program Doktor Ilmu Teknik di Universitas Negeri Yogyakarta. Selain perannya di dunia industri, penulis juga tercatat sebagai dosen tetap di Universitas Muhammadiyah Sampit.

Selama karirnya, penulis telah memperoleh berbagai sertifikasi internasional yang mengakui keahliannya di bidang teknologi informasi, termasuk *Microsoft Certified IT Professional* (MCITP), *Cisco Certified Network Associate* (CCNA), dan *Juniper*

Networks Certified Associate (JNCIA). Penulis memiliki minat besar dalam penelitian dan integrasi produk IT terbaru dengan proses bisnis, serta memiliki pemahaman mendalam tentang administrasi sistem, keamanan IT, dan jaringan.

BIODATA PENULIS

Lut Faizal, S.Kom., M.Kom.
Dosen Program Studi Sistem dan Teknologi Informasi
Fakultas Teknik
Universitas Muhammadiyah Sinjai

Penulis lahir di Sinjai pada tanggal 21 Mei 1996. Ia menempuh pendidikan dasar di SDN 108 Banoa, kemudian melanjutkan ke SMP Negeri 5 Sinjai dan SMA Negeri 1 Tellu Limpoe. Setelah itu, ia menempuh pendidikan tinggi di STMIK Handayani Makassar pada program studi Teknik Informatika, lalu melanjutkan ke jenjang pascasarjana di bidang Sistem Komputer di institusi yang sama.

Penulis kini berperan sebagai dosen tetap di Universitas Muhammadiyah Sinjai, berkontribusi dalam membentuk generasi penerus yang berkompeten. Sebagai seorang penulis, ia memanfaatkan keahliannya dalam bidang informatika untuk menginspirasi dan memberikan wawasan baru bagi para pembaca. Melalui karya-karyanya, penulis berharap dapat terus berkontribusi pada perkembangan ilmu pengetahuan dan pendidikan di Indonesia.

BIODATA PENULIS

Octsa Khairus Praharsyarendra, S.Kom., M.M.
Dosen Program Studi Sistem Informasi
Fakultas Teknik dan Ilmu Komputer Universitas Indraprasta

Penulis lahir di Jakarta tanggal 29 Oktober 1991. Penulis adalah dosen tetap pada Program Studi Sistem Informasi Fakultas Teknik dan Ilmu Komputer, Universitas Indraprasta. Menyelesaikan pendidikan S1 di Universitas Bina Nusantara Jurusan Teknik Informatika dan melanjutkan S2 di Sekolah Bisnis Institut Pertanian Bogor (IPB) Jurusan Manajemen Bisnis.