PENGENALAN JARINGAN KOMPUTER

Agung Susilo Yuda Irawan
Zen Munawar
Anindya Khrisna Wardhani
Arip Solehudin
Azhari Ali Ridha
Suwito Pomalingo
Arief Yanto Rukmana
Angga Aditya Permana
Abdurohim
Raimon Efendi
Bambang Suprayogi
Adi Heri
Shah Khadafi

GET PRESS INDONESIA

PENGENALAN JARINGAN KOMPUTER

Penulis :
Agung Susilo Yuda Irawan
Zen Munawar
Anindya Khrisna Wardhani
Arip Solehudin
Azhari Ali Ridha
Suwito Pomalingo
Arief Yanto Rukmana
Angga Aditya Permana
Abdurohim
Raimon Efendi
Bambang Suprayogi
Adi Heri
Shah Khadafi

ISBN :

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

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

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

Cetakan pertama, September 2023

KATA PENGANTAR

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

Buku ini membahas Pengantar pengenalan jaringan komputer, Dasar-dasar Switch L2 dan konfigurasi end devices, Protokol-protokol dan pemodelan jaringan komputer, Perangkat Keras/Physical Layer, Sistem Bilangan, Lapisan Data Link, Ethernet Switching, Lapisan jaringan/ Network Layer, Resolusi pengalamatan/Address Resolution, Konfigurasi Dasar Router, Pengalamatan IPv4, *Internet Control Message Protocol* (ICMP), Lapisan Transport.

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

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

Padang, September 2023

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB 1
PENGANTAR PENGENALAN JARINGAN KOMPUTER

Oleh Agung Susilo Yuda Irawan

1.1 Pendahuluan

Pada era digital saat ini, jaringan komputer memainkan peran yang sangat penting dalam hampir semua aspek kehidupan. Dari bisnis hingga pendidikan, dari komunikasi hingga hiburan, jaringan komputer menjadi tulang punggung infrastruktur yang menghubungkan orang, perangkat, dan informasi di seluruh dunia. Seiring dengan pertumbuhan pesat teknologi informasi, pemahaman tentang jaringan komputer menjadi keterampilan yang tak terelakkan.

Menurut Beasley dan Nilson dalam penelitian mereka mengenai pentingnya pemahaman jaringan komputer, "Pengenalan jaringan komputer memungkinkan kita memahami dasar-dasar teknologi yang menghubungkan dunia digital. Hal ini membantu kita mengoptimalkan kinerja jaringan, meningkatkan keamanan, dan memberikan layanan yang andal bagi pengguna" (Beasley & Nilson, 2018, hal. 25).

Pentingnya mempelajari jaringan komputer juga ditekankan oleh Tanenbaum dan Wetherall, yang menyatakan bahwa "Jaringan komputer adalah fondasi bagi komunikasi modern. Memahami konsep dan prinsip dasar jaringan komputer memberikan dasar yang kokoh dalam membangun, mengelola, dan memecahkan masalah jaringan yang kompleks" (Tanenbaum & Wetherall, 2011, hal. 2).

Buku ini bertujuan untuk memberikan pengantar yang komprehensif dan mudah dipahami mengenai jaringan komputer. Melalui pembahasan tentang konsep dasar, model referensi OSI, komponen jaringan, topologi, protokol, keamanan, dan manajemen, diharapkan pembaca dapat memperoleh pemahaman yang solid tentang jaringan komputer.

Dalam bab-bab berikutnya, kita akan mengeksplorasi berbagai aspek jaringan komputer dengan penjelasan yang jelas dan contoh praktis. Buku ini juga menyajikan diskusi tentang tren terkini, tantangan, dan peluang dalam pengelolaan jaringan komputer.

Melalui pemahaman yang mendalam tentang jaringan komputer, diharapkan pembaca dapat memanfaatkan teknologi ini dengan lebih efektif dan menghadapi berbagai perubahan yang terus terjadi di dunia digital.

1.2 Definisi Jaringan Komputer

Jaringan adalah kumpulan perangkat komputer yang saling terhubung untuk bertukar informasi dan sumber daya. Dalam konteks jaringan komputer, perangkat tersebut dapat berupa komputer, server, printer, router, switch, dan perangkat lainnya yang terhubung melalui kabel tembaga, serat optik, atau teknologi nirkabel. Tujuan utama dari jaringan komputer adalah untuk memungkinkan berbagi data, perangkat, dan layanan di antara pengguna dalam jaringan.

Definisi jaringan komputer mencakup konsep penghubung antara perangkat-perangkat tersebut melalui media transmisi seperti kabel atau gelombang elektromagnetik. Jaringan juga melibatkan penggunaan protokol komunikasi yang standar, seperti protokol TCP/IP, yang memungkinkan perangkat dalam jaringan untuk saling berkomunikasi dan bertukar informasi secara efisien.

Jaringan komputer dapat memiliki berbagai ukuran dan cakupan. Jaringan lokal (*Local Area Network*/LAN) mencakup area

terbatas, seperti dalam suatu gedung atau kantor, sedangkan jaringan luas (*Wide Area Network*/WAN) mencakup area yang lebih luas, bahkan mencakup kota, negara, atau bahkan seluruh dunia. Selain itu, ada juga jaringan metropolitan (*Metropolitan Area Network*/MAN) yang menghubungkan beberapa area dalam suatu kota atau wilayah.

Pentingnya jaringan komputer terletak pada kemampuannya untuk meningkatkan efisiensi dan produktivitas. Dengan jaringan, pengguna dalam suatu organisasi dapat berbagi sumber daya seperti file, printer, dan server, serta mengakses informasi dan aplikasi secara bersama-sama. Selain itu, jaringan komputer juga memungkinkan komunikasi yang cepat dan efisien antara pengguna, baik melalui email, pesan instan, atau panggilan suara dan video.

Dalam era digital yang terus berkembang, jaringan komputer menjadi infrastruktur yang tak terpisahkan. Dalam segala aspek kehidupan, baik itu bisnis, pendidikan, pemerintahan, atau kehidupan sehari-hari, jaringan komputer memiliki peran sentral dalam menghubungkan orang, perangkat, dan informasi, membawa dunia menjadi lebih terkoneksi dan terintegrasi.

1.3 Sejarah Perkembangan Jaringan Komputer

Sejarah perkembangan jaringan komputer dimulai dari awal abad ke-19 hingga saat ini, dengan peristiwa dan penemuan yang berperan dalam membentuk dan mengubah wajah komunikasi dan konektivitas. Pada tahun 1837, penemuan telegraf oleh Samuel Morse menjadi tonggak awal komunikasi jarak jauh dengan menggunakan kode Morse. Kemudian, pada tahun 1960-an, Departemen Pertahanan Amerika Serikat mengembangkan ARPANET sebagai jaringan komputer pertama yang menghubungkan beberapa universitas dan lembaga penelitian. ARPANET adalah pendahulu internet modern dan menjadi cikal bakal pengembangan teknologi jaringan komputer.

Pada tahun 1970-an, penemuan Ethernet oleh Robert Metcalfe di Xerox PARC mengenalkan konsep komunikasi berbasis paket dengan metode akses media bersama. Ini menjadi fondasi teknologi yang digunakan dalam jaringan lokal (LAN) dan memungkinkan perangkat untuk berkomunikasi satu sama lain secara efisien (Kurose, 2005).

Selanjutnya, pada tahun 1980-an, TCP/IP (*Transmission Control Protocol*/*Internet Protocol*) dikembangkan oleh Vint Cerf dan Robert Kahn sebagai standar protokol untuk interkoneksi jaringan yang berbeda. Hal ini menjadi kunci dalam membentuk internet modern yang memungkinkan berbagai jaringan komputer saling terhubung (Coner, 1995) .

Perkembangan selanjutnya datang pada tahun 1990-an, ketika *World Wide Web* (WWW) diciptakan oleh Tim Berners-Lee. Dengan memperkenalkan protokol HTTP (*Hypertext Transfer Protocol*) dan HTML (*Hypertext Markup Language*), WWW mengubah internet menjadi platform yang dapat diakses oleh semua orang dengan mudah dan cepat.

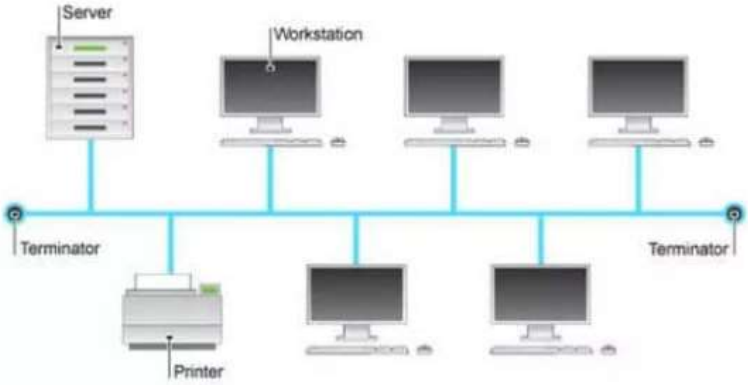
Pada awal abad ke-21, jaringan komputer semakin berkembang pesat dengan kemunculan teknologi nirkabel (*wireless*), seperti Wi-Fi, yang memungkinkan akses internet tanpa perlu kabel fisik. Selain itu, munculnya *Internet of Things* (IoT) memperluas konektivitas dengan memungkinkan perangkat dan objek non-komputer seperti peralatan rumah tangga, kendaraan, dan sensor untuk berkomunikasi melalui internet.

Dalam perkembangannya, jaringan komputer juga menghadapi berbagai tantangan, termasuk keamanan, privasi, dan skalabilitas. Namun, inovasi dan penemuan terus berlanjut untuk meningkatkan performa dan keamanan jaringan komputer, menjadikannya bagian integral dari kehidupan modern (Leiner, 2009).

1.4 Topologi Jaringan

Topologi jaringan mengacu pada susunan fisik atau logis dari perangkat dan kabel dalam suatu jaringan komputer. Pemilihan topologi jaringan sangat penting karena dapat mempengaruhi performa, keandalan, dan skalabilitas jaringan. Berikut ini beberapa jenis topologi jaringan yang umum digunakan:

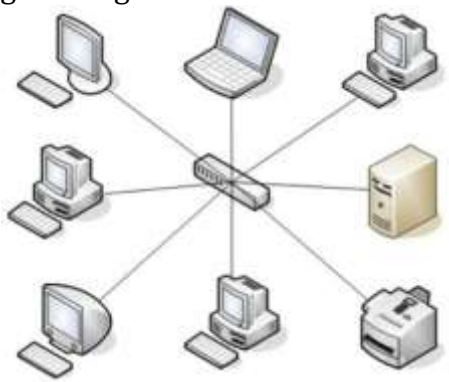
1. Topologi Bus:
   Pada topologi bus, semua perangkat terhubung ke sebuah kabel tunggal yang berfungsi sebagai jalur komunikasi. Gambar 1.1 menunjukkan contoh topologi bus. Keuntungan dari topologi ini adalah pengaturan kabel yang relatif sederhana dan hemat biaya. Namun, kelemahannya adalah jika ada gangguan atau kerusakan pada kabel pusat, maka seluruh jaringan dapat terganggu.



Gambar 1.1. Topologi Bus

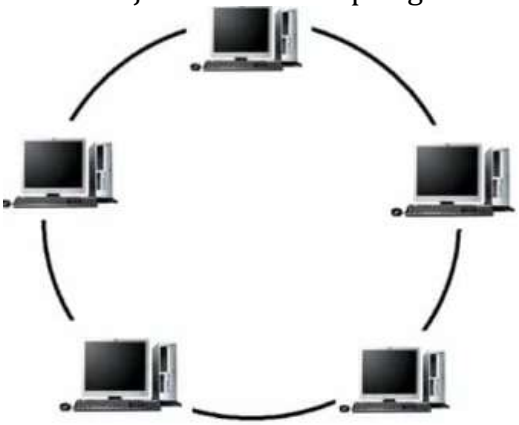
2. Topologi Bintang:
   Dalam topologi bintang, setiap perangkat terhubung langsung ke pusat atau switch sentral. Hal ini membuatnya lebih mudah untuk mengelola dan mengidentifikasi masalah karena gangguan pada salah satu perangkat tidak akan mempengaruhi seluruh jaringan. Namun, topologi ini memerlukan lebih banyak kabel dan switch, sehingga dapat

lebih mahal dalam skala besar. Gambar 1.2 menunjukkan contoh topologi bintang.



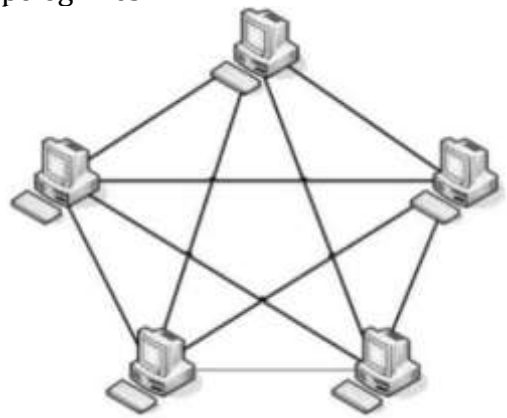
Gambar 1.2. Topologi Bintang

3. Topologi Cincin:
   Dalam topologi cincin, setiap perangkat terhubung dengan dua perangkat lainnya, membentuk lingkaran tertutup. Data bergerak dalam satu arah searah jarum jam melalui setiap perangkat. Topologi cincin memastikan akses ke media bersama secara merata, dan jika satu perangkat mengalami gangguan, data tetap bisa berputar melalui jalur alternatif. Gambar 1.3 menunjukkan contoh topologi cincin.



Gambar 1.3. Topologi Cincin

4. Topologi Mesh:
   Topologi mesh melibatkan setiap perangkat yang terhubung langsung ke semua perangkat lain dalam jaringan. Ini memastikan redundansi dan keandalan tinggi karena setiap perangkat memiliki jalur komunikasi alternatif jika ada perangkat lain yang mengalami gangguan. Namun, topologi mesh memerlukan jumlah kabel dan port yang besar, sehingga biaya implementasinya tinggi. Gambar 1.4 menunjukkan contoh topologi mesh.



Gambar 1.4. Topologi Mesh

Setiap jenis topologi memiliki kelebihan dan kelemahan, dan pemilihan topologi harus disesuaikan dengan kebutuhan dan karakteristik jaringan. Selain topologi yang disebutkan di atas, ada juga topologi lain seperti topologi pohon dan topologi hibrida yang merupakan kombinasi dari beberapa topologi.

1.5 Media Transmisi

Media transmisi dalam jaringan komputer adalah jalur fisik atau nirkabel yang digunakan untuk mengirimkan data antara perangkat dalam jaringan (Firmansyah, 2014). Pemilihan media transmisi yang tepat sangat penting karena dapat mempengaruhi

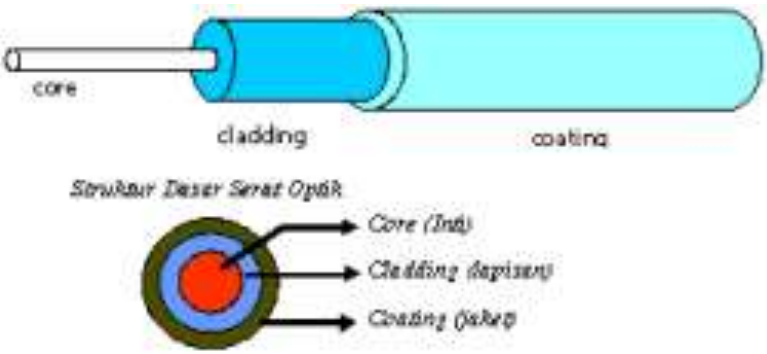
kecepatan, jangkauan, dan keandalan transmisi data (Purbawanto, 2020). Beberapa jenis media transmisi yang umum digunakan adalah sebagai berikut:

Kabel Tembaga:

Kabel tembaga merupakan media transmisi yang umum digunakan dalam jaringan komputer. Jenis kabel tembaga yang paling populer adalah twisted-pair dan coaxial. Kabel twisted-pair terdiri dari dua atau lebih kawat tembaga yang saling dijalin, seperti kabel UTP (*Unshielded Twisted Pair*) dan STP (*Shielded Twisted Pair*). Kabel ini banyak digunakan untuk jaringan LAN karena harganya yang ekonomis dan mudah dipasang. Sementara itu, kabel coaxial menggunakan konduktor tembaga di tengahnya yang dilapisi oleh lapisan isolasi dan perisai. Kabel ini sering digunakan untuk menghubungkan perangkat pada jarak yang lebih jauh dan memiliki kecepatan transmisi yang lebih tinggi daripada twisted-pair.

Serat Optik:

Serat optik menggunakan cahaya sebagai medium untuk mengirimkan data dengan sangat cepat dan aman. Serat optik terdiri dari serat kaca yang mampu menghantarkan sinyal cahaya dengan kecepatan tinggi. Serat optik memiliki keuntungan karena dapat mentransmisikan data dalam jarak yang jauh dengan kehilangan sinyal yang minimal dan bebas dari gangguan elektromagnetik (Ananto dkk, 2011). Namun, serat optik lebih mahal daripada kabel tembaga dan memerlukan penanganan khusus saat instalasi.



Gambar 1.5. Kabel Serat Optic

Media Nirkabel:

Media transmisi nirkabel menggunakan gelombang elektromagnetik untuk mentransmisikan data melalui udara. Wi-Fi merupakan contoh media nirkabel yang banyak digunakan untuk menghubungkan perangkat secara nirkabel ke jaringan. Teknologi nirkabel terus berkembang, dan ada berbagai standar, seperti 802.11ac dan 802.11ax, yang meningkatkan kecepatan dan jangkauan jaringan nirkabel.

Keputusan untuk menggunakan media transmisi tertentu tergantung pada kebutuhan jaringan, jarak transmisi, dan anggaran. Beberapa pertimbangan penting termasuk kecepatan transmisi yang diinginkan, ketahanan terhadap gangguan, dan fleksibilitas dalam pengaturan jaringan.

1.6 Perangkat Jaringan

Dalam jaringan komputer, perangkat jaringan berperan sebagai elemen kunci dalam mengatur, menghubungkan, dan mengoordinasi komunikasi antara perangkat di dalam jaringan. Beberapa perangkat jaringan utama yang sering digunakan dalam jaringan modern adalah switch, router, dan access point.

Switch: Switch adalah perangkat jaringan yang berfungsi sebagai penghubung antara berbagai perangkat dalam jaringan

lokal (LAN). Ketika perangkat seperti komputer, printer, atau server terhubung ke switch, switch akan membaca alamat MAC address masing-masing perangkat dan membuat tabel pembelajaran. Ketika switch menerima paket data, ia akan mengirimkan data hanya ke perangkat tujuan yang tepat berdasarkan alamat MAC address yang ada dalam tabelnya. Dengan cara ini, switch mengurangi lalu lintas jaringan dan meningkatkan efisiensi komunikasi antarperangkat di dalam LAN.

Gambar 1.6. Switch

Router: Router adalah perangkat jaringan yang berfungsi untuk menghubungkan dua atau lebih jaringan yang berbeda, seperti menghubungkan LAN dengan internet. Router beroperasi pada lapisan jaringan (*network layer*) dalam model OSI dan menggunakan tabel routing untuk menentukan jalur terbaik untuk mengirimkan paket data antarjaringan. Ketika data datang ke router, router akan membaca alamat IP tujuan dalam paket data dan menggunakan tabel routing untuk menentukan jalur terbaik menuju alamat tujuan tersebut. Router juga berfungsi sebagai firewall dan dapat menerapkan kebijakan keamanan untuk melindungi jaringan dari serangan dan ancaman yang tidak diinginkan dari luar.

Gambar 1.7. Router

Access Point (AP): *Access point* adalah perangkat yang memungkinkan perangkat nirkabel (seperti laptop atau smartphone) untuk terhubung ke jaringan secara nirkabel. *Access point* berfungsi sebagai titik akses ke jaringan nirkabel, dan ketika perangkat nirkabel terdekat ingin terhubung, *access point* akan mengatur sesi dan memberikan alamat IP untuk perangkat tersebut. Access point juga dapat beroperasi dalam mode jaringan yang berbeda, seperti mode infrastruktur dan mode ad hoc, yang mempengaruhi cara perangkat nirkabel berkomunikasi satu sama lain.

Gambar 1.8. Acces Point

Setiap perangkat jaringan memiliki peran dan fungsi yang unik dalam jaringan. Switch bertanggung jawab untuk menghubungkan perangkat dalam jaringan lokal dan

mengoptimalkan lalu lintas, router berfungsi sebagai penghubung antarjaringan dan menerapkan kebijakan keamanan, dan access point memungkinkan perangkat nirkabel untuk terhubung ke jaringan dengan mudah. Dengan kerjasama perangkat jaringan ini, jaringan dapat beroperasi dengan efisien, aman, dan memberikan konektivitas yang andal (Syafrizal, 2020).

1.7 Model OSI (*Open Systems Interconnection*)

Model OSI (Open Systems Interconnection) adalah sebuah model referensi yang dirancang oleh International Organization for Standardization (ISO) untuk menggambarkan struktur dan fungsi lapisan-lapisan dalam komunikasi jaringan komputer. Model ini menjadi panduan umum bagi para pengembang dan perancang jaringan untuk memahami dan mengintegrasikan perangkat dan perangkat lunak dari berbagai vendor dengan mudah. Tujuan utama dari model OSI adalah untuk memisahkan fungsi-fungsi komunikasi ke dalam lapisan-lapisan terpisah, sehingga memungkinkan para pengembang jaringan untuk bekerja secara independen pada masing-masing lapisan tanpa harus mempengaruhi lapisan lainnya. Model OSI terdiri dari tujuh lapisan, dan setiap lapisan memiliki fungsi yang unik dalam proses komunikasi.

Penjelasan tentang Setiap Lapisan Model OSI:

1. Lapisan Fisik (*Physical Layer*):
   Lapisan fisik adalah lapisan terbawah dalam model OSI yang menangani pengiriman bit-bit data melalui media transmisi fisik seperti kabel tembaga, serat optik, atau gelombang radio. Fungsi utamanya adalah mengatur bentuk sinyal fisik, transmisi, dan penerimaan data. Lapisan fisik menentukan aspek-aspek teknis seperti jenis kabel, konektor, dan metode pengkodean sinyal yang digunakan.

2. Lapisan Data Link (Data Link Layer):
   Lapisan data link beroperasi di atas lapisan fisik dan bertanggung jawab atas pengiriman frame data antara dua perangkat yang terhubung secara langsung. Lapisan ini mengatasi kesalahan dan konflik di lapisan fisik, serta mengatur aliran data. MAC (*Media Access Control*) address digunakan dalam lapisan ini untuk mengidentifikasi perangkat di dalam satu jaringan lokal.
3. Lapisan Jaringan (*Network Layer*):
   Lapisan jaringan berfokus pada pengiriman paket data dari sumber ke tujuan melalui jaringan yang berbeda. Fungsi utamanya adalah mengatur alamat IP dan menentukan jalur terbaik (routing) untuk mengirimkan paket data dari satu jaringan ke jaringan lainnya.
4. Lapisan Transport (*Transport Layer*):
   Lapisan transport bertanggung jawab atas pengiriman data yang andal dan dapat dipulihkan antara dua perangkat. Lapisan ini menyediakan mekanisme pengiriman yang terjamin, seperti koreksi kesalahan dan kontrol aliran, sehingga memastikan data sampai dengan benar dan tanpa kesalahan.
5. Lapisan Sesi (*Session Layer*):
   Lapisan sesi menyediakan dan mengelola koneksi antara dua perangkat yang berkomunikasi. Fungsi lapisan ini mencakup pembentukan, pemeliharaan, dan pengakhiran sesi, serta menyediakan sinkronisasi antara aplikasi yang berkomunikasi.
6. Lapisan Presentasi (*Presentation Layer*):
   Lapisan presentasi mengatur format data dan mengubah struktur data agar dapat dimengerti oleh perangkat penerima. Fungsi lapisan ini meliputi enkripsi, kompresi, dan konversi antarmuka data.

7. Lapisan Aplikasi (*Application Layer*):
   Lapisan aplikasi adalah lapisan tertinggi dalam model OSI yang berinteraksi langsung dengan aplikasi pengguna. Lapisan ini menyediakan layanan untuk aplikasi seperti email, web browsing, dan transfer file.

Gambar 1.9. Model OSI (*Open Systems Interconnection*)

Setiap lapisan model OSI berfungsi secara terpisah namun saling bergantung satu sama lain dalam proses komunikasi jaringan. Dengan pemisahan fungsi ke dalam lapisan-lapisan ini, model OSI memudahkan para pengembang jaringan dalam merancang, mengelola, dan memperbaiki jaringan komputer secara efisien (Zimmerman, 1980).

DAFTAR PUSTAKA

Beasley, M., & Nilson, K. 2018. Introduction to Computer Networking. Pearson.

Tanenbaum, A. S., & Wetherall, D. J. 2011. Computer Networks. Pearson.

Kurose, J.F., 2005. Computer networking: A top-down approach featuring the internet, 3/E. Pearson Education India.

Coner, D.E., 1995. Internetworking with TCP/IP: principles, protocols, and architecture. Prentice Hall.

Leiner, B.M., Cerf, V.G., Clark, D.D., Kahn, R.E., Kleinrock, L., Lynch, D.C., Postel, J., Roberts, L.G. and Wolff, S., 2009. A brief history of the Internet. ACM SIGCOMM computer communication review, 39(5), pp.22-31.

https://diskominfo.kuburayakab.go.id

Firmansyah, R. 2014. Rancang bangun jaringan komputer dengan kabel listrik sebagai media transmisi untuk komunikasi data. Jurnal Informatika, 1(2).

Ananto, B., Darjat, D., & Setiyono, B. 2011. Simulasi perambatan cahaya pada serat optik (Doctoral dissertation, Jurusan Teknik Elektro Fakultas Teknik).

Syafrizal, M. 2020. Pengantar jaringan komputer. Penerbit Andi.

Zimmermann, H. 1980. OSI reference model-the ISO model of architecture for open systems interconnection. IEEE Transactions on communications, 28(4), 425-432.

BAB 2
DASAR-DASAR SWITCH L2 DAN KONFIGURASI END DEVICES

Oleh Zen Munawar

2.1 Pendahuluan

Meningkatnya permintaan untuk jaringan berkinerja tinggi yaitu throughput tinggi dan penundaan rendah secara end-to-end, tingkat keadilan dalam mengakses bandwidth saluran yang tersedia di antara pengguna aktif di jaringan, dan kualitas penyediaan layanan telah menantang peneliti jaringan. untuk merancang arsitektur jaringan yang mampu memberikan layanan berkualitas tinggi kepada pengguna akhir (Sarkar, Byrne and Al-Qirim, 2006). Desain infrastruktur jaringan menjadi bagian penting bagi beberapa organisasi teknologi informasi beberapa tahun terakhir. Pertimbangan desain jaringan yang penting untuk jaringan saat ini adalah menciptakan potensi untuk mendukung perluasan di masa depan; jaringan yang handal dan terukur. Ini mengharuskan perancang untuk menentukan situasi unik klien, khususnya teknologi, aplikasi, dan arsitektur data saat ini. Teknologi berkembang pesat terutama setelah penggunaan jaringan nirkabel (Iswanto *et al.*, 2022). Perkembangan teknologi tidak terlepeas dari peran penggunaan big data. Big data dapat didefinisikan sebagai data dalam jumlah besar, baik terstruktur maupun tidak terstruktur, biasanya disimpan di awan (Munawar *et al.*, 2023). Prespektif teknologi informasi terus berubah. Sejumlah besar teknologi informasi tersedia untuk digunakan oleh organisasi dan rangkaian itu terus bertambah. Pemanfaatan Teknologi

Informasi digunakan seperti layanan aplikasi pada smartphone dan aplikasi berbasis web, dan penggunaan big data (Munawar, 2021).

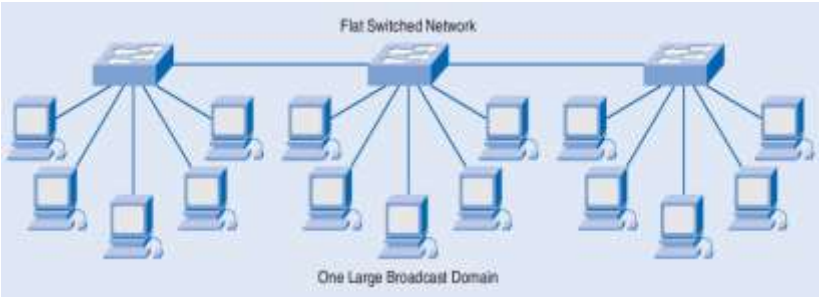
Investasi teknologi informasi yang tinggi dan laju perubahan teknologi yang cepat (Putri, Fudsyi, *et al.*, 2021). Ada banyak jenis desain jaringan yang menyediakan ketersediaan tinggi, fleksibilitas, skalabilitas, dan pengelolaan. Desain dari setiap opsi tergantung pada fungsionalitas yang tersedia di node jaringan dan juga dapat divariasikan oleh perancang atau arsitek jaringan untuk mencapai kinerja optimal dalam jaringan tertentu, atau terkadang untuk mengurangi biaya desain. Desain Top Down adalah disiplin yang tumbuh dari keberhasilan pemrograman perangkat lunak struktur dan analisis sistem terstruktur. Tujuan utama dari analisis sistem terstruktur adalah untuk lebih akurat mewakili kebutuhan pengguna, yang sayangnya sering diabaikan atau disalahartikan. Tujuan lainnya adalah membuat proyek dapat dikelola dengan membaginya menjadi modul-modul yang dapat lebih mudah dipertahankan dan diubah (Oppenheimer, 2012). Ini menyediakan topologi modular blok bangunan yang memungkinkan jaringan berkembang dengan mudah (Choi *et al.*, 2007). Keuntungan *Top Down Network Design* dimulai dengan fokus pada tujuan spesifik organisasi dan persyaratan untuk aplikasi dan layanan jaringan, sambil membiarkan potensi kebutuhan masa depan dipertimbangkan dan diperhitungkan (DiNicolo, 2007).

2.2 Layer 2 Devices Dalam Flat Network

Saat ini, ekonomi berbasis Internet sering menuntut layanan pelanggan sepanjang waktu. Ini berarti jaringan bisnis harus tersedia hampir 100 persen sepanjang waktu. Mereka harus cukup pintar untuk secara otomatis melindungi dari insiden keamanan yang tidak terduga. Jaringan bisnis ini juga harus dapat menyesuaikan diri dengan perubahan beban lalu lintas untuk mempertahankan waktu respons aplikasi yang konsisten. Tidak

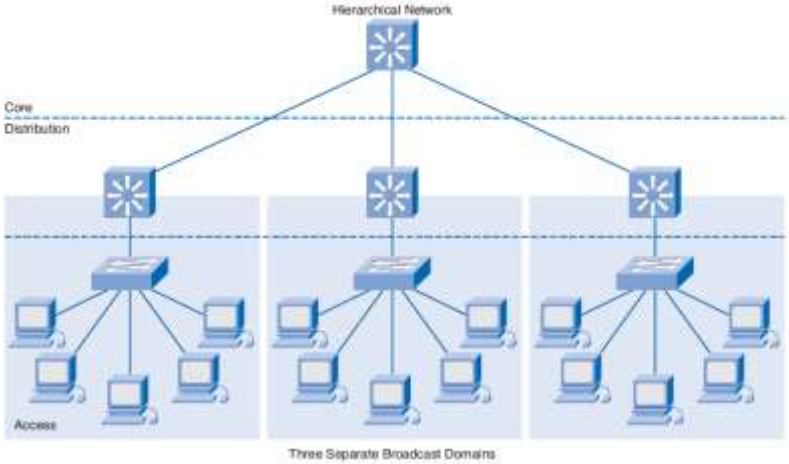
lagi praktis untuk membangun jaringan dengan menghubungkan banyak komponen mandiri tanpa perencanaan dan desain yang matang.

Pendekatan sains desain melibatkan konstruksi dan evaluasi Layanan Later 2 (L2) untuk konektivitasnya ke lapisan akses. Lapisan akses adalah titik masuk pertama ke jaringan untuk perangkat tepi dan stasiun akhir. L2 device dalam flat network memberikan sedikit peluang untuk mengontrol broadcasts atau memfilter lalu lintas yang tidak diinginkan. Semakin banyak device dan aplikasi ditambahkan ke flat network, waktu respons menurun hingga jaringan menjadi tidak dapat digunakan. Gambar 2.1 dan Gambar 2.2 menunjukkan keuntungan dari desain jaringan hirarkis versus desain flat network.



Gambar 2.1. Flat Network
Sumber : (Stewart and Adams, 2008)

Jaringan hierarkis memiliki keunggulan dibandingkan desain flat network. Manfaat membagi flat network menjadi blok hierarkis yang lebih kecil dan lebih mudah dikelola adalah lalu lintas lokal tetap lokal. Hanya lalu lintas yang ditujukan untuk jaringan lain yang dipindahkan ke lapisan yang lebih tinggi.



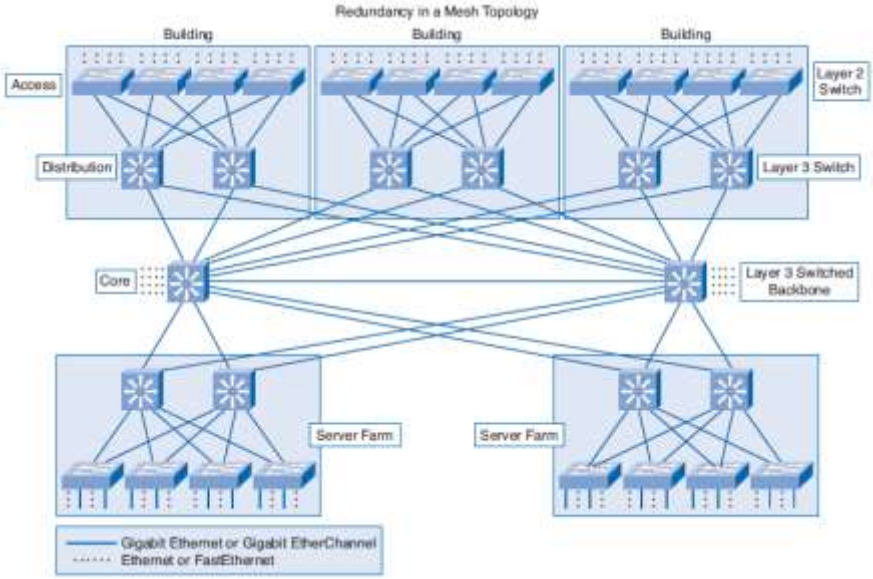
Gambar 2.2. Flat Network
Sumber : (Stewart and Adams, 2008)

2.2.1 Redundant Links

Menerapkan redundant links pada lapisan inti memastikan bahwa perangkat jaringan dapat menemukan jalur alternatif untuk mengirim data jika terjadi kegagalan. Saat perangkat Layer 3 ditempatkan di lapisan inti, tautan redundan ini dapat digunakan untuk penyeimbangan muatan selain menyediakan cadangan. Dalam desain jaringan Layer 2 yang datar, *Spanning Tree Protocol* (STP) menonaktifkan tautan yang berlebihan kecuali jika tautan utama gagal. Perilaku STP ini mencegah penyeimbangan muatan melalui tautan yang berlebihan. Teknologi mempunyai peran penting dalam mengendalikan berbagai kegiatan (Putri, Herdiana, *et al.*, 2021).

Sebagian besar lapisan inti dalam jaringan disambungkan dalam topologi mesh penuh atau sebagian. Topologi full-mesh adalah salah satu di mana setiap perangkat memiliki koneksi ke setiap perangkat lain Gambar 2.3. Meskipun topologi full-mesh memberikan manfaat dari jaringan yang sepenuhnya redundan, mereka bisa sulit untuk dihubungkan dan dikelola dan lebih mahal.

Untuk instalasi yang lebih besar, topologi mesh parsial yang dimodifikasi digunakan.



Gambar 2.3. Redundansi dalam Topologi Mesh
Sumber : (Stewart and Adams, 2008)

Dalam topologi mesh parsial, setiap perangkat terhubung ke setidaknya dua perangkat lainnya, menciptakan redundansi yang cukup tanpa kerumitan mesh penuh.

2.2.2 Perutean Lapisan Distribusi

Lapisan akses umumnya dibangun menggunakan teknologi peralihan Layer 2. Layer distribusi dibangun menggunakan perangkat Layer 3. Router atau switch multilayer, terletak di layer distribusi, menyediakan banyak fungsi penting untuk memenuhi tujuan desain jaringan, termasuk yang berikut: Menyaring dan mengelola arus lalu lintas, Menegakkan kontrol akses, kebijakan, Meringkas rute sebelum mengiklankan rute ke Core, Mengisolasi inti dari kegagalan atau gangguan lapisan akses, Perutean antara

VLAN lapisan akses, Perangkat lapisan distribusi juga digunakan untuk mengelola antrian dan memprioritaskan lalu lintas sebelum transmisi melalui inti.

Trunk links sering dikonfigurasikan antara perangkat jaringan lapisan akses dan distribusi. Trunk digunakan untuk membawa lalu lintas yang dimiliki oleh beberapa VLAN antar perangkat melalui tautan yang sama. Perancang jaringan mempertimbangkan keseluruhan strategi VLAN dan pola lalu lintas jaringan saat merancang tautan batang. Ketika tautan redundan ada di antara perangkat di lapisan distribusi, perangkat dapat dikonfigurasi untuk memuat keseimbangan lalu lintas di seluruh tautan. Tautan yang berlebihan pada lapisan distribusi. Load balancing adalah opsi lain yang meningkatkan bandwidth yang tersedia untuk aplikasi.

2.3 Konfigurasi End Device

End devices (perangkat akhir) adalah perangkat sumber dan tujuan, yang digunakan untuk data yang dikirim melalui jaringan internet apa pun. Untuk menentukan satu perangkat akhir dari yang lain, setiap perangkat akhir pada jaringan ditentukan oleh sebuah alamat. Saat perangkat akhir memulai komunikasi, ia menggunakan alamat perangkat akhir tujuan untuk menentukan ke mana pesan harus dikirim.

Terdapat beberapa jenis perangkat akhir, yaitu: *network device* (perangkat jaringan) seperti Hub, *Repeater, Bridge, Switch, Router, Gateway, dan Brouter*.

2.3.1 Network Device

Perangkat Jaringan: Perangkat jaringan, juga dikenal sebagai perangkat keras jaringan, adalah perangkat fisik yang memungkinkan perangkat keras di jaringan komputer untuk berkomunikasi dan berinteraksi satu sama lain. Misalnya Repeater, Hub, Bridge, Switch, Router, Gateway, Brouter, dan NIC, dll.

Repeater beroperasi pada physical layer. Tugasnya adalah meregenerasi sinyal melalui jaringan yang sama sebelum sinyal menjadi terlalu lemah atau rusak untuk memperpanjang panjang sinyal yang dapat ditransmisikan melalui jaringan yang sama. Poin penting yang perlu diperhatikan tentang repeater adalah bahwa mereka tidak hanya memperkuat sinyal tetapi juga meregenerasinya. Ketika sinyal menjadi lemah, mereka menyalinnya sedikit demi sedikit dan meregenerasinya di konektor topologi bintangnya yang terhubung mengikuti kekuatan aslinya. Ini adalah perangkat 2-port.

Hub pada dasarnya adalah repeater multi-port. Hub menghubungkan beberapa kabel yang berasal dari cabang yang berbeda, misalnya konektor pada topologi bintang yang menghubungkan stasiun yang berbeda. Hub tidak dapat memfilter data, sehingga paket data dikirim ke semua perangkat yang terhubung. Dengan kata lain, collision domain dari semua host yang terhubung melalui Hub tetap satu. Juga, mereka tidak memiliki kecerdasan untuk menemukan jalur terbaik untuk paket data yang mengarah pada inefisiensi dan pemborosan.

Bridge beroperasi pada lapisan data link. Sebuah bridge adalah pengulang, dengan menambahkan fungsi pemfilteran konten dengan membaca alamat MAC dari sumber dan tujuan. Ini juga digunakan untuk menghubungkan dua LAN yang bekerja pada protokol yang sama. Ini memiliki input tunggal dan port output tunggal, sehingga menjadikannya perangkat 2 port.

Switch adalah jembatan multiport dengan penyangga dan desain yang dapat meningkatkan efisiensinya (sejumlah besar port menyiratkan lebih sedikit lalu lintas) dan kinerja. Switch adalah perangkat lapisan tautan data. Switch dapat melakukan pemeriksaan kesalahan sebelum meneruskan data, yang membuatnya sangat efisien karena tidak meneruskan paket yang memiliki kesalahan dan meneruskan paket yang baik secara

selektif ke port yang benar saja. Dengan kata lain, *switch* membagi *domain collision* dari host, tetapi *domain broadcast* tetap sama.

2.3.2 Konfigurasi dan Mengatur End Device

Dalam aktivitas ini, akan membuat jaringan packet tracer sederhana dan menyelesaikan konfigurasi dasar perangkat akhir (Shadit, 2022). Langkah-langkah untuk mengonfigurasi dan mengatur *end device di Cisco Packet Tracer*, seperti terlihat pada tabel di bawah ini :

Tabel 2.1. Device, Model dan Jumlah

No	Device	Nama Model	Jumlah
1.	PC	PC	2
2.	Switch	PT-Switch	1
3.	Server	PT-Server	1

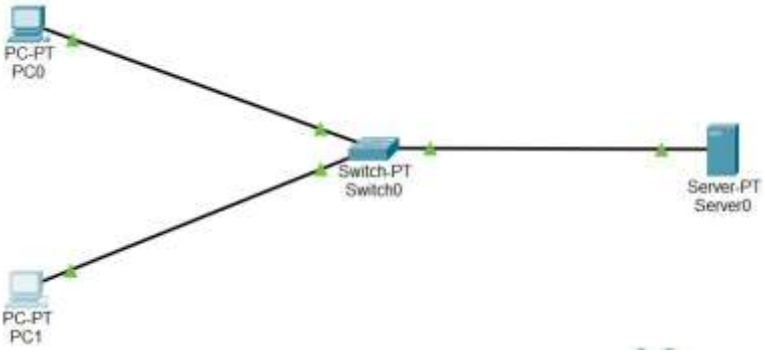
Selanjutnya lakukan tabel pengalamatan Ip, seperti terlihat pada tabel dibawah ini :

Tabel 2.2. Device, Model dan Jumlah

No	Device	IPv4 Address	Subnet Mask
1.	Server0	192.168.1.1	255.255.255.0
2.	PC0	192.168.1.2	255.255.255.0
3.	PC1	192.168.1.3	255.255.255.0

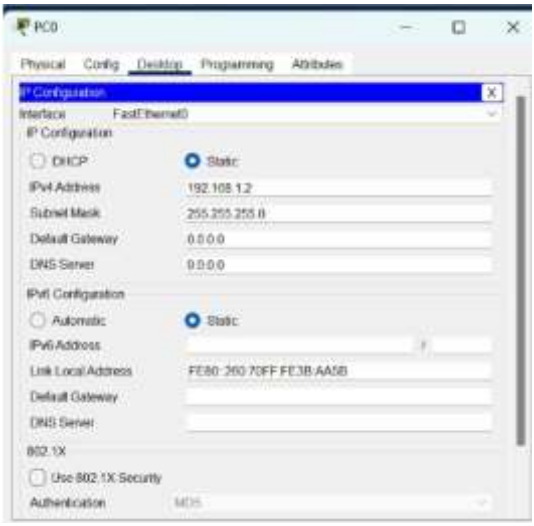
Kemudian, buat topologi jaringan seperti gambar di bawah ini. Gunakan kabel penghubung Otomatis untuk menyambungkan perangkat dengan yang lain.

Perhatikan gambar pada gambar 2.4.



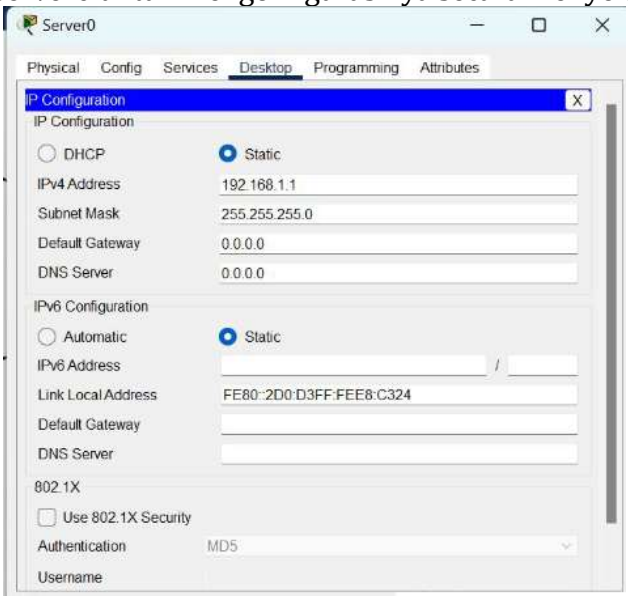
Gambar 2.4. Membangun Topologi 3 Device
Sumber : (Shadit, 2022)

Selanjutnya konfigurasikan PC (*host*) dan server dengan alamat IPv4 dan Subnet Mask sesuai dengan tabel pengalamatan IP di atas. Untuk menetapkan alamat IP di PC0, klik PC0.



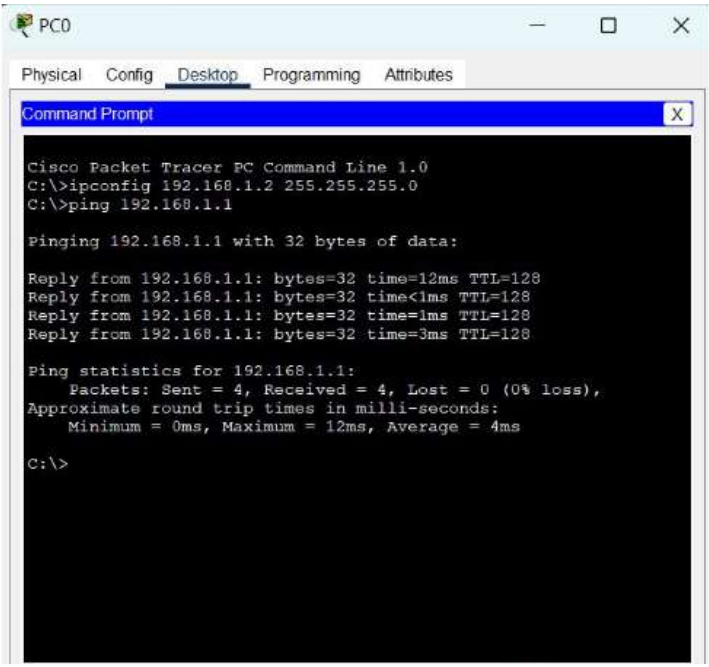
Gambar 2.5. Konfigurasi PC IP 192.168.1.2 dan Server
Sumber : (Shadit, 2022)

Kemudian, pergi ke konfigurasi desktop dan IP dan di sana Anda akan menemukan konfigurasi IPv4. Isi alamat IPv4 dan subnet mask. Demikian pula, ulangi prosedur yang sama dengan PC1 dan server0 untuk mengonfigurasinya secara menyeluruh.



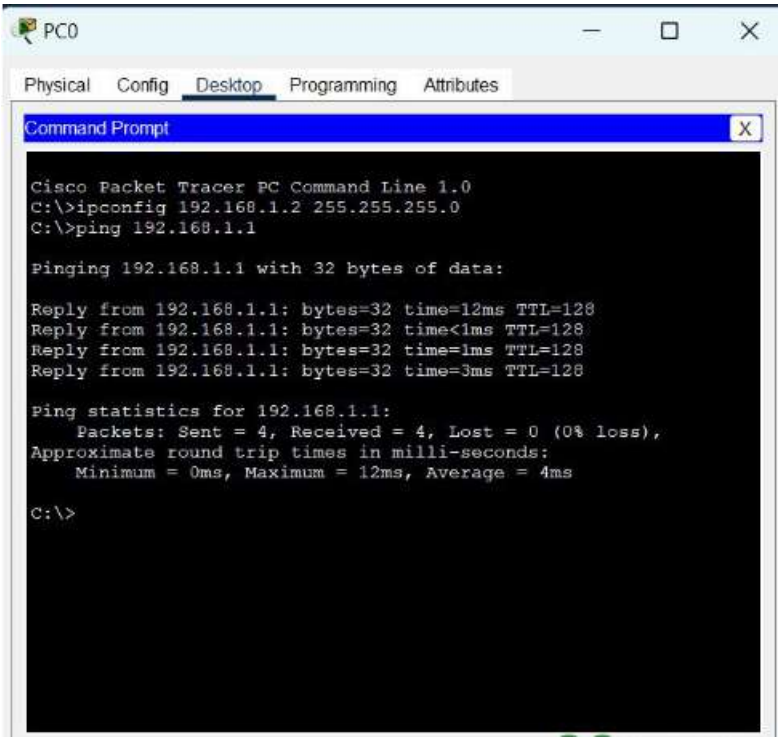
Gambar 2.6. Konfigurasi PC dan Server IP 192.168.1.1
Sumber : (Shadit, 2022)

Juga, kita dapat Menetapkan alamat IP menggunakan perintah ipconfig, atau kita juga dapat menetapkan alamat IP dengan bantuan perintah.
Menuju ke terminal perintah PC.
Lalu, ketik ipconfig <IPv4 address><subnet mask><default gateway>(bila perlu)
Contoh: ipconfig 192.168.1.2 255.255.255.0



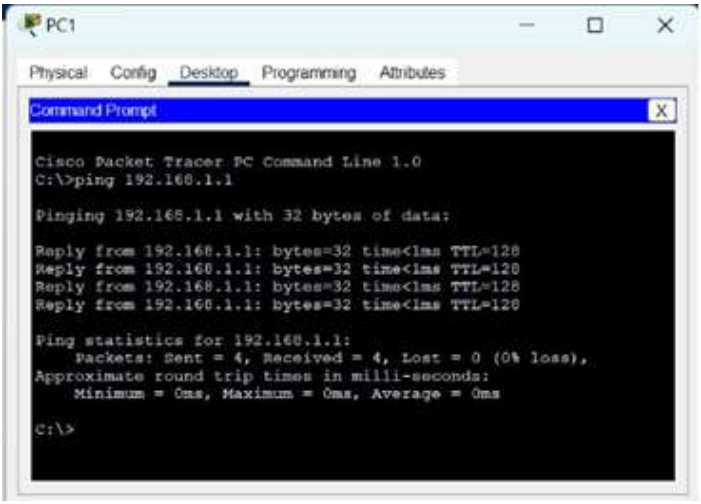
Gambar 2.7. Menetapkan alamat IP dengan ipconfig
Sumber : (Shadit, 2022)

Pada langkah ketiga, lakukan verifikasi koneksi dengan melakukan ping ke alamat IP dari semua host di PC0. Gunakan perintah ping untuk memverifikasi koneksi. Selanjutnya akan memeriksa apakah akan mendapatkan balasan atau tidak. Di sini akan mendapat balasan dari node yang ditargetkan di kedua PC. Jadi, koneksi diverifikasi.



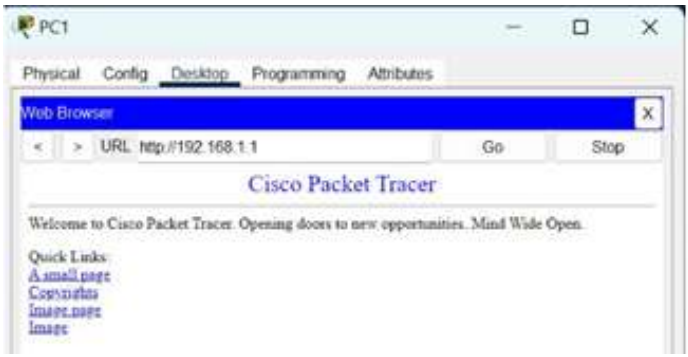
Gambar 2.8. Verifikasi Koneksi Dengan Perintah Ping PC0
Sumber : (Shadit, 2022)

Terlihat ada balasan dari node, maka koneksi akan terverifikasi lakukan verifikasi koneksi dengan melakukan ping ke alamat IP dari semua host di PC1. Selanjutnya menggunakan perintah ping untuk memverifikasi koneksi. Maka akan diperiksa apakah akan mendapatkan balasan atau tidak. Di sini akan mendapat balasan dari node yang ditargetkan di kedua PC. Jadi, koneksi diverifikasi.



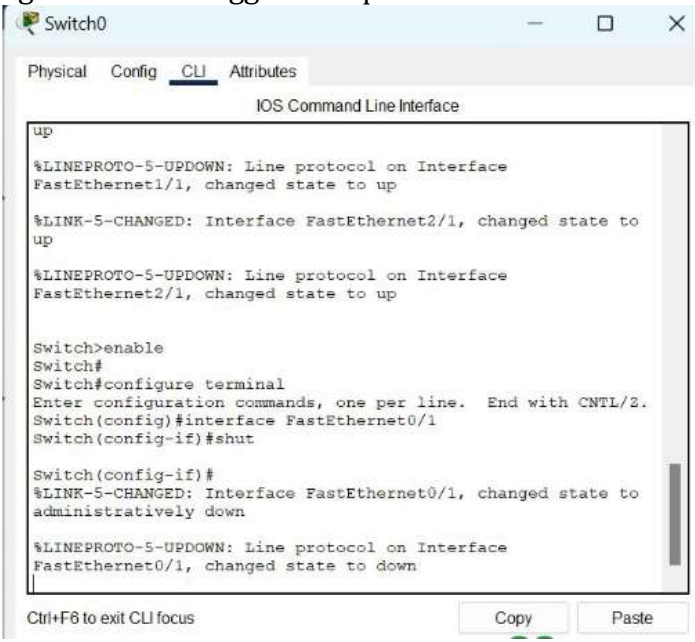
Gambar 2.9. Verifikasi Koneksi Dengan Perintah Ping PC1
Sumber : (Shadit, 2022)

Terlihat ada balasan dari node, maka koneksi akan terverifikasi. Pada langkah 4, lakukan verifikasi server dengan menggunakan browser web di PC1. Seperti yang kita lihat server bekerja sangat baik dan itu menunjukkan hasilnya.

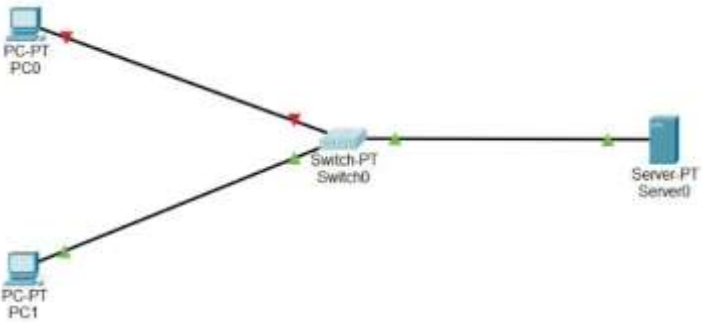


Gambar 2.10. Verifikasi Server dengan Browser di PC1
Sumber : (Shadit, 2022)

Langkah terakhir atau langkah 5: Matikan port FastEthernet 0/1 dengan sakelar menggunakan perintah shutdown.



Gambar 2.11. Mematikan Port FastEthernet 0/1
Sumber : (Shadit, 2022)



Gambar 2.12. Topologi Akhir 3 Device
Sumber : (Shadit, 2022)

DAFTAR PUSTAKA

Choi, B.-Y. *et al.* 2007. 'Outage Analysis of a University Campus Network', in *16th International Conference on Computer Communications and Networks (ICCCN)*. IEEE Explore, pp. 1–7. doi: 10.1109/ICCCN.2007.4317895.

DiNicolo, D. 2007. *Advantages and Disadvantages of Different Network Design Approaches*, *CCDA Study Guide, Network Design*. Available at: https://www.2000trainers.com/ccda-study-guide/comparing-network-design-approaches/ (Accessed: 2 July 2023).

Iswanto *et al.* 2022. 'Pemanfaatan Teknologi Blockchain di Bidang Pendidikan', *Tematik : Jurnal Teknologi Informasi Komunikasi (e-Journal)*, 9(2), pp. 171–181. doi: 10.38204/tematik.v9i2.1082.

Munawar, Z. 2021. 'Manfaat Teknologi Informasi di Masa Pandemi Covid-19', *J-SIKA|Jurnal Sistem Informasi Karya Anak Bangsa*, 3(2), pp. 53–63. Available at: https://ejournal.unibba.ac.id/index.php/j-sika/article/view/692.

Munawar, Z. *et al.* 2023. *Big Data Analytics: Konsep, Implementasi, dan Aplikasi Terkini*. 1st edn. Edited by N. I. Putri. Bandung: Kaizen Media Publishing.

Oppenheimer, P. 2012. *Top-Down Network Design*. 3rd edn. Indiapolis: Cisco Press.

Putri, N. I., Fudsyi, M. I., *et al.* 2021. 'Peran Teknologi Informasi Pada Perubahan Organisasi dan Fungsi Akuntansi Manajemen', *Jurnal Riset Akuntansi dan Bisnis*, 7(2), pp. 47–58. Available at:https://jurnal.plb.ac.id/index.php/JRAK/article/view/625.

Putri, N. I., Herdiana, Y., *et al.* 2021. 'Teknologi Pendidikan dan Transformasi Digital di Masa', *Jurnal ICT: Information Communication & Technology*, 20(7), pp. 53–57. Available at: https://ejournal.ikmi.ac.id/index.php/jict-ikmi/article/view/306/pdf.

Sarkar, N., Byrne, C. and Al-Qirim, N. 2006. 'Gigabit Ethernet Implementation: The Case of a Large New Zealand Organization', *International Journal of Business Data Communications and Networking*, 2(4), pp. 59–77. doi: 10.4018/jbdcn.2006100105.

Shadit. 2022. *How to Configure End Devices on Packet Tracer?*, *Geeks Forgeeks*. Available at: https://www.geeksforgeeks.org/how-to-configure-end-devices-on-packet-tracer/ (Accessed: 2 July 2023).

Stewart, K. D. and Adams, A. 2008. *Designing and Supporting Computer Networks: CCNA Discovery Learning Guide*. 1st edn. Cisco Systems.

BAB 3
PROTOKOL-PROTOKOL DAN PEMODELAN JARINGAN KOMPUTER

Oleh Anindya Khrisna Wardhani

3.1 Pendahuluan

Protokol jaringan merupakan perangkat aturan untuk menentukan cara memformat, mengirim, dan menerima data sehingga sebuah jaringan komputer dapat berkomunikasi meskipun ada perbedaan dalam infrastruktur, desain, atau standar yang mendasarinya(Ananda et al., 2019). Mereka berfungsi sebagai bahasa umum untuk perangkat untuk mengaktifkan komunikasi terlepas dari perbedaan dalam perangkat lunak, perangkat keras, atau proses internal. Protokol jaringan sangat penting untuk komunikasi digital modern, karena memungkinkan pertukaran informasi di internet dan bekerja di belakang layar dengan sangat efektif sehingga banyak pengguna tidak berpikir dua kali tentangnya atau cara kerja internet(Yamafidro et al., 2022).

Pemodelan jaringan komputer melibatkan pembagian konsep jaringan menjadi beberapa lapisan, dengan setiap lapisan diberi tugas tertentu. Arsitektur berlapis dari model jaringan memungkinkan modularitas dan fungsionalitas eksplisit, membuatnya lebih mudah untuk menguji dan memodifikasi perangkat lunak untuk subsistem komunikasi (Romadhondaru & Basuki, 2022).Ada beberapa model jaringan komputer yang berbeda, termasuk model OSI dan model Internet. Model OSI mempartisi aliran data dalam sistem komunikasi menjadi tujuh lapisan abstraksi, masing-masing melayani kelas fungsionalitas ke lapisan di atasnya dan dilayani oleh lapisan di bawahnya (Nesrine

et al., 2019).Model Internet, yang digunakan internet untuk semua komunikasinya, berisi arsitektur empat lapis. Berbagai model yang terkait dengan jaringan berurusan dengan parameter seperti membangun komunikasi antara sistem sumber dan tujuan, mentransmisikan data dengan lancar, dan memastikan bahwa informasi yang dikirim dari sumber mencapai tujuannya dengan paling efisien (Arief *et al.,* 2023).

3.2 Protokol Jaringan

Protokol jaringan berfungsi sebagai bahasa umum untuk perangkat untuk memungkinkan komunikasi, terlepas dari perbedaan dalam perangkat lunak, perangkat keras, atau proses internal(Sopian *et al.,* 2022). Berikut adalah beberapa poin penting tentang protokol jaringan:

1. Protokol jaringan yang terhubung untuk berkomunikasi satu sama lain, memfasilitasi komunikasi digital dan penggunaan internet.
2. Ada ribuan protokol jaringan yang berbeda, masing-masing melakukan salah satu dari tiga tindakan utama: komunikasi, manajemen, atau keamanan.
3. Protokol komunikasi mengatur aturan dan format untuk mentransfer data melalui jaringan, menangani aspek seperti sintaks, semantik, deteksi kesalahan, dan otentikasi.
4. Protokol manajemen menentukan prosedur dan kebijakan yang digunakan dalam manajemen jaringan, memastikan operasi jaringan yang efisien dan efektif.
5. Protokol keamanan memastikan transmisi data yang aman melalui jaringan, melindungi dari akses tidak sah dan menjaga integritas data.
6. Protokol jaringan dikategorikan ke dalam berbagai lapisan model OSI, seperti lapisan aplikasi, lapisan transport, lapisan jaringan, dan lapisan data link.

7. Contoh protokol jaringan yang umum antara lain *Address Resolution Protocol* (ARP), *Border Gateway Protocol* (BGP), *Domain Name System* (DNS), dan *Transmission Control Protocol* (TCP).

Singkatnya, protokol jaringan sangat penting untuk memungkinkan komunikasi antar perangkat dalam jaringan, memastikan transmisi data yang efisien dan aman. Mereka memainkan peran penting dalam komunikasi digital modern dan fungsi internet.

Ada tiga jenis protokol dalam jaringan: komunikasi, manajemen, dan keamanan. Protokol komunikasi menentukan aturan dan format untuk mentransfer data melalui jaringan, sedangkan protokol manajemen menentukan dan menjelaskan berbagai prosedur yang diperlukan untuk mengoperasikan jaringan komputer secara efektif(Wang, 2020). Protokol keamanan, di sisi lain, memungkinkan komunikasi jaringan komputer yang aman dan efisien serta melindungi data, sumber daya, dan jaringan.

Model paling populer untuk protokol jaringan adalah model *Open System Interface* (OSI), yang menunjukkan bagaimana sistem komputer berkomunikasi melalui jaringan. Model tujuh lapis ini memvisualisasikan protokol jaringan membagi proses komunikasi menjadi tugas-tugas terpisah di setiap lapisan model OSI. Untuk mengaktifkan komunikasi jaringan, satu atau lebih protokol beroperasi di setiap lapisan. Misalnya, Protokol Internet (IP) merutekan data dengan mengelola informasi seperti alamat sumber dan tujuan paket data untuk memungkinkan komunikasi jaringan-ke-jaringan (Nesrine et al., 2019).

3.2.1 Fungsi Protokol Jaringan

Di bawah ini adalah beberapa protokol jaringan yang paling umum dan fungsinya :

1. *Address Resolution Protocol* (ARP).
   ARP menerjemahkan alamat IP ke alamat MAC dan sebaliknya sehingga titik akhir LAN dapat berkomunikasi satu sama lain.
2. *Border Gateway Protocol* (BGP).
   BGP digunakan untuk bertukar informasi routing antar jaringan yang berbeda di internet.
3. *Domain Name System* (DNS).
   DNS menerjemahkan nama domain menjadi alamat IP sehingga komputer dapat menemukan sumber daya di internet.
4. *File Transfer Protocol* (FTP).
   FTP digunakan untuk mentransfer file antar komputer di jaringan.
5. *Hypertext Transfer Protocol* (HTTP)
   HTTP digunakan untuk mentransfer data melalui World Wide Web.
6. *Internet Control Message Protocol* (ICMP).
   ICMP digunakan untuk mengirim pesan kesalahan dan informasi operasional tentang kondisi jaringan.
7. *Protokol Manajemen Grup Internet* (IGMP).
   IGMP digunakan untuk mengelola keanggotaan grup multicast.
8. *Simple Mail Transfer Protocol* (SMTP).
   SMTP digunakan untuk mengirim pesan email antar server.
9. Protokol Manajemen Jaringan Sederhana (SNMP).
   SNMP digunakan untuk mengelola dan memantau perangkat jaringan.

10. *Transmission Control Protocol* (TCP).
    TCP digunakan untuk membuat koneksi yang andal antar aplikasi di komputer yang berbeda.
11. *User Datagram Protocol* (UDP).
    UDP digunakan untuk mengirim datagram antar aplikasi di komputer yang berbeda.
12. *Virtual Extensible* LAN (VXLAN).
    VXLAN digunakan untuk membuat jaringan virtual melalui jaringan fisik.

3.2.2 Jenis Protokol Jaringan

Jumlah jaringan komputer yang semakin hari semakin bertambah, membuat protokol jaringan komputer juga memiliki berbagai jenis (Ananda *et al.,* 2019). Beberapa contoh jenis protokol yang tersedia :

1. Protokol Datagram Pengguna (UDP)
   User Packet Protocol adalah transport TCP/IP yang dapat mendukung komunikasi tanpa koneksi dan tidak dapat diandalkan antara host di jaringan. UDP adalah untuk koneksi non-kritis. Contohnya termasuk transmisi audio/video (VoIP dan streaming audio/video). Jenis protokol jaringan ini tidak cocok untuk mengirimkan paket besar karena dapat kehilangan banyak paket.
2. Protokol Kontrol Transmisi dan Protokol Internet (TCP/IP)
   Seperti disebutkan dalam pembahasan UDP, TCP/IP adalah protokol jaringan standar untuk komunikasi data yang banyak digunakan oleh pengguna Internet. Standar TCP/IP ini mendefinisikan proses pertukaran data dari satu komputer ke komputer lain melalui koneksi Internet. Protokol yang cocok untuk pengiriman yang sangat andal seperti HTTP, Telnet, FTP, SSH.

3. HTTPS
   HTTPS muncul saat Anda mengunjungi situs web yang menggunakan SSL. Akan mudah menemukan jenis protokol ini, apalagi sudah banyak website yang menggunakan protokol HTTPS. HTTPS berasal dari *Hypertext Transfer Protocol* (HTTP) yang merupakan protokol yang mengatur komunikasi antara klien dan server. Sedangkan HTTPS merupakan versi yang lebih aman dari HTTP itu sendiri.
   HTTPS dan HTTP masih merupakan protokol yang sama, hanya saja HTTPS merupakan gabungan dari komunikasi HTTP biasa melalui *Transport Layer Security* (TLS) atau *Socket Secure Layer* (SSL). Kombinasi ini dilakukan untuk menjaga keamanan terhadap kemungkinan serangan pihak ketiga. Serangan yang dilakukan biasanya berupa penyadapan informasi dalam komunikasi yang terjadi.

3.3 Pemodelan Jaringan Komputer

Model OSI (*Open System Interconnection*) dan model TCP/IP (*Transmission Control Protocol/Internet Protocol*) merupakan model konseptual yang digunakan untuk menggambarkan komunikasi jaringan(Romadhondaru & Basuki, 2022). Namun, terdapat beberapa perbedaan antara kedua model tersebut, yaitu sebagai berikut:

1. Jumlah Lapisan: Model OSI memiliki tujuh lapisan, sedangkan model TCP/IP memiliki empat lapisan.
2. Kemandirian Protokol: Model OSI adalah standar umum yang tidak tergantung protokol, sedangkan model TCP/IP didasarkan pada protokol standar yang dikembangkan oleh Internet.
3. Pengembangan: Model OSI dikembangkan terlebih dahulu, kemudian protokol dibuat agar sesuai dengan kebutuhan arsitektur jaringan. Sebaliknya, protokol dibuat terlebih dahulu, dan kemudian model TCP/IP dibuat.

4. Layanan: Model OSI mendefinisikan administrasi, antarmuka, dan konvensi serta menjelaskan lapisan mana yang menyediakan layanan. Sebaliknya, model TCP/IP tidak menyebutkan layanan, antarmuka, dan protokol.
5. Kualitas Layanan: Model OSI menyediakan layanan berkualitas, sedangkan model TCP/IP tidak menyediakan layanan berkualitas.
6. Ukuran Header: Header model OSI adalah 5 byte, sedangkan ukuran header TCP/IP adalah 20 byte.
7. Enkapsulasi: Kedua model menggunakan konsep enkapsulasi, tetapi protokol model OSI lebih baik tidak terlihat dan dapat diganti dengan protokol lain yang sesuai dengan cepat. Sebaliknya, protokol model TCP/IP tidak tersembunyi, dan tumpukan protokol baru tidak dapat dipasang di dalamnya.

Singkatnya, model OSI dan model TCP/IP adalah model konseptual yang digunakan untuk menggambarkan komunikasi jaringan. Model OSI memiliki tujuh lapisan, sedangkan model TCP/IP memiliki empat lapisan. Model OSI tidak tergantung protokol dan menyediakan layanan berkualitas, sedangkan model TCP/IP didasarkan pada protokol standar yang dikembangkan oleh Internet dan tidak menyediakan layanan berkualitas. Protokol model OSI lebih baik tidak terlihat dan dapat diganti dengan protokol lain yang sesuai dengan cepat, sedangkan protokol model TCP/IP tidak disembunyikan, dan tumpukan protokol baru tidak dapat dipasang di dalamnya.

3.3.1 Pemodelan Jaringan Komputer

Pada komputer terdapat pula beragam jenis jaringan komputer yang pembagiannya didasarkan pada besar kecilnya cakupan jaringan yang menghubungkan antar komputer.

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

   Local Area Network merupakan jaringan yang terbatas di area yang relatif kecil, biasanya jaringan LAN dibatasi dalam area lingkungan seperti kantor di gedung atau sekolah, dan biasanya tidak jauh dari sekitar 1 kilometer persegi. Secara umum terdapat dua jenis LAN yaitu jaringan *peer-to-peer* dan client-server (Sopian *et al.,* 2022).

   Peer-to-peer yaitu setiap komputer yang terhubung ke jaringan dapat bertindak sebagai komputer pengguna (workstation) atau komputer penyedia layanan (server). Sedangkan Client-Server, hanya ada satu komputer yang bertindak sebagai server dan yang lainnya adalah Klien. Dalam beberapa konfigurasi LAN, komputer biasanya digunakan sebagai file server untuk menampung perangkat lunak yang mengatur operasi jaringan atau sebagai perangkat lunak yang dapat digunakan oleh komputer yang terhubung ke jaringan. Biasanya kapasitas workstation berada di bawah server file dan memiliki aplikasi lain di hard drive selain aplikasi untuk jaringan. Sebagian besar LAN menggunakan kabel untuk menghubungkan satu komputer ke komputer lainnya.

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

   Metropolitan Area Network atau yang biasa disebut MAN merupakan jaringan yang lebih besar dari LAN, misalnya antar wilayah dalam provinsi yang sama. Beberapa jaringan yang menghubungkan jaringan kecil di area lingkungan yang lebih besar, sebagai contoh jaringan perusahaan di mana beberapa cabang perusahaan di kota besar saling terhubung(Arief *et al*., 2023).

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

Wide Area Network (WAN) merupakan jaringan yang bisa dijangkau, biasanya menggunakan satelit atau kabel bawah tanah. WAN menjangkau wilayah geografis yang luas seperti mencakup negara atau benua. Sebagai contoh, dengan menggunakan WAN, sebuah perusahaan di Jakarta dapat menghubungi cabangnya di Singapura hanya dalam beberapa menit. ukuran dan luas komputer yang terhubung tersebut. LAN memiliki jangkauan dari 10m hingga 1km, MAN mencakup 10km dan WAN hingga 100 - 1000km (Romadhondaru & Basuki, 2022).

Secara umum ada tiga macam topologi fisik yang sering digunakan dalam LAN, yaitu:

1. **Topologi Bus**

Topologi bus biasanya menggunakan kabel coax. Seluruh jaringan biasanya merupakan saluran kabel tunggal yang diakhiri di kedua ujungnya oleh Terminator. Keuntungan topologi bus adalah hemat kabel, tata letak kabel sederhana, mudah diperluas. Namun terdapat beberapa kekurangan topologi bus yaitu sangat sedikit deteksi dan isolasi kesalahan, kepadatan lalu lintas data, jika salah satu klien mati, jaringan tidak dapat berfungsi dan diperlukan repeater untuk jarak jauh.

2. **Topologi Ring**

Pada topologi ini, kabel yang digunakan akan membentuk loop tertutup sehingga memberikan kesan loop tak berujung. Secara keseluruhan, tata letak topologi ring juga relatif sederhana. Keuntungan topologi ring adalah hemat kabel. Namun terdapat kekurangan topologi ring yaitu kepekaan terhadap kesalahan dan kesulitan dalam mengembangkan jaringan yang lebih erat (Romadhondaru & Basuki, 2022).

3. Topologi Star

Dalam topologi bintang, setiap node dalam jaringan berkomunikasi melalui hub atau hub. Aliran data dari setiap node akan terlebih dahulu menuju ke hub (HUB) sebelum mencapai node tujuan. Menggunakan topologi jenis ini, mudah memperluas jaringan dengan menarik kabel ke hub/node pusat (Romadhondaru & Basuki, 2022). Keuntungan topologi star adalah paling fleksibel, pemasangan/perubahan stasiun sangat mudah dan tidak mengganggu bagian jaringan lain, kontrol terpusat, kemudahan deteksi dan isolasi kesalahan/kerusakan, kemudahaan pengelolaan jaringan. Namun kelemahan topologi star adalah boros kabel, perlu penanganan khusus dan kontrol terpusat (HUB) jadi elemen kritis. Selain topologi di atas ada beberapa topologi yang ada antara lain topologi mesh dan tree (pohon).

DAFTAR PUSTAKA

Badan Penelitian dan Pengembangan Pemukiman. 2012. 'Modul Rumah Sehat*Kementrian Pekerjaan Umum*, 66, pp. 37–39.

Bogolasky, F. and Ward, P. M. (2018 'Housing, Health, and Ageing in Texas Coloniasand Informal Subdivisions*Current Urban Studies*, 06(01), pp. 70–101. doi: 10.4236/cus.2018.61004.

Dr. Muhammad Ikhtiar. 2018. *Pengantar Kesehatan Lingkungan*.

Keman, S. 2007. 'Enam Kebutuhan Fundamental Perumahan Sehat*Jurnal Kesehatan Lingkungan Unair*, 3(2), p. 3933.

Kemenkes. 2002. 'Syarat - syarat dan pengawasan kualitas air minum.

Kementerian Kesehatan RI. 1990. 'Syarat - syarat dan Pengawasan Kualitas Air. doi: 10.1007/978-1-4684-0955-0_19.

Kementerian Kesehatan RI. 1999. 'KEPMENKES_829_1999.pdf, pp. 1–6.

Krieger, J. and Higgins, D. L. 2002. 'Housing and health: Time again for public health action*American Journal of Public Health*, 92(5), pp. 758–768. doi: 10.2105/AJPH.92.5.758.

Marlinae, L*et al.* 2019. 'Buku Ajar Dasar-Dasar Kesehatan Lingkungan*Fakultas Kedokteran Universitas Lambung Mangkurat Banjarbaru*, pp. 1–120. Available at: http://kesmas.ulm.ac.id/id/wp-content/uploads/2019/02/BUKU-AJAR-DASAR-DASAR-KESEHATAN-LINGKUNGAN.pdf.

Purnama, S. G. 2018. 'Diktat Dasar Kesehatan Lingkungan, pp. 1–97.

Sub-Committee, G. B. C. H. A. C. S. of F. for H. and Health, G. B. M. of (1946 *Report of the Standards of Fitness for Habitation Sub-Committee*. H.M. Stationery Office. Available at: https://books.google.co.id/books?id=hCmlzQEACAAJ.

Undang-Undang No 1 Tahun . 2011. 'Perumahan dan Kawasan Pemukiman.

World Health Organization (WHO). 2010. 'WHO Healthy Workplace Framework and Model. Available at: http://www.ncbi.nlm.nih.gov/pubmed/17514926.

BAB 4
PERANGKAT KERAS/PHYSICAL LAYER

Oleh Arip Solehudin

4.1 Pendahuluan

Perangkat keras atau physical layer merupakan komponen penting dalam suatu jaringan komputer yang memiliki peran krusial dalam melakukan transmisi data secara fisik antara perangkat-perangkat yang terhubung (Iskandar dkk, 2022). Komponen-komponen perangkat keras ini meliputi berbagai elemen seperti kabel, konektor, dan perangkat transmisi lainnya yang memungkinkan transfer data melalui media transmisi yang digunakan.

Dalam konteks jaringan komputer, perangkat keras pada physical layer memainkan peran vital dalam memastikan keandalan dan efisiensi dalam proses transmisi data. Physical layer bertanggung jawab untuk mengirimkan bit-data dari satu perangkat ke perangkat lainnya melalui media transmisi yang digunakan, seperti kabel tembaga, serat optik, atau gelombang radio.

Rangkaian perangkat keras pada physical layer mencakup pengiriman data secara fisik, modulasi sinyal, pengaturan daya, serta pemulihan dan pemrosesan sinyal. Proses ini melibatkan pemilihan dan penyesuaian media transmisi yang sesuai, serta penggunaan teknik dan protokol yang mendukung transmisi data yang andal dan efisien.

Dalam era digital ini, di mana jaringan komputer semakin kompleks dan data yang ditransmisikan semakin besar, penting untuk memiliki perangkat keras yang andal dan efisien pada physical layer. Pengembangan teknologi perangkat keras terus berlanjut untuk meningkatkan kecepatan, kapasitas, dan keandalan transmisi data.

4.2 Pengantar Physical Layer

Perangkat keras atau physical layer memainkan peran yang sangat penting dalam jaringan komputer modern. Kita akan menjelajahi secara rinci konsep dan fungsi dari physical layer serta pentingnya perangkat keras dalam memfasilitasi transmisi data yang efisien dan andal. Membahas komponen utama yang terlibat dalam physical layer, perannya dalam memastikan konektivitas yang stabil antara perangkat, dan bagaimana media transmisi berperan dalam transfer data. Buku ini ditujukan untuk memberikan pemahaman yang komprehensif tentang perangkat keras pada physical layer, serta mengikuti perkembangan terkini dalam teknologi jaringan yang relevan.

Dalam bab ini, kita akan memulai dengan mendefinisikan dan memahami tujuan dari physical layer dalam konteks jaringan komputer. Physical layer bertindak sebagai jembatan antara perangkat keras dan media transmisi yang digunakan. Kami juga akan menjelaskan peran penting physical layer dalam menjaga keandalan dan efisiensi transmisi data di seluruh jaringan (Komputer, 2006). Selanjutnya, kita akan menjelajahi komponen-komponen utama dalam perangkat keras physical layer, seperti kabel, konektor, dan perangkat transmisi lainnya. Memahami peran dan fungsi setiap komponen ini akan membantu kita mengenali bagaimana mereka bekerja secara bersama-sama untuk mengirimkan data dengan baik.

Selain itu, kita akan mempelajari ragam media transmisi yang digunakan dalam physical layer. Kabel tembaga, serat optik, dan teknologi nirkabel seperti gelombang radio adalah beberapa contoh media transmisi yang umum digunakan. Kami akan membahas karakteristik, keuntungan, dan keterbatasan dari masing-masing media ini, serta pertimbangan penting dalam pemilihan media transmisi yang sesuai dengan kebutuhan jaringan.

4.2.1 Definisi dan Tujuan Physical Layer

Physical layer dalam jaringan komputer merujuk pada tingkat terbawah dalam model referensi OSI (*Open Systems Interconnection*). Definisi physical layer adalah sebagai lapisan pertama atau lapisan fisik dalam jaringan komputer, yang bertanggung jawab atas transmisi data secara fisik antara perangkat-perangkat yang terhubung (Utomo, 2011).

Tujuan utama dari physical layer adalah untuk mengatur dan mengelola transmisi data dalam bentuk bit-bit melalui media transmisi yang digunakan, seperti kabel tembaga, serat optik, atau gelombang radio. Physical layer bertanggung jawab untuk mengirimkan bit-data dari satu perangkat ke perangkat lainnya dengan menjaga integritas data, kecepatan, dan keandalan transmisi.

Selain itu, *physical layer* juga memiliki tujuan untuk mengkonversi data digital yang dihasilkan oleh perangkat jaringan menjadi sinyal fisik yang sesuai dengan media transmisi yang digunakan. Hal ini melibatkan teknik modulasi sinyal untuk mentransfer data dalam bentuk gelombang elektromagnetik yang dapat diinterpretasikan oleh media transmisi.

Selama proses transmisi, physical layer juga berperan dalam mengatur daya sinyal, menentukan kecepatan transmisi (baud rate), dan menjaga stabilitas sinyal selama perjalanan melalui media transmisi (Huda, 2019). Tujuan lainnya adalah memastikan kesesuaian antara perangkat pengirim dan penerima

serta mendeteksi dan memperbaiki kesalahan yang mungkin terjadi selama transmisi.

Secara keseluruhan, tujuan dari physical layer adalah untuk menyediakan infrastruktur yang handal dan efisien dalam melakukan transmisi data fisik antara perangkat-perangkat jaringan. Dengan demikian, physical layer menjadi fondasi penting dalam jaringan komputer, memungkinkan komunikasi yang efektif dan sukses antara perangkat-perangkat yang terhubung..

4.2.2 Peran penting physical layer dalam jaringan komputer

Physical layer memiliki peran yang sangat penting dalam menjaga keberhasilan komunikasi dan kinerja jaringan komputer. Berikut ini adalah beberapa peran penting physical layer dalam jaringan komputer:

1. **Transmisi Data Fisik**: Physical layer bertanggung jawab atas transmisi data secara fisik antara perangkat-perangkat yang terhubung. Ini melibatkan mengirimkan bit-data dari satu perangkat ke perangkat lainnya melalui media transmisi yang digunakan, seperti kabel tembaga, serat optik, atau gelombang radio (Rahadian Aria, 2014). Keandalan dan efisiensi transmisi data sangat tergantung pada kualitas dan performa perangkat keras pada physical layer.

2. **Modulasi Sinyal**: Physical layer melakukan konversi data digital yang dihasilkan oleh perangkat jaringan menjadi sinyal fisik yang sesuai dengan media transmisi yang digunakan. Teknik modulasi sinyal digunakan untuk mentransfer data dalam bentuk gelombang elektromagnetik yang dapat diinterpretasikan oleh media transmisi (Agustini dkk, 2019). Dalam proses ini, physical layer memastikan bahwa sinyal terkirim dengan tepat dan dapat diinterpretasikan oleh perangkat penerima.

3. **Pengaturan Daya dan Pengukuran Sinyal**: Physical layer mengatur daya sinyal yang dikirimkan melalui media transmisi. Ini melibatkan pengaturan kekuatan sinyal agar sesuai dengan karakteristik media transmisi yang digunakan. Selain itu, physical layer juga melakukan pengukuran dan evaluasi terhadap kualitas sinyal, seperti kekuatan sinyal, tingkat kebisingan, dan parameter sinyal lainnya, untuk memastikan transmisi yang optimal.

4. **Pemulihan dan Pemrosesan Sinyal**: Physical layer bertanggung jawab dalam pemulihan dan pemrosesan sinyal. Ini termasuk deteksi dan koreksi kesalahan yang terjadi selama transmisi data. Physical layer menggunakan teknik deteksi kesalahan seperti *cyclic redundancy check* (CRC) dan teknik koreksi kesalahan seperti *forward error correction* (FEC) untuk memastikan integritas data yang tinggi dan mengurangi dampak kesalahan pada transmisi.

4.2.3 Komponen-komponen utama yang terdapat dalam perangkat keras physical layer

Perangkat keras physical layer terdiri dari beberapa komponen utama yang berperan penting dalam transmisi data fisik dalam jaringan komputer. Berikut ini adalah penjelasan mengenai komponen-komponen utama tersebut :

1. **Kabel**: Kabel merupakan salah satu komponen utama dalam perangkat keras physical layer. Ada berbagai jenis kabel yang digunakan dalam jaringan komputer, seperti kabel tembaga (seperti kabel UTP dan STP) dan kabel serat optik (Rafiudin, R., 2003). Kabel berfungsi sebagai media transmisi yang mengirimkan sinyal data antara perangkat-perangkat yang terhubung dalam jaringan.

2. **Konektor**: Konektor adalah komponen yang digunakan untuk menghubungkan kabel dengan perangkat jaringan seperti switch, router, atau perangkat terminal lainnya. Konektor memastikan sambungan fisik yang kokoh dan dapat mentransmisikan data dengan baik antara kabel dan perangkat (Arius , 2020).

3. **Perangkat Transmisi**: Perangkat transmisi, seperti modem atau transceiver, berperan dalam mengubah sinyal digital menjadi bentuk yang dapat ditransmisikan melalui media transmisi yang digunakan. Perangkat ini melakukan modulasi dan demodulasi sinyal serta mengatur daya dan frekuensi transmisi untuk memastikan transmisi data yang efisien dan andal.

4. **Jembatan atau Repeater**: Jembatan atau repeater digunakan untuk memperkuat sinyal data saat melakukan transmisi melalui kabel atau media transmisi (Rustini, 2021). Komponen ini diperlukan ketika sinyal melemah selama perjalanan melalui jaringan, sehingga memastikan integritas dan kekuatan sinyal tetap terjaga.

5. **Penguji Jaringan**: Penguji jaringan atau network tester adalah perangkat yang digunakan untuk menguji dan menganalisis performa jaringan serta mendeteksi masalah pada kabel, konektor, atau perangkat transmisi lainnya (Alfurqon, 2018). Penguji jaringan membantu dalam pemecahan masalah dan pemeliharaan jaringan dengan memberikan informasi penting tentang kondisi fisik jaringan.

Memahami dan mengelola komponen-komponen utama dalam perangkat keras *physical layer* adalah penting untuk

menjaga keandalan dan performa jaringan komputer. Dengan pemilihan yang tepat, pemasangan yang benar, dan pemeliharaan yang baik terhadap komponen-komponen ini, kita dapat memastikan transmisi data yang andal dan efisien dalam jaringan komputer.

4.2.4 Ragam Media Transmisi yang Digunakan untuk Transfer Data

Media transmisi memainkan peran sentral dalam perangkat keras physical layer untuk mentransmisikan data dalam jaringan komputer. Ada beberapa jenis media transmisi yang digunakan, masing-masing dengan karakteristik unik dan keunggulannya. Berikut ini adalah penjelasan mengenai ragam media transmisi yang digunakan untuk transfer data:

1. **Kabel Tembaga**: Kabel tembaga merupakan salah satu media transmisi yang paling umum digunakan dalam jaringan komputer. Jenis kabel tembaga yang populer termasuk kabel UTP (*Unshielded Twisted Pair*) dan STP (*Shielded Twisted Pair*). Kabel tembaga dapat mentransmisikan data dengan kecepatan yang tinggi dan biayanya relatif lebih terjangkau. Namun, jarak transmisi kabel tembaga cenderung terbatas, dan sinyal dapat mengalami degradasi ketika melewati jarak yang lebih jauh.

2. **Serat Optik**: Serat optik adalah media transmisi yang menggunakan serat kaca atau plastik yang mampu menghantarkan cahaya untuk mentransmisikan data dalam bentuk sinyal optik. Serat optik memiliki kecepatan transmisi yang sangat tinggi dan dapat mengatasi jarak transmisi yang lebih jauh dibandingkan dengan kabel tembaga. Selain itu, serat optik juga memiliki keunggulan keamanan yang tinggi karena tidak mudah terpengaruh oleh gangguan elektromagnetik.

3. **Teknologi Nirkabel**: Teknologi nirkabel menggunakan gelombang radio atau gelombang elektromagnetik lainnya untuk mentransmisikan data secara wireless. Hal ini memungkinkan koneksi jaringan tanpa menggunakan kabel fisik. Contoh teknologi nirkabel termasuk Wi-Fi, Bluetooth, dan teknologi jaringan seluler seperti 4G dan 5G. Teknologi nirkabel sangat fleksibel dan memungkinkan mobilitas yang tinggi, namun kecepatan dan jarak transmisi dapat dipengaruhi oleh faktor-faktor lingkungan seperti kepadatan sinyal dan hambatan fisik.

Setiap media transmisi memiliki keunggulan dan keterbatasannya masing-masing. Pemilihan media transmisi yang tepat harus mempertimbangkan kecepatan transmisi yang dibutuhkan, jarak transmisi, keamanan, dan kondisi lingkungan tempat jaringan diimplementasikan. Kombinasi yang tepat antara media transmisi dapat digunakan dalam jaringan yang kompleks untuk memastikan transfer data yang andal, cepat, dan efisien.

4.3 Prinsip Pengiriman Data Fisik

Pengiriman data fisik merupakan fondasi utama dalam jaringan komputer. Pada bab ini, kita akan menjelajahi prinsip-prinsip penting yang terkait dengan pengiriman data fisik melalui perangkat keras *physical layer*. Beberapa prinsip yang akan kita bahas meliputi konsep dasar pengiriman data fisik, teknik modulasi sinyal, pengaturan daya dan pengukuran sinyal, serta proses pemulihan dan pemrosesan sinyal.

4.3.1 Konsep Dasar Pengiriman Data secara Fisik

Pengiriman data secara fisik merupakan konsep dasar yang menjadi dasar dalam jaringan komputer. Pada bagian ini, kita akan membahas secara rinci tentang konsep dasar pengiriman data fisik melalui perangkat keras physical layer. Beberapa poin penting

yang akan dibahas termasuk pembagian data menjadi unit-unit yang lebih kecil, pengkodean bit-bit data, dan pengemasan data dalam frame atau paket.

Konsep dasar pengiriman data fisik melibatkan langkah-langkah untuk mengubah data digital yang akan dikirimkan melalui jaringan menjadi serangkaian bit-bit yang dapat ditransmisikan melalui media transmisi yang digunakan. Proses ini melibatkan pembagian data menjadi unit-unit yang lebih kecil, seperti frame atau paket. Dalam unit-unit tersebut, data dikodekan menjadi bit-bit yang dapat dihantarkan melalui perangkat keras physical layer.

Pembagian data menjadi unit-unit yang lebih kecil memiliki manfaat penting dalam pengiriman data fisik. Unit-unit tersebut memudahkan pengelompokan dan pengiriman data secara efisien. Selain itu, dengan memecah data menjadi unit-unit terkelompok, kemampuan untuk mendeteksi dan memperbaiki kesalahan dalam transmisi data meningkat. Jika ada kesalahan dalam satu unit, hanya unit tersebut yang perlu dikirim ulang, bukan seluruh data yang dikirim.

Selain pembagian data, pengkodean bit-bit juga menjadi bagian penting dalam pengiriman data fisik. Bit-bit data digital dikodekan menjadi bentuk sinyal fisik yang sesuai dengan media transmisi yang digunakan. Teknik modulasi sinyal digunakan untuk mengubah bit-bit menjadi gelombang elektromagnetik yang dapat ditransmisikan melalui media transmisi. Dalam proses ini, karakteristik sinyal, seperti amplitudo, frekuensi, atau fase, diubah untuk merepresentasikan bit-bit data.

Pengemasan data dalam frame atau paket juga merupakan aspek penting dalam pengiriman data fisik. Data yang akan dikirimkan dikemas dalam unit-unit yang lebih besar, seperti frame atau paket, yang berisi bit-bit data serta informasi tambahan, seperti alamat pengirim dan penerima, deteksi kesalahan, dan informasi kontrol lainnya. Pengemasan data dalam unit-unit ini

membantu dalam mengorganisir dan mengontrol pengiriman data secara efisien dalam jaringan.

4.3.2 Teknik Modulasi Sinyal dalam Transmisi Data

Dalam pengiriman data melalui perangkat keras physical layer, teknik modulasi sinyal memainkan peran penting dalam mentransmisikan data secara efisien melalui media transmisi yang digunakan. Pada bagian ini, kita akan menjelajahi secara mendalam tentang teknik modulasi sinyal, termasuk tujuan, jenis, dan penggunaannya dalam transmisi data.

Tujuan utama dari teknik modulasi sinyal adalah mengubah data digital menjadi bentuk sinyal fisik yang dapat ditransmisikan melalui media transmisi. Data digital yang dihasilkan oleh perangkat jaringan harus diubah menjadi bentuk gelombang elektromagnetik yang sesuai dengan media transmisi yang digunakan. Dalam proses ini, karakteristik sinyal seperti amplitudo, frekuensi, atau fase diubah untuk merepresentasikan bit-bit data.

Ada beberapa jenis teknik modulasi sinyal yang umum digunakan dalam transmisi data:

1. *Amplitudo Shift Keying* (ASK): Pada teknik ASK, amplitudo sinyal dibuat bervariasi untuk merepresentasikan bit-bit data. Nilai amplitudo yang lebih tinggi mewakili nilai logika 1, sedangkan nilai amplitudo yang lebih rendah mewakili nilai logika 0. ASK dapat digunakan dalam transmisi data dengan bandwidth rendah.

2. *Frekuensi Shift Keying* (FSK): Dalam FSK, frekuensi gelombang dibuat bervariasi untuk mewakili bit-bit data. Frekuensi yang berbeda digunakan untuk mewakili nilai logika 1 dan 0. FSK umum digunakan dalam komunikasi wireless dan modems.

3. *Phase Shift Keying* (PSK): PSK menggunakan perubahan fase sinyal untuk merepresentasikan bit-bit data. Perubahan fase yang spesifik digunakan untuk mewakili nilai logika 1 dan 0. PSK dapat digunakan dalam komunikasi digital yang memiliki kecepatan tinggi.

4. *Quadrature Amplitude Modulation* (QAM): QAM menggabungkan modulasi amplitudo dan modulasi fase untuk mengirimkan lebih banyak bit dalam satu waktu. Dalam QAM, amplitudo dan fase sinyal digunakan untuk mewakili beberapa bit-bit data. QAM digunakan dalam komunikasi data dengan kecepatan tinggi, seperti dalam komunikasi digital dan transmisi video.

Setiap teknik modulasi sinyal memiliki kelebihan dan kelemahan tertentu dan cocok untuk berbagai aplikasi. Pemilihan teknik modulasi yang tepat tergantung pada kecepatan transmisi yang diinginkan, kehandalan, dan lingkungan jaringan. Dengan menggunakan teknik modulasi yang tepat, data dapat ditransmisikan dengan akurasi tinggi dan efisiensi yang optimal melalui media transmisi yang digunakan.

4.3.3 Pengaturan Daya dan Pengukuran Sinyal

Pengaturan daya dan pengukuran sinyal adalah aspek penting dalam pengiriman data fisik melalui perangkat keras physical layer. Dalam bagian ini, kita akan menjelajahi lebih lanjut tentang pentingnya pengaturan daya sinyal yang tepat dan pengukuran sinyal yang akurat dalam jaringan komputer.

Pengaturan daya sinyal melibatkan penyesuaian kekuatan sinyal yang dikirimkan melalui media transmisi. Daya sinyal yang dikirimkan harus disesuaikan agar sesuai dengan karakteristik media transmisi yang digunakan. Jika daya sinyal terlalu rendah, maka dapat terjadi degradasi sinyal dan mungkin mengakibatkan

kesalahan pada pengiriman data. Di sisi lain, jika daya sinyal terlalu tinggi, dapat menyebabkan distorsi sinyal dan gangguan pada lingkungan jaringan. Pengaturan daya sinyal yang tepat adalah kunci untuk menjaga keandalan dan kualitas transmisi data.

Pengukuran sinyal juga merupakan bagian penting dalam pengiriman data fisik. Pengukuran sinyal dilakukan untuk memastikan bahwa sinyal tetap dalam rentang yang dapat diterima dan memenuhi standar yang ditetapkan. Beberapa parameter sinyal yang umum diukur termasuk kekuatan sinyal, tingkat kebisingan, dan kualitas sinyal. Pengukuran yang akurat memungkinkan kita untuk mengetahui kondisi sinyal yang sedang ditransmisikan dan memantau kualitas transmisi data dalam jaringan.

Dalam pengaturan daya dan pengukuran sinyal, perangkat jaringan yang dilengkapi dengan fitur pengaturan daya dan pemantauan sinyal sangat penting. Ini memungkinkan administrator jaringan untuk mengatur daya sinyal yang dikirimkan dan memantau kualitas sinyal secara real-time. Selain itu, penguji jaringan atau alat pengukur sinyal dapat digunakan untuk melakukan pengukuran yang lebih rinci dan mendeteksi potensi masalah dalam transmisi data.

4.3.4 Proses Pemulihan dan Pemrosesan Sinyal

Pemulihan dan pemrosesan sinyal merupakan tahapan kritis dalam pengiriman data fisik melalui perangkat keras physical layer. Dalam bagian ini, kita akan menjelajahi proses pemulihan dan pemrosesan sinyal serta pentingnya dalam memastikan integritas data dan keandalan transmisi.

Selama proses transmisi data, sinyal dapat mengalami degradasi, gangguan, atau kehilangan kualitas karena faktor lingkungan atau kesalahan dalam transmisi. Oleh karena itu, physical layer harus dilengkapi dengan mekanisme yang mampu mendeteksi dan memulihkan sinyal yang rusak atau terganggu.

Proses pemulihan sinyal melibatkan penggunaan teknik deteksi kesalahan seperti *cyclic redundancy check* (CRC) untuk mengidentifikasi adanya kesalahan dalam data yang diterima. Jika kesalahan terdeteksi, physical layer dapat mengaktifkan mekanisme pemulihan, seperti pengulangan transmisi data yang rusak atau penggunaan teknik koreksi kesalahan seperti *forward error correction* (FEC) untuk memperbaiki kesalahan tersebut.

Selain pemulihan, pemrosesan sinyal juga diperlukan dalam transmisi data fisik. Pemrosesan sinyal melibatkan manipulasi dan analisis sinyal yang diterima untuk mendapatkan informasi yang berguna. Misalnya, dalam pemrosesan sinyal, sinyal dianalisis untuk mengukur kualitas sinyal, tingkat kebisingan, dan parameter sinyal lainnya. Hal ini memungkinkan physical layer untuk mengambil tindakan yang diperlukan, seperti menyesuaikan daya sinyal atau melakukan perubahan pada pengaturan transmisi untuk memperbaiki atau mempertahankan kualitas transmisi yang baik.

Pemulihan dan pemrosesan sinyal merupakan bagian penting dalam menjaga integritas dan keandalan transmisi data dalam jaringan komputer. Dengan adanya mekanisme pemulihan, kesalahan dalam transmisi dapat dideteksi dan diperbaiki, sehingga meminimalkan dampaknya terhadap integritas data. Selain itu, pemrosesan sinyal yang baik memungkinkan physical layer untuk melakukan pengukuran dan pengendalian yang akurat terhadap transmisi data, sehingga memastikan kualitas transmisi yang optimal.

Dalam jaringan komputer, penting bagi administrator jaringan untuk memahami dan mengelola proses pemulihan dan pemrosesan sinyal dengan baik. Dengan menggunakan teknik deteksi dan koreksi kesalahan yang tepat, serta memantau kualitas sinyal secara teratur, kita dapat memastikan keandalan dan keberhasilan transmisi data melalui perangkat keras *physical layer*.

4.4 Keandalan dan Performa dalam Physical Layer

Keandalan dan performa yang tinggi dalam perangkat keras physical layer sangat penting dalam menjaga kualitas transmisi data dalam jaringan komputer (Hasrul, 2017). Dalam bagian ini, kita akan membahas beberapa faktor yang berkontribusi terhadap keandalan dan performa dalam physical layer, termasuk teknik deteksi dan koreksi kesalahan, pengukuran latensi dan throughput, serta evaluasi kualitas sinyal dan parameter terkait.

4.4.1 Teknik Deteksi dan Koreksi Kesalahan

Dalam perangkat keras *physical layer*, teknik deteksi dan koreksi kesalahan memainkan peran penting dalam menjaga integritas data selama proses transmisi. Dalam bagian ini, kita akan menjelajahi lebih lanjut tentang teknik-deteksi dan koreksi kesalahan, termasuk tujuan, mekanisme, dan penggunaannya dalam memastikan keandalan transmisi data.

Tujuan utama dari teknik deteksi dan koreksi kesalahan adalah untuk mendeteksi keberadaan kesalahan dalam data yang dikirimkan dan memperbaikinya jika diperlukan. Ketika data dikirim melalui jaringan, ada kemungkinan terjadinya gangguan, kehilangan bit, atau kesalahan dalam transmisi. Teknik deteksi dan koreksi kesalahan dirancang untuk mengatasi masalah ini dan menjaga integritas data (Pradana, 2023).

Salah satu teknik deteksi kesalahan yang umum digunakan adalah *cyclic redundancy check* (CRC). Dalam CRC, data dikirim bersama dengan nilai checksum yang dihitung dari data itu sendiri. Penerima akan menghitung kembali checksum dari data yang diterima dan membandingkannya dengan nilai checksum yang dikirim. Jika nilai checksum tidak cocok, itu menandakan adanya kesalahan dalam transmisi.

Selain teknik deteksi kesalahan, teknik koreksi kesalahan juga digunakan untuk memperbaiki data yang rusak atau terganggu selama transmisi. Salah satu teknik koreksi kesalahan yang umum digunakan adalah *forward error correction* (FEC).

Dalam FEC, bit-bit redundant ditambahkan ke data sebelum dikirim. Penerima menggunakan bit-bit redundant ini untuk mendeteksi dan memperbaiki kesalahan dalam data yang diterima.

Dengan adanya teknik deteksi dan koreksi kesalahan yang efektif, kesalahan dalam transmisi data dapat diidentifikasi dan diperbaiki dengan cepat. Hal ini memastikan integritas data yang tinggi dan mengurangi kemungkinan terjadinya kesalahan dalam pengiriman data fisik.

Penggunaan teknik deteksi dan koreksi kesalahan sangat penting dalam berbagai aplikasi, termasuk komunikasi nirkabel, transmisi data jarak jauh, dan komunikasi satelit. Dalam semua situasi ini, ketepatan dan keandalan data sangat penting. Dengan menggunakan teknik deteksi dan koreksi kesalahan yang tepat, kita dapat memastikan keandalan transmisi data fisik dan meminimalkan dampak kesalahan dalam jaringan komputer.

4.4.2 Pengukuran Latensi, Throughput, dan Faktor-faktor yang Mempengaruhinya

Pengukuran latensi*, throughput*, dan faktor-faktor yang mempengaruhinya adalah aspek penting dalam mengevaluasi performa perangkat keras *physical layer* dalam jaringan komputer. Dalam bagian ini, kita akan menjelajahi lebih lanjut tentang pengukuran latensi dan throughput, serta faktor-faktor yang dapat mempengaruhi keduanya (Solehudin, 2017).

Latensi mengacu pada waktu yang diperlukan untuk mengirimkan data dari satu titik ke titik lain dalam jaringan. Latensi dapat terdiri dari beberapa komponen, termasuk waktu yang dibutuhkan untuk mengirimkan data melalui media transmisi, waktu yang dibutuhkan untuk pemrosesan pada perangkat jaringan, dan waktu yang diperlukan untuk pengiriman data dalam bentuk paket melalui jaringan. Pengukuran latensi penting dalam mengevaluasi responsivitas jaringan dan memastikan kinerja yang

baik dalam aplikasi real-time seperti video streaming, gaming, dan panggilan suara.

Throughput mengacu pada jumlah data yang dapat ditransmisikan dalam satu waktu. Pengukuran throughput mengindikasikan seberapa cepat data dapat dikirim melalui perangkat keras physical layer. Throughput yang tinggi menghasilkan transfer data yang lebih cepat dan efisien dalam jaringan. Pengukuran throughput sering kali dinyatakan dalam bit per detik (bps) atau kilobit per detik (Kbps) (Nasir, 2018).

Ada beberapa faktor yang mempengaruhi latensi dan throughput dalam perangkat keras physical layer:

1. **Jarak Transmisi**: Jarak fisik antara pengirim dan penerima dapat mempengaruhi latensi dan throughput. Semakin jauh jarak transmisi, semakin besar kemungkinan terjadi peningkatan latensi dan penurunan throughput.

2. **Jenis Media Transmisi**: Media transmisi yang digunakan, seperti kabel tembaga atau serat optik, dapat mempengaruhi latensi dan throughput. Serat optik, misalnya, cenderung memiliki latensi lebih rendah dan throughput yang lebih tinggi dibandingkan dengan kabel tembaga.

3. **Kecepatan Transmisi**: Kecepatan transmisi data yang digunakan dalam perangkat keras physical layer juga dapat mempengaruhi latensi dan throughput. Kecepatan transmisi yang lebih tinggi dapat menghasilkan latensi yang lebih rendah dan throughput yang lebih tinggi, namun memerlukan perangkat keras yang mendukung kecepatan tersebut.

4. **Tingkat Kebisingan**: Tingkat kebisingan dalam lingkungan jaringan dapat mempengaruhi latensi dan throughput.

Kebisingan elektromagnetik dapat menyebabkan gangguan dan kesalahan dalam transmisi data, yang dapat meningkatkan latensi dan mengurangi throughput.

Dalam merancang dan mengelola jaringan komputer, penting untuk memperhatikan faktor-faktor yang mempengaruhi latensi dan throughput. Dengan memahami dan mengukur latensi dan throughput secara teratur, serta mengoptimalkan faktor-faktor yang mempengaruhi keduanya, kita dapat memastikan kinerja yang baik dan efisiensi dalam perangkat keras physical layer dalam jaringan komputer.

4.4.3 Pengukuran dan evaluasi kualitas sinyal

Pengukuran dan evaluasi kualitas sinyal adalah langkah penting dalam memastikan transmisi data yang andal dan berkualitas tinggi melalui perangkat keras physical layer. Dalam bagian ini, kita akan menjelajahi lebih lanjut tentang pengukuran dan evaluasi kualitas sinyal, termasuk parameter-parameter yang terkait dan pentingnya pemantauan sinyal dalam jaringan komputer.

Pengukuran kualitas sinyal melibatkan penilaian terhadap berbagai parameter sinyal untuk mengevaluasi keandalan dan kekuatan transmisi data. Beberapa parameter kualitas sinyal yang umum diukur meliputi:

1. **Kekuatan Sinyal**: Parameter ini mengukur kekuatan atau level sinyal yang diterima oleh perangkat penerima. Semakin tinggi kekuatan sinyal, semakin baik kualitas sinyal dan keandalan transmisi.

2. **Tingkat Kebisingan**: Tingkat kebisingan mengindikasikan sejauh mana gangguan atau interferensi yang ada dalam sinyal. Semakin rendah tingkat kebisingan, semakin baik kualitas sinyal.

3. **Rasio Sinyal-ke-Kebisingan (*Signal-to-Noise Ratio*/SNR)**: SNR menggambarkan perbandingan antara kekuatan sinyal yang diinginkan dengan tingkat kebisingan dalam sinyal. Semakin tinggi SNR, semakin baik kualitas sinyal.

4. ***Bit Error Rate* (BER)**: BER mengukur frekuensi terjadinya kesalahan bit dalam transmisi data. Semakin rendah BER, semakin baik kualitas sinyal dan keandalan transmisi.

Pengukuran dan evaluasi kualitas sinyal dilakukan untuk memastikan bahwa sinyal tetap dalam rentang yang dapat diterima dan memenuhi standar yang ditetapkan. Melalui pengukuran ini, kita dapat memantau perubahan dalam kualitas sinyal dan mengidentifikasi potensi masalah dalam transmisi data.

Evaluasi kualitas sinyal memainkan peran penting dalam pemecahan masalah dan pemeliharaan jaringan komputer. Dengan memantau kualitas sinyal secara teratur, kita dapat mendeteksi gangguan atau gangguan dalam transmisi data, serta mengambil tindakan yang diperlukan untuk memperbaiki kualitas sinyal.

Penting untuk menggunakan alat pengukur sinyal yang tepat dan akurat dalam melakukan pengukuran dan evaluasi kualitas sinyal. Alat ini memungkinkan administrator jaringan untuk mengukur dan memantau parameter-parameter sinyal dengan tepat, serta untuk melakukan analisis yang mendalam terhadap kualitas transmisi data.

Dengan melakukan pengukuran dan evaluasi kualitas sinyal secara teratur, kita dapat memastikan keandalan dan kualitas transmisi data melalui perangkat keras physical layer dalam jaringan komputer. Hal ini memungkinkan kita untuk mengidentifikasi dan memperbaiki masalah sinyal dengan cepat, sehingga menjaga performa jaringan yang optimal.

4.5 Perkembangan Terkini dalam Perangkat Keras Physical Layer

Perkembangan teknologi terus mendorong inovasi dalam perangkat keras physical layer. Dalam bagian ini, kita akan menjelajahi beberapa perkembangan terkini yang mempengaruhi perangkat keras physical layer, termasuk jaringan 5G, teknologi media transmisi terbaru, dan perangkat keras physical layer untuk Internet of Things (IoT)..

4.5.1 Jaringan 5G dan dampaknya pada physical layer

Jaringan 5G telah menjadi salah satu terobosan paling signifikan dalam industri telekomunikasi modern. Sebagai generasi terbaru jaringan seluler, 5G menjanjikan kecepatan yang jauh lebih tinggi, latency yang rendah, kapasitas yang lebih besar, dan konektivitas yang lebih andal (Hidayat, 2017). Perkembangan ini memiliki dampak yang signifikan pada perangkat keras physical layer dalam jaringan komputer.

Salah satu dampak utama jaringan 5G pada physical layer adalah peningkatan kecepatan transmisi data. Dengan kecepatan yang dapat mencapai gigabit per detik, perangkat keras physical layer harus dapat mendukung throughput yang tinggi dan kapasitas transmisi yang lebih besar. Teknik modulasi yang lebih canggih, seperti modulasi OFDM (*Orthogonal Frequency Division Multiplexing*), digunakan untuk mengirimkan data dengan kecepatan yang tinggi melalui saluran frekuensi yang lebih lebar.

Selain itu, jaringan 5G menggunakan frekuensi yang lebih tinggi, termasuk frekuensi milimeter gelombang (mmWave), untuk mencapai kecepatan yang lebih tinggi. Hal ini mengharuskan perangkat keras physical layer untuk mampu mengatasi tantangan dalam transmisi pada frekuensi yang lebih tinggi, seperti penyimpangan sinyal yang lebih signifikan dan interferensi yang lebih besar. Penanganan transmisi pada frekuensi tinggi membutuhkan antena yang lebih canggih dan perangkat penguat sinyal yang efisien.

Selain itu, jaringan 5G membutuhkan infrastruktur yang padat dan sering kali memerlukan pemasangan stasiun basis yang lebih dekat satu sama lain. Oleh karena itu, perangkat keras physical layer harus mendukung infrastruktur yang lebih padat, termasuk pemasangan antena yang lebih banyak dan pemrosesan sinyal yang lebih kompleks. Selain itu, manajemen daya yang efisien menjadi penting agar perangkat keras physical layer dapat beroperasi dengan efisiensi yang tinggi.

Dalam rangka mendukung jaringan 5G yang kuat, perangkat keras physical layer harus mampu mengatasi tantangan dalam transmisi data dengan kecepatan tinggi, frekuensi tinggi, dan kepadatan infrastruktur yang lebih tinggi. Ini melibatkan pengembangan perangkat keras yang canggih seperti antena yang lebih canggih, pemrosesan sinyal yang lebih kuat, dan manajemen daya yang lebih efisien. Dengan perkembangan jaringan 5G, diharapkan performa dan kapabilitas perangkat keras physical layer akan terus ditingkatkan untuk mendukung kebutuhan komunikasi masa depan yang semakin kompleks dan terhubung secara nirkabel.

4.5.2 Teknologi terbaru dalam media transmisi

Perkembangan teknologi terus mendorong inovasi dalam media transmisi yang digunakan dalam perangkat keras physical layer. Dalam bagian ini, kita akan membahas beberapa teknologi terbaru dalam media transmisi yang memiliki dampak signifikan pada perangkat keras physical layer.

1. **Serat Optik Berkecepatan Tinggi**:
   Serat optik berkecepatan tinggi telah menjadi salah satu teknologi terbaru yang mengubah cara transmisi data. Dibandingkan dengan media transmisi tradisional seperti kabel tembaga, serat optik memungkinkan transmisi data dengan kecepatan yang jauh lebih tinggi dan kapasitas yang

lebih besar. Teknologi serat optik berkecepatan tinggi membutuhkan perangkat keras physical layer yang mampu mentransmisikan dan menerima data dengan tingkat kecepatan yang tinggi, serta menghadapi tantangan dalam pemrosesan sinyal optik.

2. **WiFi 6 dan Wi-Fi 6E**:
   Teknologi nirkabel terbaru seperti WiFi 6 dan Wi-Fi 6E telah menghadirkan kemajuan yang signifikan dalam media transmisi tanpa kabel. WiFi 6 menggunakan teknologi OFDMA (Orthogonal Frequency Division Multiple Access) dan MU-MIMO (Multi-User Multiple Input Multiple Output) untuk meningkatkan kapasitas dan efisiensi jaringan nirkabel. Wi-Fi 6E memperluas frekuensi yang tersedia untuk transmisi data nirkabel, memungkinkan kecepatan dan kapasitas yang lebih tinggi. Perangkat keras physical layer harus mendukung teknologi ini dan mampu mengelola lalu lintas data nirkabel dengan cepat dan efisien.

3. **Pengembangan Kabel Tembaga Lebih Cepat**:
   Meskipun serat optik telah menjadi pilihan utama untuk kecepatan transmisi yang tinggi, pengembangan kabel tembaga terus dilakukan untuk meningkatkan kecepatan dan kapasitas transmisi. Misalnya, pengembangan terbaru dalam kabel tembaga seperti kabel Ethernet Cat 8 dan Cat 8.1 telah memungkinkan kecepatan transmisi yang mencapai 40 Gbps atau bahkan 100 Gbps. Perangkat keras physical layer yang mendukung teknologi ini harus dirancang untuk mengatasi tantangan dalam transmisi pada frekuensi yang lebih tinggi dan mengoptimalkan kecepatan dan kualitas sinyal.

Teknologi terbaru dalam media transmisi terus menghadirkan kemajuan dalam kecepatan, kapasitas, dan efisiensi transmisi data. Perangkat keras physical layer harus terus beradaptasi dan dikembangkan untuk mendukung teknologi media transmisi terbaru ini. Dengan dukungan perangkat keras yang tepat, transmisi data melalui media transmisi yang canggih dapat dijamin keandalannya, kecepatannya, dan kualitasnya.

4.5.3 Perangkat keras physical layer untuk *Internet of Things* (IoT)

Internet of Things (IoT) telah menjadi tren yang mengubah cara kita menghubungkan dan berinteraksi dengan perangkat-perangkat di sekitar kita. Dalam ekosistem IoT yang semakin berkembang, perangkat keras physical layer memainkan peran krusial dalam mendukung konektivitas yang andal dan efisien antara perangkat IoT (Yudistriansyah, 2019).

Perangkat keras physical layer untuk IoT harus dirancang dengan mempertimbangkan beberapa faktor penting. Pertama, perangkat keras tersebut harus mendukung konektivitas yang handal dalam jaringan. Konektivitas nirkabel seperti teknologi Bluetooth, Zigbee, atau Z-Wave sering digunakan dalam aplikasi IoT. Perangkat keras physical layer harus mampu memahami dan berinteraksi dengan protokol komunikasi ini untuk memastikan komunikasi yang mulus antara perangkat IoT.

Selain itu, efisiensi energi juga menjadi faktor kunci dalam perangkat keras physical layer untuk IoT. Banyak perangkat IoT bekerja dengan daya yang terbatas, seperti baterai, sehingga perangkat keras harus dirancang untuk mengoptimalkan konsumsi daya. Ini dapat mencakup penggunaan teknik seperti low-power modes, sleep modes, atau protokol komunikasi yang hemat energi. Dengan meminimalkan konsumsi daya perangkat keras physical layer, masa pakai baterai perangkat IoT dapat diperpanjang dan ketergantungan pada sumber daya eksternal dapat dikurangi.

Selanjutnya, skalabilitas juga menjadi aspek penting dalam perangkat keras physical layer untuk IoT. Dalam lingkungan IoT yang cenderung terdiri dari banyak perangkat yang saling terhubung, perangkat keras physical layer harus mampu mengelola lalu lintas data yang tinggi dan mempertahankan kinerja yang baik dalam jumlah perangkat yang semakin meningkat. Hal ini dapat mencakup penggunaan teknologi jaringan seperti LPWAN (*Low-Power Wide Area Network*) atau mesh network yang dapat menangani konektivitas yang skalabel dengan baik.

Perangkat keras physical layer untuk IoT juga harus mendukung keamanan yang kuat. Dalam konteks IoT, keamanan data dan privasi menjadi kritis, terutama karena perangkat IoT seringkali mengirimkan dan menerima data yang sensitif. Perangkat keras physical layer harus memperhatikan mekanisme enkripsi dan autentikasi yang kuat untuk melindungi data dan mencegah akses yang tidak sah.

Perkembangan perangkat keras physical layer untuk IoT terus berlanjut dengan peningkatan konektivitas, efisiensi energi, skalabilitas, dan keamanan. Dalam menjelajahi potensi IoT yang semakin berkembang, perangkat keras physical layer berperan penting dalam menyediakan konektivitas yang andal dan mendukung pertukaran data yang efisien antara perangkat IoT. Dengan perangkat keras physical layer yang tepat, IoT dapat memberikan dampak yang signifikan pada berbagai bidang, seperti rumah pintar, industri, transportasi, dan kesehatan.

4.6 Studi Kasus dan Implementasi

Studi kasus dan implementasi adalah pendekatan praktis dalam menerapkan perangkat keras physical layer di lingkungan jaringan nyata. Dalam studi kasus, kita menganalisis penerapan perangkat keras physical layer, pemeliharaan rutin, dan pemecahan masalah yang muncul. Melalui pendekatan ini, kita mempelajari bagaimana perangkat keras physical layer digunakan,

dikembangkan, dan dikelola untuk memenuhi kebutuhan konektivitas, kecepatan, keamanan, dan skalabilitas dalam lingkungan jaringan yang sebenarnya.

4.6.1 Penerapan Perangkat Keras Physical Layer dalam Lingkungan Jaringan Nyata

Dalam bab ini, kita akan melihat beberapa studi kasus dan implementasi nyata tentang penerapan perangkat keras physical layer dalam lingkungan jaringan. Studi kasus ini mencakup penerapan perangkat keras physical layer dalam berbagai industri dan skenario yang berbeda, serta analisis kasus-kasus terkait pengembangan, pemeliharaan, dan pemecahan masalah.

1. **Studi Kasus 1: Penerapan Perangkat Keras *Physical Layer* dalam Jaringan Kantor Pusat**
   Perusahaan manufaktur ABC memiliki kantor pusat yang terdiri dari beberapa lantai dengan ratusan pengguna. Mereka menghadapi tantangan dalam mengelola konektivitas jaringan yang handal dan cepat antara departemen dan pengguna. Untuk mengatasi hal ini, mereka menerapkan perangkat keras physical layer yang sesuai, seperti switch managed dengan multiple gigabit uplinks dan fitur keamanan yang diperlukan. Selain itu, mereka melakukan pemeliharaan rutin pada perangkat keras physical layer, seperti pemeriksaan koneksi, pembersihan perangkat keras, dan pembaruan firmware. Ketika terjadi masalah koneksi atau performa yang buruk, tim pemecahan masalah melakukan analisis dan pemecahan masalah yang diperlukan untuk memastikan jaringan kantor pusat tetap beroperasi dengan baik.

2. **Studi Kasus 2: Penerapan Perangkat Keras *Physical Layer* dalam Lingkungan Industri**
   Sebuah pabrik manufaktur menggunakan jaringan komputer yang kompleks untuk menghubungkan mesin-

mesin produksi, sensor-sensor, dan sistem kontrol. Mereka mengandalkan perangkat keras physical layer yang kuat untuk mendukung konektivitas yang andal dan waktu respons yang cepat. Perangkat keras physical layer yang mereka terapkan mencakup switch industri dengan kemampuan tahan debu dan goncangan, serta teknologi komunikasi nirkabel seperti Bluetooth Low Energy (BLE) untuk menghubungkan sensor-sensor. Selain itu, mereka memiliki tim pemeliharaan yang secara rutin memeriksa dan mengelola perangkat keras physical layer, serta melibatkan tim pemecahan masalah yang terlatih untuk mengatasi masalah jaringan yang mungkin muncul.

3. **Studi Kasus 3: Penerapan Perangkat Keras Physical Layer dalam Jaringan Cloud**
   Sebuah perusahaan layanan cloud menyediakan infrastruktur jaringan yang besar untuk menyimpan dan mengelola data pelanggan. Mereka menerapkan perangkat keras physical layer yang sangat skalabel dan tingkat ketersediaan yang tinggi untuk mendukung kebutuhan komputasi awan. Perangkat keras physical layer yang mereka gunakan mencakup switch modular dengan kemampuan redundant power supply dan hot-swappable modules. Selain itu, mereka memiliki mekanisme pemantauan jaringan yang canggih untuk mendeteksi dan memperbaiki masalah dengan cepat. Tim pengembangan dan pemeliharaan perangkat keras physical layer terus mengembangkan dan mengoptimalkan jaringan cloud mereka untuk memastikan performa dan ketersediaan yang optimal.

4.6.2 Analisis Kasus Pengembangan, Pemeliharaan, dan Pemecahan Masalah

Selama proses pengembangan, pemeliharaan, dan pemecahan masalah perangkat keras physical layer, perusahaan harus mempertimbangkan beberapa faktor kunci. Pengembangan perangkat keras physical layer harus mempertimbangkan kebutuhan spesifik dari lingkungan jaringan yang akan digunakan, seperti skala, kecepatan transmisi, dan tingkat keamanan yang diperlukan (Huwae, 2023). Pemeliharaan rutin harus dilakukan untuk memastikan perangkat keras physical layer tetap dalam kondisi baik dan optimal. Ketika masalah muncul, tim pemecahan masalah harus memiliki keahlian yang diperlukan dan alat yang sesuai untuk mendiagnosis dan memperbaiki masalah dengan cepat.

Dalam studi kasus dan analisis kasus yang dilakukan, dapat disimpulkan bahwa penerapan perangkat keras physical layer yang efektif dalam lingkungan jaringan nyata memerlukan pemahaman yang mendalam tentang kebutuhan dan tantangan yang ada. Dengan pengembangan yang tepat, pemeliharaan yang teratur, dan pemecahan masalah yang terlatih, perusahaan dapat memastikan performa, keandalan, dan keamanan yang optimal.

4.7 Kesimpulan

Dalam buku ini, kami telah memaparkan konsep-konsep penting yang terkait dengan perangkat keras physical layer. Kami memulai dengan memahami definisi dan tujuan physical layer sebagai komponen kritis dalam jaringan komputer. Kami juga membahas komponen-komponen utama dalam perangkat keras *physical layer*, termasuk kabel, switch, router, dan antena.

Selanjutnya, kami membahas ragam media transmisi yang digunakan untuk transfer data, termasuk kabel tembaga, serat optik, dan teknologi nirkabel. Kami juga menjelajahi prinsip

pengiriman data fisik, seperti teknik modulasi sinyal dan pengaturan daya.

Selain itu, kami membahas pentingnya keandalan dan performa dalam physical layer, termasuk teknik deteksi dan koreksi kesalahan, pengukuran latensi dan throughput, serta evaluasi kualitas sinyal. Kami juga mengeksplorasi perkembangan terkini dalam perangkat keras physical layer, seperti pengaruh jaringan 5G, teknologi media transmisi terbaru, dan perangkat keras physical layer untuk *Internet of Things* (IoT).

Dalam mengimplementasikan perangkat keras physical layer dalam lingkungan jaringan nyata, kami melihat studi kasus dan analisis kasus tentang penerapan, pengembangan, pemeliharaan, dan pemecahan masalah. Studi kasus ini memberikan wawasan tentang bagaimana perangkat keras physical layer diterapkan dalam berbagai industri dan lingkungan, serta bagaimana tantangan diatasi dalam penggunaan dan pemeliharaan perangkat keras physical layer.

Dengan melihat masa depan dan arah perkembangan perangkat keras physical layer, kita dapat melihat implikasi yang menarik. Perkembangan teknologi seperti jaringan 5G, teknologi media transmisi terbaru, dan pertumbuhan IoT akan terus mempengaruhi perangkat keras physical layer. Hal ini mencakup peningkatan kecepatan, kapasitas, efisiensi energi, dan keamanan dalam perangkat keras physical layer. Dalam menghadapi masa depan yang semakin terhubung dan kompleks, penting bagi perangkat keras physical layer untuk terus berkembang dan beradaptasi dengan kemajuan teknologi.

Dengan demikian, buku ini memberikan wawasan mendalam tentang perangkat keras physical layer dan berbagai aspek yang terkait dengannya. Konsep-konsep yang telah dibahas dalam buku ini akan memberikan dasar yang kuat bagi pembaca untuk memahami, menerapkan, dan mengelola perangkat keras physical layer dalam lingkungan jaringan komputer

DAFTAR PUSTAKA

Iskandar, A., Geni, B.Y., Prabiantissa, C.N., Kurnaedi, D., Wahyuddin, S., Samosir, K., Indriyani, T., Alfian, D., Nurmuslimah, S. and Supriyadi, A., 2022. Pengantar Jaringan Komputer. Get Press.

Komputer, W., 2006. SPP Menginstal Jaringan Komputer. Elex Media Komputindo.

Huda, M. and Kom, M., 2019. Open Systems Interconnection: Lapisan Fisik. bisakimia.

DJ, R.A., 2014. ANALISIS KINERJA ROUTING PROTOCOL AODV DAN AOMDV PADA WIRELESS SENSOR NETWORK DENGAN MENGGUNAKAN TOPOLOGI MESH (Doctoral dissertation, Universitas Widyatama).

Agustini, M., Oktaviani, S., Muhammad, F. and Mozef, E., 2019, August. Perancangan dan Realisasi Sistem Komunikasi Suara dengan Penjelasan Suara yang Ditransmisikan dari Cahaya Lampu Penerangan LED. In Prosiding Industrial Research Workshop and National Seminar (Vol. 10, No. 1, pp. 387-395).

Rafiudin, R., 2003. Panduan Membangun Jaringan Komputer Untuk Pemula. Elex Media Komputindo.

Arius, D., 2020. Komunikasi data. Penerbit Andi.

Alfurqon, D. and Assegaff, S., 2018. Analisis Dan Perancangan Jaringan Local Area Network Pada Laboratorium Smk Negeri 1 Kota Jambi. Jurnal Manajemen Sistem Informasi, 3(3), pp.1149-1163.

Hasrul, H. and Lawani, A.M., 2017. Pengembangan Jaringan Wireless Menggunakan Mikrotik Router Os Rb750 Pada Pt. Amanah Finance Palu. Jurnal Elektronik Sistem Informasi Dan Komputer, 3(1), pp.11-19.

Pradana, I.F., 2023, Deteksi keamanan server menggunakan cowriedan fortigatepada web server (Bachelor's thesis, Fakultas Sains dan Teknologi UIN Syarif Hidayatullah Jakarta).

Solehudin, A. and Garno, G. 2017. "PROTOTYPE API PADA APLIKASI PEMBATASAN AKSES INTERNET DENGAN PEMANFAATAN HAK AKSES USER PROFILE HOTSPOT", JURNAL REKAYASA INFORMASI, 6(2).

Nasir, J. and Andrianto, E., 2018. Implementasi Quality of Service, Limit Bandwidth Dan Load Balancing Dengan Menggunakan Firmware Dd-Wrt Pada Router Buffalo Whr-Hp-G300N. Simetris: Jurnal Teknik Mesin, Elektro dan Ilmu Komputer, 9(1), pp.403-412.

Hidayat, R., 2017. Analisis Potensi Kunci Teknologi 5G Untuk Implementasi Optimal Di Jawa Barat Key Potential Analysis of 5G Technology for Optimal Implementation in West Java. CR J, 3(2), pp.115-131.

Yudistriansyah, A., Suryanegara, M., Gunawan, D., Arifin, A. and Krisnadi, I., 2019. Evaluasi Maturity Level Keamanan dan Rekomendasi Perbaikan Keamanan Internet of Things (IOT) PT XYZ Berdasarkan Kerangka Kerja IOT Security Maturity Model. Universitas Indonesia, pp.1-2.

Huwae, R.B., Jatmika, A.H. and Alamsyah, N., 2023. Evaluasi Performansi Protokol 6LoWPAN terhadap CSMA/CA pada perangkat IoT. Jurnal Teknologi Informasi, Komputer, dan Aplikasinya (JTIKA), 5(1), pp.104-111.

BAB 5
SISTEM BILANGAN

Oleh Azhari Ali Ridha

5.1 Pendahuluan

Sistem bilangan memainkan peran krusial dalam dunia komputer dan teknologi informasi. Sistem bilangan digunakan untuk merepresentasikan, memproses, dan menyimpan informasi dalam bentuk digital. Pemahaman tentang sistem bilangan penting dalam pemrograman, desain perangkat keras, pemrosesan citra, keamanan siber, dan bidang lain dalam teknologi informasi. Dengan pemahaman ini, para profesional dapat efektif bekerja dengan representasi data dan memahami bagaimana komputer beroperasi dalam tingkat yang lebih rendah.

Pemahaman tentang sistem bilangan penting dalam pemrograman, desain perangkat keras, pemrosesan citra, keamanan siber, dan bidang lain dalam teknologi informasi. Dengan pemahaman ini, para profesional dapat efektif bekerja dengan representasi data dan memahami bagaimana komputer beroperasi dalam tingkat yang lebih rendah.

5.2 Sistem Basis Bilangan

Sistem bilangan adalah cara atau metode yang digunakan untuk mewakili dan menghitung jumlah atau kuantitas dalam bentuk angka atau simbol-simbol tertentu. Sistem bilangan merupakan konsep fundamental dalam matematika dan ilmu komputer yang digunakan untuk melakukan operasi matematika seperti penjumlahan, pengurangan, perkalian, dan pembagian. Basis Bilangan 2 (Binary- digit, digunakan dalam Representasi Data, Representasi Angka, Pemrosesan Instruksi dll), Basis

Bilangan 8 (Octadecimal, digunakan dalam pengalamatan di memori, Perintah Pemrograman Kuno), dan Basis Bilangan 16 (Hexadecimal, biasanya digunakan dalam pengalamatan di memori dan Representasi Warna, pengkodean karakter).

1. DECimal :
   Desimal adalah sistem bilangan yang umum digunakan dalam matematika dan kehidupan sehari-hari. Sistem desimal menggunakan basis 10, yang berarti terdapat 10 simbol yang digunakan untuk merepresentasikan angka, yaitu 0, 1, 2, 3, 4, 5, 6, 7, 8, dan 9.
   Dalam sistem desimal, setiap digit memiliki nilai tempatannya sendiri berdasarkan posisinya dalam angka. Nilai tempatannya meningkat dari kanan ke kiri, dengan digit paling kanan sebagai tempat satuan. Misalnya, dalam angka 532, digit 2 mewakili satuan (10^0), digit 3 mewakili puluhan (10^1), dan digit 5 mewakili ratusan (10^2). Contoh: $(37)_{10}$ = 23_{10} = DEC37 $(97)_{10}$ = 97_{10} = DEC97
2. Binary digit, juga dikenal sebagai "bit," adalah unit terkecil dari data dalam sistem bilangan biner (basis 2). Binary digit dapat memiliki dua nilai yang mungkin, yaitu 0 atau 1. Bit merupakan fondasi dari sistem bilangan biner yang digunakan dalam komputasi dan pemrosesan data dalam komputer.
   Contoh: $(1101)_2$ = 1101_2 panjang data = 4 bit
   $(10010)_2$ = 10010_2 panjang data = 5 bit
3. Oktal adalah sistem bilangan yang menggunakan basis delapan (8) untuk merepresentasikan nilai numerik. Sistem bilangan oktal menggunakan angka dari 0 hingga 7 sebagai digit-diginya. Dalam konteks komputasi dan matematika, oktal sering digunakan untuk merepresentasikan data dalam bentuk bilangan bulat.
   Setiap digit oktal mewakili kombinasi tiga digit biner (binary digit atau bit). Oleh karena itu, sistem bilangan oktal lebih

kompak daripada sistem bilangan biner dalam merepresentasikan nilai-nilai tertentu. Misalnya, digit oktal "7" mewakili nilai biner "111," dan digit oktal "3" mewakili nilai biner "011."rentang: 0 s.d 7, selengkapnya: 0,1,2,3,4,5,6,7.

Contoh: $(23)_8 = 23_8 = 023$

4. Hexa (atau disebut juga "Hexadecimal") adalah sistem bilangan yang menggunakan basis 16. Sistem ini sering digunakan dalam komputer dan matematika terutama dalam konteks pengkodean dan representasi data.

   Dalam sistem heksadesimal, angka-angka digambarkan dengan menggunakan 16 simbol, yaitu 0-9 seperti dalam sistem desimal, dan tambahan 6 simbol lagi yang diwakili oleh huruf A, B, C, D, E, dan F. Simbol A mewakili nilai 10, B mewakili nilai 11, dan seterusnya hingga F mewakili nilai 15.

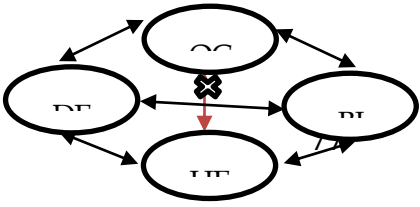
   Contoh beberapa angka dalam sistem heksadesimal dan nilai mereka dalam sistem desimal:

   0x1 = 1 (dalam desimal)
   0xA = 10 (dalam desimal)
   0xF = 15 (dalam desimal)
   0x10 = 16 (dalam desimal)

5.3 Konversi Sistem Bilangan

Konversi sistem bilangan adalah proses mengubah sebuah angka dari satu sistem bilangan ke sistem bilangan lainnya. Sistem bilangan yang umum digunakan adalah desimal (basis 10), biner (basis 2), oktal (basis 8), dan heksadesimal (basis 16).

Konversi antara sistem bilangan melibatkan pengubahan representasi angka dalam satu basis menjadi representasi angka dalam basis yang lain. Proses ini melibatkan pemahaman tentang



Gambar 1 Alur konversi sistem

nilai tempat (nilai posisi) digit-digit dalam setiap basis bilangan.

5.3.1 Konversi Basis Bilangan N ke Decimal

Misalkan, sebuah bilangan basis bilangan 10 diketahui sebagai 24351 maka dituliskan:
$(24351)_{10}$ atau 2435_{10} atau DEC24351.
Jika diuraikan dalam basis bilangan 10, maka numerik 24351 dituliskan sebagai berikut:
$(24351)_{10}$ = 2-puluh ribuan+4-ribuan+3-ratusan + 5-puluhan + 1-satuan
$= 2*10^4 + 4*10^3 + 3*10^2 + 5*10^1 + 1*10^0$

Ingat!

Pangkat bilangan dengan eksponen 0 memiliki aturan khusus yang berlaku untuk semua bilangan kecuali 0. Aturan ini berlaku untuk bilangan positif, bilangan negatif, bilangan pecahan, dan bilangan irasional. Pangkatkan bilangan dengan eksponen 0 menghasilkan nilai 1, kecuali jika bilangan tersebut juga bernilai 0.

Pangkatkan bilangan dengan eksponen 1 adalah operasi yang sederhana. Pangkatkan bilangan dengan eksponen 1 tidak akan mengubah nilai bilangan tersebut.

Berdasar pendekatan di atas, dapat dilakukan konversi Basis Bilangan N ke dalam DECimal.
Biner ke Desimal
Dirumuskan:

$$DEC \sum_{i=0}^{n} a_i 2^i \quad \begin{matrix} \text{i} = 0,1,2,\ldots,\text{N} \\ \text{a} = 0 \text{ atau } 1 \end{matrix}$$

Contoh: $(10101)_2$ = (...)$_{10}$

Solusi:

$(10101)_2 = 1*2^4 + 0*2^3 + 1*2^2 + 0*2^1 + 1*2^0$

$= 16+0+4+0+1 = 5_{10}$

= DEC21

Oktadesimal (Oktal) ke Desimal

Dirumuskan:

$$DEC \sum_{i=0}^{n} a_i 8^i \qquad i = 0,1,2,\cdots,N \qquad a = 0,1,2,3,4,5,6,7$$

Contoh: $(1105)_8 = (...)_{10}$

Solusi:

$(1105)_8 = 1*8^3 + 1*8^2 + 0*8^1 + 5*8^0$

$= 512 + 64 + 0 + 5 = 581_{10}$

= DEC581

Heksadesimal (Heksal) ke Desimal

Dirumuskan:

$$DEC \sum_{i=0}^{n} a_i 8^i \qquad i = 0,1,2,\cdots,N \qquad a = 0,1,2,3,4,5,6,7,8,9,A,B,\ldots,F$$

Contoh: $(10c)_{16} = (...)_{10}$

Solusi:

$(AC)_{16} = 10*16^2 + A*16^0$

$= 10*16^1 + 12*16^0$

$= 160 + 12 = 178_{10}$

= DEC178

5.3.2 Konversi Decimal ke Basis Bilangan N

Untuk mengkonversi bilangan desimal ke basis bilangan N (basis yang lebih besar dari 1), Anda dapat menggunakan metode pembagian berulang. Berikut adalah langkah-langkah umum untuk mengkonversi bilangan desimal ke basis bilangan N:
Bagi bilangan desimal dengan basis bilangan N.
Catat hasil bagi (hasil integer) dan sisa pembagian.
Ulangi langkah 1 dan 2 dengan hasil bagi sebagai bilangan desimal yang baru, hingga hasil bagi menjadi 0.
Susun sisa pembagian dari langkah 2 dalam urutan terbalik untuk mendapatkan representasi bilangan dalam basis N.
Contoh: Konversi Decimal ke Binary (Basis 2)

Misalkan kita ingin mengkonversi bilangan DEC 14 ke basis biner (basis 2).

Langkah 1: 14 ÷ 2 = 7 (Hasil Bagi), Sisa = 0
Langkah 2: 7 ÷ 2 = 3 (Hasil Bagi), Sisa = 1
Langkah 3: 3 ÷ 2 = 1 (Hasil Bagi), Sisa = 1
Langkah 4: 1 ÷ 2 = 0 (Hasil Bagi), Sisa = 1

Menggabungkan sisa-sisa pembagian dari langkah 4 ke langkah 1 dalam urutan terbalik: 1110

Jadi, bilangan desimal 14 dalam basis biner adalah 1110.

Anda dapat mengikuti langkah-langkah serupa untuk mengkonversi bilangan desimal ke basis bilangan lain, seperti basis oktal (basis 8) atau basis heksadesimal (basis 16). Hanya perlu mengganti basis pembagian pada langkah 1 dengan nilai yang sesuai (yaitu 8 untuk basis oktal atau 16 untuk basis heksadesimal).

Dengan algoritma yang sama, seperti di atas dapat dilakukan untuk basis bilangan berikut ini:

Desimal ke Basis Bilangan 2 (DEC BIN) Contoh: Untuk mengkonversi bilangan desimal ke basis bilangan biner (basis 2), Anda dapat menggunakan metode pembagian berulang. Berikut adalah langkah-langkah untuk mengkonversi bilangan desimal ke biner:

Bagi bilangan desimal dengan 2.
Catat hasil bagi (hasil integer) dan sisa pembagian (0 atau 1).
Ulangi langkah 1 dan 2 dengan hasil bagi sebagai bilangan desimal yang baru, hingga hasil bagi menjadi 0.
Susun sisa pembagian dari langkah 2 dalam urutan terbalik untuk mendapatkan representasi bilangan dalam basis biner.
Contoh: Konversi Decimal ke Binary

Misalkan kita ingin mengkonversi bilangan DEC2121 ke basis biner.
$2341_{10} = (...)_2$
Langkah 1: 2341 ÷ 2 = 1170 (Hasil Bagi), Sisa = 1
Langkah 2: 11702 ÷ 2 = 585 (Hasil Bagi), Sisa = 0
Langkah 3: 585 ÷ 2 = 292 (Hasil Bagi), Sisa = 1
Langkah 4: 292 ÷ 2 = 146 (Hasil Bagi), Sisa = 0
Langkah 5: 146 ÷ 2 = 73 (Hasil Bagi), Sisa = 0
Langkah 6: 73 ÷ 2 = 36 (Hasil Bagi), Sisa = 1
Langkah 7: 36 ÷ 2 = 18 (Hasil Bagi), Sisa = 0
Langkah 8: 18 ÷ 2 = 9 (Hasil Bagi), Sisa = 0
Langkah 9: 9 ÷ 2 = 4 (Hasil Bagi), Sisa = 1
Langkah 10: 4 ÷ 2 = 2 (Hasil Bagi), Sisa = 0
Langkah 11: 2 ÷ 2 = 1 (Hasil Bagi), Sisa = 0

Menggabungkan sisa-sisa pembagian dari langkah 5 ke langkah 1 dalam urutan terbalik: 11001

Jadi, bilangan desimal 2341 dalam basis biner adalah 1001 0010 0101.

Anda dapat mengikuti langkah-langkah yang sama untuk mengkonversi bilangan desimal lainnya ke basis biner. Pada setiap langkah, catat hasil bagi dan sisa pembagian, dan akhirnya susun sisa-sisa pembagian dalam urutan terbalik untuk mendapatkan representasi biner.

Desimal ke Basis Bilangan 8 (DEC OCT) Contoh:

Tentukan DEC1478 dalam Oktal.
$1478_{10} = (...)_8$
Solusi:
1478 /8 = 184 sisa 6 Least Significant Digit (LSD)
184 / 8 = 23 sisa 0
23 / 8 = 2 sisa 7
2 / 8 = 0 sisa 2 Most Significant Digit (MSD)Dituliskan: 02706 atau 027068
Desimal ke Basis Bilangan 16 (DEC HEX) Contoh: Tentukan DEC2136 dalam Heksal.
$2136_{10} = (...)_{16}$
Solusi:
2136 /16 = 132 sisa 8 *Least Significant Digit* (LSD)
133 /16 = 8 sisa 5
8 /16 = 0 sisa 8 Most Significant Bit(MSB)

Dituliskan: 0x858 atau 858_{16}

Untuk konversi dari hex ke oct tidak bisa langsung harus melalui konversi baik melalui BIN atau dari DEC Sistem bilangan

heksadesimal menggunakan 16 simbol, yaitu 0-9 dan huruf A-F, sedangkan sistem bilangan oktal hanya menggunakan 8 simbol, yaitu 0-7. Karena jumlah simbol yang berbeda, tidak ada cara langsung untuk mengonversi satu sistem bilangan ke sistem bilangan lainnya tanpa melibatkan sistem bilangan desimal sebagai perantara.

5.4 Bilangan Pecahan (*Floating-Point Number*)

Bilangan pecahan dalam komputer adalah representasi dari angka-angka yang bukan bilangan bulat atau bilangan utuh. Bilangan pecahan juga dikenal sebagai bilangan desimal atau bilangan real. Representasi bilangan pecahan diperlukan karena tidak semua nilai numerik dapat diwakili secara akurat dalam bentuk bilangan bulat.

Dalam komputer, bilangan pecahan direpresentasikan menggunakan format khusus yang disebut titik mengambang (*floating-point*). Format titik mengambang mengizinkan representasi angka dalam bentuk mantissa (pada basis biner) yang dikalikan dengan pangkat dari basis (eksponen). Ini memungkinkan representasi bilangan pecahan yang lebih luas dengan tingkat akurasi tertentu.Bilangan pecahan digunakan untuk menggambarkan nilai yang tidak tepat sebagai bilangan bulat. Contohnya, dalam bilangan bulat, kita hanya dapat mewakili nilai yang tepat seperti 1, 2, 3, dst. Namun, dalam kasus di mana kita perlu menggambarkan bagian dari suatu bilangan, bilangan pecahan diperlukan.

Contoh bilangan pecahan:

1/2 (satu per dua)
3/4 (tiga per empat)
2/5 (dua per lima)

Bilangan pecahan juga dapat diubah menjadi bentuk desimal dengan membagi pembilang oleh penyebut. Misalnya, 1/2 dalam bentuk desimal adalah 0.5, dan 3/4 adalah 0.75.

Pada pembahasan sebelumnya lebih berfokus pada seputar bilangan bulat atau bisa juga disebut *integer number system*, Representasi bilangan pecahan dalam komputer sangat penting dalam berbagai aplikasi, termasuk pemrosesan data ilmiah, perhitungan matematika, simulasi, pemrograman grafis, dan lain-lain. Pemahaman tentang format titik mengambang dan keterbatasannya penting untuk menghindari kesalahan pembulatan dan mengoptimalkan akurasi dalam perhitungan yang melibatkan bilangan pecahan.

Dasar bagaimana melakukan konversi Basis Bilangan N (BIN,OCT,HEX) ke DECimal pada bentuk pecahan tetap berdasar pada bagaimana melakukan konversi pada bentuk bilangan bulat (*integer*)
yang sebelumnya telah dipaparkan.

Lihat operasi konversi dibawah ini:
Konversi Pecahan BI⇨ DEC

Contoh:

$1111.1011_2 = (\ldots)_{10}$

Solusi:

$1111.1011_2 = 0.1011_2 + 1011_2$

$= (1) + (2)$

Eksekusi (1):

$0.1011_2 = (\ldots)_{10}$

$= 1.2^{-1} + 0 + 1.2^{-3}$

$= 0.5 + 0.125$

$= 0.625_{10}$

Eksekusi (2):

$1111_2 = (\ldots)_{10}$

$= 1.2^4 + 1.2^3 + 1.2^2 + 1.2^1 + 1.2^0$
$= 16 + 8 + 4 + 2 + 1$
$= 32_{10}$

Dimana (1) dan (2) dioperasikan dengan menggunakan cara menjumlahkan semuanya dengan teknik:
$(1) + (2) = 0.625_{10} + 32_{10} = 32.625_{10}$
Hasilnya
$1101.101_2 = (32.625)_{10}$

Konversi Pecahan OCT ⇨DEC
Contoh:
$47.11 = 47.11_8 = (\ldots)_{10}$
Solusi:
$47.11_8 = 0.11_8 + 47_8$
$= (1) + (2)$
Eksekusi (1):
$0.11_8 = (\ldots)_{10}$
$= 1.8^{-1} + 1.8^{-2}$
$= 0.125 + 0.015625$
$= 0.140625_{10}$
Eksekusi (2):
$47_8 = (\ldots)_{10} = 4.8^1 + 7.8^0$
$= 32 + 7$
$= 39_{10}$

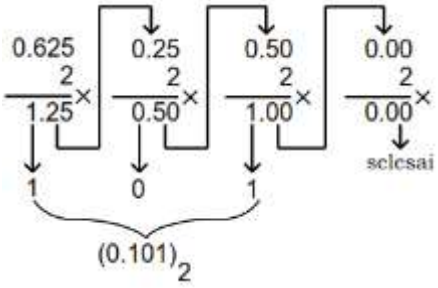
Dimana(1) dan (2) dioperasikan dengan menggunakan cara menjumlahkan semuanya dengan teknik:
$(1) + (2) = 0.140625_{10} + 39_{10} = 39.140625_{10}$
hasilnya:
$47.11_8 = (39.140625)_{10}$

Konversi Pecahan HEX ⇨ DEC
kasus:
$0x67.11 = 57.11_{16} = (\ldots)_{10}$
caranya:
$67.11_{16} = 0.11_{16} + 67_{16}$
$= (1) + (2)$
Eksekusi (1):
$0.11_{16} = (\ldots)_{10}$
$= 1.16^{-1} + 1.16^{-2}$
$= 0.0625 + 0.00390625$
$= 0.0664062_{10}$
Eksekusi (2):
$67_{16} = (\ldots)_{10}$
$= 6.16^{1} + 7.16^{0}$
$= 96 + 7$
$= 103_{10}$

Selanjutnya (1) dan (2) dioperasikan dengan menggunakan cara menjumlahkan semuanya dengan teknik:
$(1) + (2) = 0.0664062_{10} + 103_{10} = 103.0664062_{10}$
hasilnya:
$67.11_{16} = (103.06640625)_{10}$

Selanjutnya, bagaimana perubahan konversi sebaliknya, bentuk pecahan, dari DECimal ke Basis Bilangan N (BIN,OCT,HEX), adalah caranya akan sama dengan bentuk bilangan bulat (*integer*).
Konversi Pecahan DEC ⇨ BIN
Kasus:
$23.625_{10} = (\ldots)_{2}$

Perubahan konversi:
23.625_{10} = 0.625_{10} + 23_{10}
= (1) + (2)
Eksekusi (1):
0.625_{10} = $(\ldots)_2$

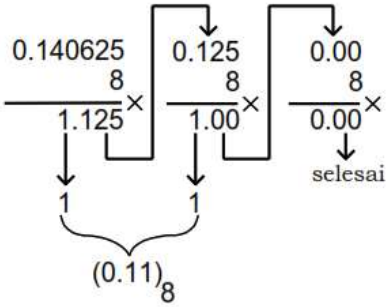


Eksekusi (2):
23_{10} = $(\ldots)_2$
23 / 2 = 11 sisa 1 *Least Significant Bit* (LSB)
11 / 2 = 6 sisa 1
6 / 2 = 3 sisa 0
3 / 2 = 1 sisa 1
1 / 2 = 0 sisa 1 *Most Significant Bit* (MSB)
dituliskan menjadi: 10111_2

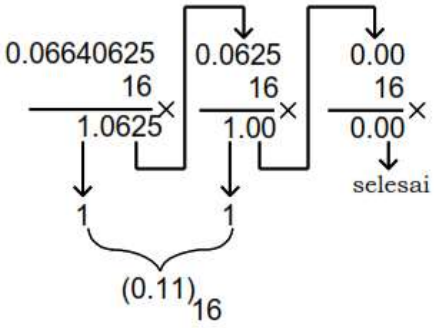
Selanjutnya (1) dan (2) dioperasikan dengan menggunakan cara menjumlahkan semuanya dengan teknik:
(1) + (2) = 0.101_2 + 10111_2 = 11011.101_2
maka, didapatkan:
$11011.101_2 = (13.625)_{10}$

Konversi Pecahan DEC ⇨ OCT
Contoh:
$57.14062_{10} = (\ldots)_8$
Solusi:

$57.14062_{10} = 0.14062_{10} + 47_{10}$
= (1) + (2)
Eksekusi (1):
$0.14062_{10} = (...)_8$
Eksekusi (2):



$57_{10} = (...)_8$
57 / 8 = 7 sisa 1 *Least Significant Digit* (LSD)
7 / 8 = 0 sisa 7 *Most Significant Digit* (MSD)
dituliskan menjadi: 71_8
Selanjutnya (1) dan (2) dioperasikan dengan menggunakan cara menjumlahkan semuanya dengan teknik:
(1) + (2) = $0.11_8 + 71_8 = 71.11_8$
maka, hasil yang didapatkan:
$57.14062_{10} = (71.11)_8$
Konversi Pecahan DES HEX
Contoh:
$1771.0664062_{10} = (...)_{16}$
Solusi:
$1771.0664062_{10} = 0.0664062_{10} + 77_{10}$
= (1) + (2)



Eksekusi (1):
0.0664062_{10} = (...)$_{16}$

Eksekusi (2):
177_{10} = (...)$_{16}$
177 / 16 = 110 sisa 11 atau B *Least Significant Digit* (LSD)
110 / 16 = 6 sisa 14 atau E
6 /16 = 0 Sisa 6 *Most Significant Digit* (MSD)

Dapat ditulis menjadi: $6EB_{16}$

Selanjutnya (1) dan (2) dioperasikan dengan menggunakan cara menjumlahkan semuanya dengan teknik:
(1) + (2) = 0.11_{16} + $6EB_{16}$ = $6EB.11_{16}$
maka, didapatkan hasilnya:
1771.14062_{10} = $(6EB.11)_{16}$

Untuk bahasan berikutnya, akan membahas bagaimana teknik melakukan konversi bentuk pecahan (*floating point*) dari Basis Bilangan N ke Basis Bilangan M, antara basis bilangan yang ada dalam bahasa mesin.
Misalkan: Bagaimanakah untuk OCT⇨ BIN
Contoh:

$14.23_8 = (\ldots)_2$

Solusi:

Lakukan dengan dua tahapan, yaitu:

langkah ke-1: OCT⇨ DEC

Langkah ke-2: DEC⇨ BIN

Jawab:

OCT ⇨ DEC

$184.23_8 = 0.23_8 + 14_8$

$= (1) + (2)$

Eksekusi (1):

$0.23_8 = (\ldots)_{10}$

$= 2.8^{-1} + 3.8^{-2}$

$= 0.25 + 0.046875$

$= 0.296875_{10}$

Eksekusi (2):

$174_8 = (\ldots)_{10}$

$= 1.8^2 + 7.8^1 + 4.8^0$

$= 64 + 56 + 4$

$= 124_{10}$

Selanjutnya (1) dan (2)) dioperasikan dengan menggunakan cara menjumlahkan semuanya dengan teknik :

$(1) + (2) = 0.296875_{10} + 9_{10} = 9.296875_{10}$

maka, didapatkan:

$(14.23)_8 = (9.296875)_{10}$

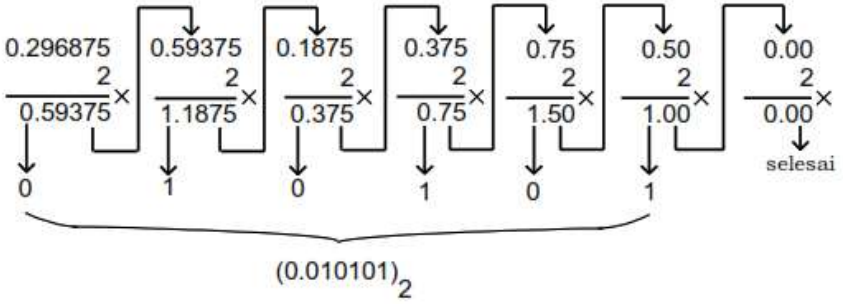
OCT⇨ BIN

$9.296875_{10} = 0.296875_{10} + 9_{10}$

$= (1) + (2)$

Eksekusi (1):

$0.296875_{10} = (\ldots)_2$



Eksekusi (2):

9_{10} = (...)2

9 / 2 = 4 sisa1 *Least Significant Bit* (LSB)

4 / 2 = 2 sisa 0

2 / 2 = 1 sisa 0

1 / 2 = 0 sisa 1 *Most Significant Bit* (MSB)

dituliskan menjadi: 1001_2

Selanjutnya (1) dan (2)) dioperasikan dengan menggunakan cara menjumlahkan semuanya dengan teknik :

(1) + (2) = $0.0101012_2 + 1001_2 = 1001.010101_2$

maka, didapatkan:

$9.296875_{10} = (1001.010101)_2 = (00001000.010101)_2$

atau dengan kata lain, maka didapatkan:

$14.23_8 = 8.296875_{10} = 1001.010101_2$

Untuk mendapatkan konversi ⇨ilangan ⇨ecahan HEX BIN, algoritmanya seperti mendapatkan konversi Bilangan Pecahan OCT BIN, yakni konversikan terlebih dahulu ke dalam DEC.

DAFTAR PUSTAKA

Ir. Edi Nur Sasongko, M.Kom, http://kuliah.dinus.ac.id/edi-nur/sb1-9.html

Computer System, Periyadi, Sihar NMP Simamora, Nina Hendra, Dudi Soegiarto, Anak Agung Gde Agung, Idham, Sistem Komputer, *Telkom Polytechnic, 2009*

BAB 6
LAPISAN DATA LINK

Oleh Suwito Pomalingo

6.1 Pendahuluan

Jaringan komputer telah menjadi komponen penting dalam berbagai aspek kehidupan kita, mulai dari komunikasi hingga transaksi finansial. Data yang kita kirim dan terima melalui jaringan ini harus melewati beberapa lapisan dalam model referensi jaringan, salah satunya adalah Data Link Layer. Lapisan ini memiliki peran penting dalam memastikan data yang kita kirimkan dapat sampai ke tujuan dengan tepat dan efisien.

Data Link Layer, yang merupakan lapisan kedua dalam model referensi OSI, bertanggung jawab dalam pengiriman data antar perangkat di dalam jaringan lokal yang sama. Data Link Layer menangani berbagai aspek teknis penting seperti framing, addressing, dan error detection. Pemahaman yang mendalam tentang Data Link Layer sangat penting bagi siapa saja yang ingin mempelajari atau bekerja di bidang teknologi jaringan. Dalam bab ini, kita akan membahas secara rinci tentang berbagai konsep dan protokol yang berkaitan dengan Data Link Layer.

6.2 Pengenalan Data Link Layer

6.2.1 Pengertian dan Tujuan

Data Link Layer, atau Lapisan Tautan Data, merupakan lapisan kedua dalam hierarki model OSI (*Open Systems Interconnection*), sebuah model referensi yang dikembangkan oleh *International Organization for Standardization* (ISO) (Tanenbaum and Wetherall, 2010). Model OSI ini adalah sebuah kerangka kerja yang menjelaskan bagaimana jaringan komputer harus beroperasi,

dimulai dari pengiriman data fisik hingga interaksi aplikasi. Pada model ini, Data Link Layer berada di antara Physical Layer dan Network Layer, berperan penting dalam pengiriman data yang efektif dan efisien.

Data Link Layer memiliki tugas utama untuk mengontrol transmisi data antar perangkat dalam suatu jaringan lokal atau yang lebih sering dikenal dengan Local Area Network (LAN) (Forouzan, 2007). Peran utamanya adalah untuk menyediakan mekanisme untuk komunikasi data yang efektif antar perangkat dan untuk mengendalikan akses ke media transmisi. Ia menjamin bahwa data yang dikirim dari perangkat sumber dapat diterima oleh perangkat tujuan dengan baik dan tanpa error.

Dalam konteks pengiriman data, Data Link Layer bertugas untuk memecah data yang diterima dari lapisan di atasnya (Network Layer) menjadi bingkai atau frame yang lebih kecil, kemudian mengirimkannya ke Physical Layer (Stallings, 2013). Proses ini dikenal sebagai proses framing. Framing ini penting untuk memastikan bahwa setiap bagian data yang dikirim dapat diproses dengan efisien dan efektif.

Selain itu, Data Link Layer juga bertanggung jawab untuk menangani kesalahan yang mungkin terjadi selama transmisi data (Forouzan, 2007). Dengan adanya mekanisme deteksi dan koreksi kesalahan di Data Link Layer, setiap frame data yang rusak atau hilang dapat segera dideteksi dan dikoreksi. Ini membantu memastikan bahwa data yang diterima oleh perangkat tujuan adalah data yang akurat dan lengkap.

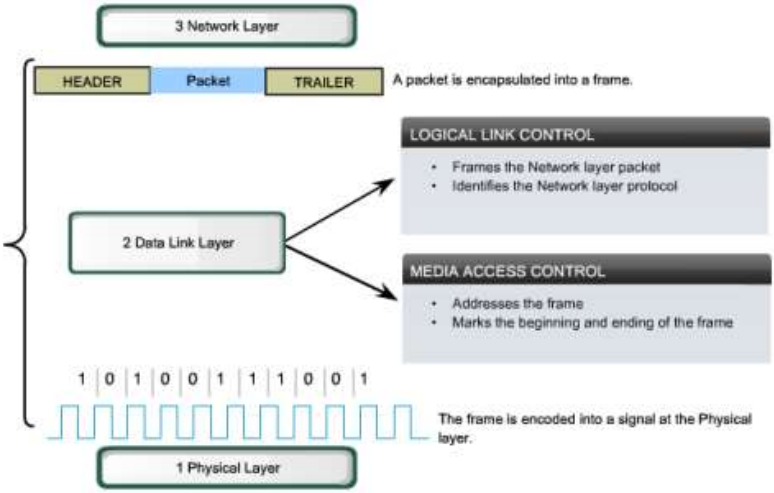
6.2.2 Struktur Umum

Struktur umum dari Data Link Layer terdiri dari dua sub-lapisan, yaitu *Logical Link Control* (LLC) dan *Media Access Control* (MAC) (Kurose and Ross, 2016). Pembagian ini memungkinkan standarisasi fungsi-fungsi lapisan Data Link Layer. Kedua sub-

lapisan ini bekerja sama untuk memastikan transmisi data yang efisien dan handal antara dua perangkat dalam suatu jaringan.

Sub-lapisan pertama, *Logical Link Control* (LLC), bertanggung jawab untuk mengatur komunikasi antara perangkat-perangkat di dalam suatu jaringan (Forouzan, 2007). Sub-lapisan ini menangani kontrol aliran data dan kontrol kesalahan, yang berarti ia memastikan bahwa data diterima dan dikirim dengan cara yang dapat diandalkan. Selain itu, LLC juga bertugas untuk memastikan bahwa data dikirim dengan urutan yang tepat dan tidak ada data yang hilang selama proses transmisi.

Sub-lapisan kedua, *Media Access Control* (MAC), memiliki peran yang berbeda namun sangat penting (Tanenbaum and Wetherall, 2010). MAC bertanggung jawab untuk mengendalikan akses perangkat ke media transmisi dalam jaringan. Dengan kata lain, MAC menentukan kapan dan bagaimana suatu perangkat dapat mengirim data melalui jaringan. Ini sangat penting dalam jaringan dimana banyak perangkat berusaha mengakses media transmisi secara bersamaan.



Gambar 6.1. Struktur Data Link Layer
(Sumber : Tanenbaum and Wetherall, 2010)

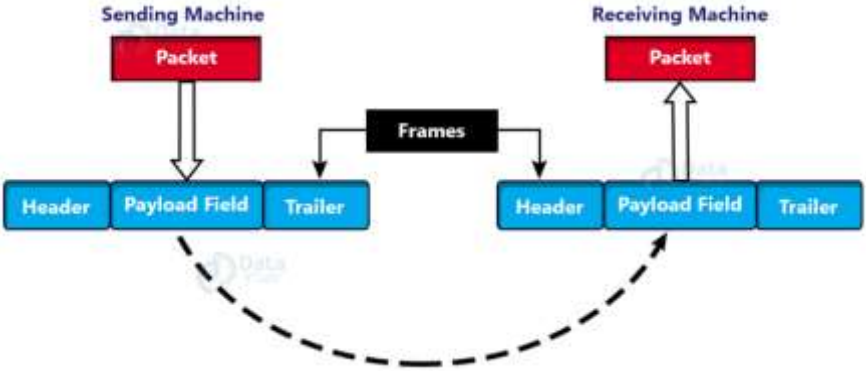
Selain itu, MAC juga menangani alamat fisik atau yang dikenal dengan MAC Address (Stallings and Brown, 2018). Setiap perangkat yang terhubung ke jaringan memiliki alamat MAC yang unik, yang digunakan untuk mengidentifikasi perangkat tersebut dalam jaringan. Alamat MAC ini sangat penting dalam proses komunikasi data, karena memastikan bahwa data dikirim ke perangkat yang benar.

6.3 Elemen Dasar Data Link Layer

Dalam komunikasi data melalui jaringan komputer, pengiriman informasi harus dilakukan dengan cara yang terstruktur dan efisien. Dua konsep kunci dalam hal ini adalah Framing dan Format Frame. Bagian ini akan menjelaskan kedua konsep ini dengan detail, termasuk teknik framing yang berbeda, komponen frame, dan contoh format frame dalam Ethernet.

6.3.1 Framing dan Format Frame

Framing adalah proses pembagian aliran data menjadi frame yang lebih kecil untuk transmisi. Dalam lapisan Data Link, framing memainkan peran penting dalam pengiriman data yang efisien dan akurat. Frame adalah unit data yang terdiri dari header, payload, dan trailer. Header berisi informasi kontrol seperti alamat sumber dan tujuan, sedangkan trailer biasanya berisi checksum untuk deteksi kesalahan.



Gambar 6.2. Frame
(Sumber : Tanenbaum and Wetherall, 2010)

Contoh frame, misalkan ada aliran data "1101011011", dan kita menggunakan metode framing berdasarkan jumlah bit tetap, misalnya 4 bit per frame. Maka framing akan menghasilkan frame-frame sebagai berikut: "1101", "0110", "1011".
Framing bertujuan untuk:

1. Memudahkan sinkronisasi antara pengirim dan penerima.
2. Memungkinkan deteksi dan koreksi kesalahan.
3. Mengatur aliran data untuk menghindari kelebihan beban pada penerima.

Ada beberapa teknik framing yang umum digunakan dalam jaringan komputer, antara lain:

1. Framing Berdasarkan Panjang
   Frame ditandai dengan panjangnya, dan panjang frame ditambahkan dalam header.
2. Framing Berdasarkan Karakter
   Frame dimulai dan diakhiri dengan karakter khusus, seperti SOF (*Start of Frame*) dan EOF (*End of Frame*).
3. Framing Berdasarkan Bit
   Bit khusus digunakan untuk menandai awal dan akhir frame.

Struktur atau skema yang digunakan untuk menyusun bagian-bagian dari frame disebut sebagai format frame. Format ini biasanya mencakup alamat sumber, alamat tujuan, panjang data, data itu sendiri, dan checksum. Ethernet adalah teknologi jaringan yang umum digunakan, dan format frame-nya adalah sebagai berikut:

1. Preamble: 7 byte, digunakan untuk sinkronisasi.
2. *Start Frame Delimiter* (SFD): 1 byte, menandai awal frame.
3. Alamat Tujuan (DA): 6 byte, menentukan tujuan frame.
4. Alamat Sumber (SA): 6 byte, menentukan sumber frame.
5. Type/Length: 2 byte, menentukan jenis protokol atau panjang data.
6. Data dan Padding: 46-1500 byte, berisi data dan padding jika diperlukan.
7. *Frame Check Sequence* (FCS): 4 byte, berisi nilai CRC untuk deteksi kesalahan.

Gambar 6.3. Ethernet Frame Format
(Sumber : www.geeksforgeeks.org)

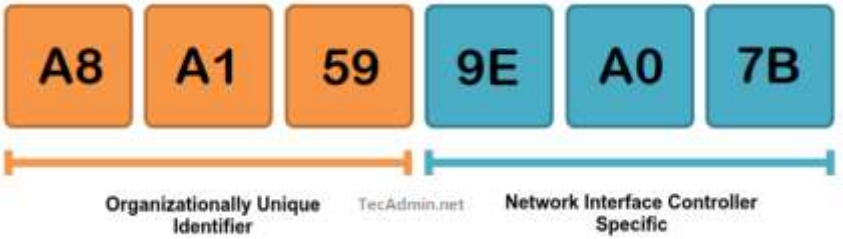
6.3.2 Alamat Fisik (Physical Addressing)

Alamat fisik, juga dikenal sebagai alamat MAC (*Media Access Control*), adalah alamat unik yang diberikan kepada setiap perangkat keras jaringan seperti kartu jaringan (NIC). Alamat ini digunakan dalam lapisan Data Link dari model OSI untuk mengidentifikasi perangkat pada jaringan lokal. Alamat fisik adalah alamat enam byte yang biasanya ditulis dalam format heksadesimal. Setiap byte dipisahkan oleh titik dua atau tanda hubung. Misalnya, alamat MAC seperti "00:1A:2B:3C:4D:5E" adalah

alamat fisik yang valid. Produsen perangkat keras biasanya memberikan alamat MAC ini, dan itu bersifat unik di seluruh dunia. Ini berarti tidak ada dua perangkat yang memiliki alamat MAC yang sama. Alamat fisik digunakan oleh switch dalam jaringan untuk mengarahkan frame ke tujuan yang tepat.

Dalam konteks jaringan Ethernet, alamat fisik memainkan peran penting dalam proses pengiriman dan penerimaan data. Ketika perangkat ingin mengirim data ke perangkat lain dalam jaringan lokal, ia menggunakan alamat MAC tujuan untuk mengarahkan data ke perangkat yang tepat. Switch dalam jaringan membaca alamat MAC tujuan dan menggunakan tabel MAC yang disimpan untuk menentukan port yang tepat untuk meneruskan frame. Jika alamat MAC tujuan tidak ditemukan dalam tabel, switch akan menyiarkan frame ke semua port kecuali port asal. Ini dikenal sebagai proses pembelajaran MAC, di mana switch "mempelajari" alamat MAC dari perangkat yang terhubung dan menyimpannya dalam tabel MAC.

Alamat fisik tidak hanya penting dalam pengiriman data, tetapi juga dalam aspek keamanan jaringan (Yusuf and Gunawan, 2021). Dengan menggunakan fitur seperti pengikatan alamat MAC, administrator jaringan dapat membatasi akses ke jaringan berdasarkan alamat MAC perangkat. Ini berarti hanya perangkat dengan alamat MAC yang telah disetujui yang dapat mengakses jaringan. Selain itu, alamat fisik juga digunakan dalam beberapa protokol jaringan tingkat tinggi, seperti *Address Resolution Protocol* (ARP), yang menghubungkan alamat IP dengan alamat MAC yang sesuai. Meskipun alamat fisik bersifat unik dan tetap, beberapa perangkat keras dan perangkat lunak memungkinkan penggantian alamat MAC, yang bisa digunakan untuk tujuan yang sah atau penyalahgunaan.



Gambar 6.4. MAC Address
(Sumber : www. tecadmin.net)

6.3.3 Kontrol Aliran (*Flow Control*)

Kontrol Aliran atau *Flow Control* adalah mekanisme penting dalam komunikasi data yang bertujuan untuk mengoordinasikan laju pengiriman data antara pengirim dan penerima. Ini memastikan bahwa pengirim tidak mengirim data lebih cepat daripada yang dapat diproses oleh penerima. Dalam jaringan komputer, kontrol aliran diperlukan untuk menghindari kelebihan beban pada penerima yang mungkin memiliki sumber daya terbatas seperti memori buffer. Ada beberapa teknik kontrol aliran yang umum digunakan, seperti kontrol aliran berbasis jendela dan kontrol aliran berbasis umpan balik. Kontrol aliran berbasis jendela menggunakan konsep "jendela" yang menentukan jumlah data yang dapat dikirim sebelum memerlukan pengakuan dari penerima. Kontrol aliran berbasis umpan balik, di sisi lain, memungkinkan penerima untuk mengirim umpan balik ke pengirim tentang kapasitasnya untuk menerima data lebih lanjut.

Salah satu teknik kontrol aliran yang terkenal adalah protokol Stop-and-Wait. Dalam protokol ini, pengirim mengirim satu frame dan menunggu pengakuan dari penerima sebelum mengirim frame berikutnya. Jika pengakuan tidak diterima dalam waktu yang ditentukan, pengirim akan mengirim ulang frame. Teknik ini sederhana tetapi tidak efisien, terutama dalam jaringan dengan latensi tinggi. Sebagai alternatif, protokol seperti TCP

menggunakan kontrol aliran berbasis jendela geser, di mana pengirim dapat mengirim sejumlah frame sebelum memerlukan pengakuan, dan jendela ini "digeser" seiring dengan pengiriman dan pengakuan. Ini memungkinkan penggunaan lebih efisien dari bandwidth dan sumber daya, tetapi juga lebih kompleks dalam implementasinya.

Kontrol aliran adalah aspek penting dari keandalan dalam komunikasi data. Tanpa kontrol aliran yang tepat, penerima mungkin menjadi kewalahan dengan data yang masuk, menyebabkan kehilangan data atau penurunan kinerja. Kontrol aliran juga berinteraksi erat dengan kontrol kesalahan, di mana mekanisme seperti pengakuan dan pengiriman ulang digunakan untuk memastikan integritas data. Dalam konteks jaringan yang kompleks dengan berbagai jenis perangkat dan kapasitas, kontrol aliran memungkinkan komunikasi yang lancar dan efisien antara perangkat dengan kecepatan dan kapasitas yang berbeda. Dengan demikian, kontrol aliran adalah komponen kunci dalam desain dan operasi jaringan komputer yang efektif dan andal.

6.3.4 Deteksi dan Koreksi Kesalahan (*Error Detection and Correction)*

Deteksi dan Koreksi Kesalahan adalah aspek penting dalam komunikasi data untuk memastikan integritas dan keakuratan informasi yang dikirimkan. Kesalahan dapat terjadi karena berbagai alasan, seperti gangguan sinyal, kehilangan data, atau masalah perangkat keras. Teknik deteksi kesalahan melibatkan penggunaan algoritma khusus yang memungkinkan penerima untuk mengetahui apakah ada kesalahan dalam data yang diterima. Salah satu metode yang umum digunakan adalah checksum, di mana nilai khusus dihitung berdasarkan data dan dikirim bersama dengan data itu sendiri. Penerima kemudian menghitung ulang nilai ini dan membandingkannya dengan nilai yang diterima untuk

mendeteksi kesalahan. Jika ada ketidakcocokan, maka diasumsikan ada kesalahan dalam transmisi.

Deteksi dan Koreksi Kesalahan adalah fundamental dalam banyak protokol komunikasi, termasuk protokol jaringan populer seperti TCP. Dalam TCP, misalnya, teknik seperti pengakuan dan pengiriman ulang digunakan bersama dengan checksum untuk memastikan integritas data. Jika penerima mendeteksi kesalahan dalam paket yang diterima, ia dapat meminta pengirim untuk mengirim ulang paket tersebut. Ini menunjukkan bagaimana deteksi dan koreksi kesalahan berinteraksi dengan mekanisme lain seperti kontrol aliran untuk memastikan komunikasi data yang efisien dan andal. Dalam dunia yang semakin terhubung, di mana data dikirimkan melalui jaringan yang kompleks dan sering kali tidak dapat diandalkan, teknik deteksi dan koreksi kesalahan tetap menjadi komponen kunci dalam desain dan operasi jaringan komputer yang sukses.

6.3.5 Kontrol Akses Media (*Media Access Control*)

Kontrol Akses Media (*Media Access Control* atau MAC) adalah prosedur yang mengatur bagaimana perangkat dalam jaringan dapat mengakses media untuk mengirim data. Dalam jaringan yang menggunakan media bersama, kontrol ini penting untuk mencegah tabrakan data dan memastikan pengiriman yang efisien. Beberapa metode umum yang digunakan termasuk CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*), yang mendeteksi tabrakan dalam Ethernet; CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*), yang menghindari tabrakan dalam Wi-Fi; Token Passing, di mana izin khusus diperlukan untuk mengirim; dan TDMA (*Time Division Multiple Access*), yang membagi waktu akses ke media dalam slot yang tetap.

Pentingnya Kontrol Akses Media terletak pada kemampuannya untuk memungkinkan komunikasi data yang

terkoordinasi dan andal. Tanpa kontrol yang tepat, tabrakan antara paket data dari perangkat yang berbeda dapat mengganggu komunikasi dan menurunkan kinerja jaringan. Kontrol Akses Media adalah komponen kunci dalam protokol jaringan seperti Ethernet dan Wi-Fi, dan pemahaman tentang cara kerjanya adalah esensial bagi siapa saja yang bekerja dalam bidang jaringan komputer. Dengan berbagai metode yang disesuaikan dengan kebutuhan spesifik jaringan, kontrol akses media memastikan bahwa data dapat ditransmisikan dengan lancar dan efisien dalam berbagai lingkungan jaringan.

6.4 Framing di Data Link Layer

6.4.1 Konsep Dasar Framing

Seperti yang telah dijelaskan sebelumnya, framing adalah salah satu aspek penting dalam komunikasi data, terutama pada lapisan Data Link Layer. Proses ini melibatkan pembagian aliran data menjadi frame atau paket yang lebih kecil untuk memudahkan transmisi. Framing membantu dalam mendeteksi dan mengoreksi kesalahan yang mungkin terjadi selama transmisi, sehingga integritas data dapat terjaga.

Framing dalam konteks jaringan komputer adalah proses pengorganisasian data yang dikirim dari satu perangkat ke perangkat lain dalam paket atau frame. Proses ini penting dalam komunikasi data untuk memastikan bahwa setiap bagian informasi diterima dengan urutan yang benar dan tanpa kesalahan.

Konsep framing membantu dalam mengidentifikasi awal dan akhir dari setiap paket data, sehingga penerima dapat dengan mudah memproses informasi yang diterima. Tanpa framing, aliran data yang kontinu akan sulit untuk dipisahkan menjadi unit yang berarti, dan kesalahan dalam satu bagian dapat mengganggu seluruh pesan.

Framing juga memungkinkan pengiriman informasi kontrol bersama dengan data itu sendiri. Informasi ini dapat mencakup

checksum untuk deteksi kesalahan, alamat pengirim dan penerima, serta informasi lain yang diperlukan untuk pengolahan data yang efektif. Dengan demikian, framing tidak hanya memfasilitasi pengiriman data tetapi juga membantu dalam pemeliharaan dan manajemen komunikasi antara perangkat.

Selain itu, framing memungkinkan pengelolaan lalu lintas dalam jaringan yang sibuk. Dengan membagi data menjadi frame yang dapat dikelola, perangkat dapat lebih mudah mengatur kapan dan bagaimana data dikirim, sehingga mengoptimalkan penggunaan bandwidth dan mengurangi kemungkinan tabrakan.

Secara keseluruhan, konsep framing adalah fondasi dari komunikasi data yang efisien dan handal. Tanpa proses ini, transmisi data dalam jaringan modern akan menjadi proses yang jauh lebih kompleks dan rentan terhadap kesalahan. Framing, dengan cara yang sederhana namun efektif, memungkinkan pengiriman data yang terstruktur dan terorganisir, yang merupakan kunci dari komunikasi digital yang sukses.

6.4.2 Teknik-teknik Framing: *Character Count, Flag Bytes* dengan *Byte Stuffing, Bit Stuffing*

Ada beberapa teknik framing yang umum digunakan, seperti framing karakter dan framing bit. Framing karakter menggunakan karakter khusus untuk menandai awal dan akhir frame, sedangkan framing bit menggunakan pola bit tertentu.

1. *Character Count* adalah teknik framing yang menggunakan jumlah karakter dalam frame sebagai informasi untuk menentukan batas frame. Teknik ini cukup sederhana dan langsung, di mana jumlah karakter dalam frame ditambahkan di awal frame untuk memberi tahu penerima berapa banyak karakter yang harus dibaca.
   Contoh:
   Data "HALO" akan dikirim sebagai "4HALO", di mana 4 adalah jumlah karakter dalam frame.

Teknik ini memiliki kelebihan dalam simplicitasnya, tetapi juga rentan terhadap kesalahan. Jika karakter hitungan rusak, seluruh frame bisa salah dibaca.

2. *Flag Bytes* dengan *Byte Stuffing* adalah teknik yang lebih kompleks. Teknik ini menggunakan byte khusus (flag) untuk menandai awal dan akhir frame. Jika flag muncul dalam data, maka akan dilakukan proses yang disebut Byte Stuffing.
   Contoh:
   Misalkan flag adalah "F". Data "HELFO" akan dikirim sebagai "FHELFOF". Jika ada karakter "F" dalam data, maka akan ditambahkan karakter khusus, misalnya "X". Jadi, "HELF" menjadi "FHELXF".
   Teknik ini lebih kuat dalam mendeteksi kesalahan dibandingkan dengan Character Count, tetapi juga lebih kompleks dalam implementasinya.
3. *Bit Stuffing* adalah teknik yang mirip dengan Byte Stuffing, tetapi diterapkan pada level bit. Jika ada pola bit tertentu yang digunakan sebagai flag, dan pola yang sama muncul dalam data, maka akan ditambahkan bit khusus untuk menghindari kebingungan.
   Contoh:
   Misalkan flag adalah "01111110". Jika pola ini muncul dalam data, maka akan ditambahkan bit 0 setelah lima bit 1 berurutan. Jadi, "01111110" dalam data menjadi "011111010".
   Bit Stuffing adalah teknik yang kuat dan fleksibel, tetapi juga memerlukan pemrosesan lebih untuk mengidentifikasi dan menangani bit tambahan.

6.5 Alamat Fisik di Data Link Layer

6.5.1 Konsep Dasar Alamat Fisik

Alamat fisik, juga dikenal sebagai alamat *Media Access Control* (MAC), adalah identifikasi unik yang diberikan kepada setiap perangkat keras jaringan, seperti kartu jaringan dalam komputer. Alamat ini digunakan dalam proses komunikasi pada lapisan Data Link Layer dalam model referensi OSI. Berikut adalah penjelasan tentang konsep dasar alamat fisik.

Alamat fisik biasanya terdiri dari 48 bit atau 6 byte. Format ini terbagi menjadi dua bagian: 24 bit pertama adalah kode produsen, dan 24 bit sisanya adalah nomor seri perangkat. Ini memastikan bahwa setiap alamat fisik adalah unik di seluruh dunia.

Alamat fisik digunakan untuk mengidentifikasi perangkat dalam jaringan lokal. Ketika data dikirim dari satu komputer ke komputer lain dalam jaringan yang sama, alamat fisik digunakan untuk menentukan perangkat tujuan. Ini berbeda dari alamat IP, yang digunakan untuk mengidentifikasi perangkat dalam jaringan yang lebih luas atau internet.

Ketika data dikirim dalam jaringan, informasi tentang alamat fisik pengirim dan penerima disertakan dalam frame. Switch atau hub dalam jaringan menggunakan alamat fisik ini untuk menentukan ke mana frame harus diteruskan. Ini memastikan bahwa data hanya dikirim ke perangkat tujuan yang tepat.

Alamat fisik biasanya ditetapkan oleh produsen perangkat keras dan disimpan dalam memori yang hanya bisa dibaca (ROM). Ini berarti alamat fisik tetap terkait dengan perangkat keras dan tidak berubah, meskipun perangkat tersebut dipindahkan ke jaringan yang berbeda.

Sebuah alamat fisik mungkin terlihat seperti ini: 1A-2B-3C-4D-5E-6F. Setiap pasangan karakter mewakili satu byte dari alamat 6 byte.

Konsep alamat fisik adalah bagian penting dari komunikasi jaringan. Ini memungkinkan perangkat dalam jaringan lokal untuk mengidentifikasi satu sama lain dan berkomunikasi dengan efisien. Tanpa alamat fisik, proses pengiriman data dalam jaringan lokal akan menjadi jauh lebih kompleks dan rentan terhadap kesalahan.

6.5.2 Peran dan Fungsi MAC Address

Berikut adalah penjelasan tentang peran dan fungsi alamat MAC dalam jaringan komputer.

1. Identifikasi Unik Perangkat
   Alamat MAC memberikan identifikasi unik untuk setiap perangkat dalam jaringan. Setiap alamat MAC adalah unik di seluruh dunia, yang memungkinkan perangkat untuk diidentifikasi secara spesifik dalam jaringan lokal maupun global.
2. Pengiriman Data dalam Jaringan Lokal
   Alamat MAC digunakan untuk mengarahkan data ke perangkat tujuan yang tepat dalam jaringan lokal (LAN). Ketika paket data dikirim, alamat MAC penerima dan pengirim disertakan dalam frame, memungkinkan switch atau router untuk mengarahkan paket ke perangkat yang tepat.
3. Keamanan Jaringan
   Dalam beberapa kasus, alamat MAC dapat digunakan untuk tujuan keamanan. Misalnya, administrator jaringan dapat membatasi akses ke jaringan berdasarkan alamat MAC, sehingga hanya perangkat dengan alamat MAC yang dikenali yang dapat terhubung.
4. Integrasi dengan Protokol Tingkat Tinggi
   Alamat MAC berfungsi pada lapisan Data Link Layer dan berinteraksi dengan protokol tingkat lebih tinggi seperti IP. Ini memungkinkan integrasi antara identifikasi perangkat

pada jaringan lokal dengan identifikasi dalam jaringan yang lebih luas atau internet.

5. Pembentukan Frame Data
   Dalam proses framing, alamat MAC pengirim dan penerima disertakan dalam frame data. Ini membantu dalam proses pengiriman dan penerimaan data, memastikan bahwa frame dikirim ke perangkat yang tepat dan memungkinkan penerima untuk mengidentifikasi pengirim.
6. Penggunaan dalam Jaringan Nirkabel
   Dalam jaringan Wi-Fi, alamat MAC digunakan untuk mengidentifikasi perangkat yang terhubung, memungkinkan router untuk mengelola koneksi dan mengalokasikan bandwidth dengan tepat.

Alamat MAC adalah komponen penting dalam jaringan komputer yang memungkinkan identifikasi unik perangkat dan pengelolaan komunikasi data yang efisien. Dari pengiriman data yang tepat hingga keamanan jaringan, peran alamat MAC sangat penting dalam memastikan operasi jaringan yang lancar dan handal.

6.6 Kontrol Aliran di Data Link Layer

6.6.1 Konsep Dasar Kontrol Aliran

Kontrol aliran adalah salah satu konsep fundamental dalam jaringan komputer yang mengatur seberapa cepat pengirim mengirimkan data ke penerima. Ini penting untuk memastikan bahwa pengirim tidak mengirimkan data lebih cepat daripada yang dapat diproses oleh penerima.

Kontrol aliran diperlukan untuk menciptakan keseimbangan antara pengirim dan penerima. Tanpa kontrol aliran, pengirim yang cepat dapat menghambat penerima yang lambat dengan data, menyebabkan buffer penerima penuh dan data hilang. Kontrol aliran bertujuan untuk mencegah situasi ini

dengan memastikan bahwa pengirim menyesuaikan laju pengiriman dengan kapasitas penerima.

Beberapa protokol jaringan telah dikembangkan untuk mengimplementasikan kontrol aliran, termasuk:

1. TCP (*Transmission Control Protocol*)
   TCP menggunakan kontrol aliran berbasis jendela untuk mengatur laju pengiriman data antara pengirim dan penerima.
2. XON/XOFF
   Ini adalah contoh kontrol aliran berbasis umpan balik di mana penerima mengirimkan sinyal khusus (XON atau XOFF) untuk memberi tahu pengirim kapan harus memulai atau menghentikan pengiriman.

Kontrol aliran sering dikaitkan dengan kontrol kemacetan, tetapi keduanya berbeda. Kontrol aliran berfokus pada hubungan antara pengirim dan penerima, sedangkan kontrol kemacetan berfokus pada menghindari kemacetan dalam jaringan secara keseluruhan.

Implementasi kontrol aliran yang efektif memerlukan pertimbangan beberapa faktor, termasuk kapasitas penerima, latensi jaringan, dan dinamika lalu lintas. Menemukan keseimbangan yang tepat dapat menjadi kompleks dan memerlukan pemahaman mendalam tentang karakteristik jaringan.

Kontrol aliran adalah aspek penting dari komunikasi jaringan yang memungkinkan pengiriman data yang efisien dan handal. Dengan mengatur laju pengiriman data sesuai dengan kapasitas penerima, kontrol aliran membantu mencegah kehilangan data dan memaksimalkan penggunaan sumber daya jaringan. Pemahaman tentang konsep dan teknik kontrol aliran adalah penting bagi siapa saja yang bekerja dalam bidang jaringan komputer.

6.6.2 Teknik Kontrol Aliran: Stop-and-Wait, Sliding Window

Ada beberapa teknik kontrol aliran yang umum digunakan, termasuk:

1. Teknik Stop-and-Wait adalah metode kontrol aliran yang sederhana dan mudah diimplementasikan.
   Cara Kerja: Pengirim mengirim satu frame dan kemudian berhenti (*stop*) dan menunggu (*wait*) sampai mendapatkan pengakuan (*acknowledgment*) dari penerima bahwa frame telah diterima dengan sukses. Baru setelah itu, pengirim akan mengirim frame berikutnya.
   Pengakuan: Penerima mengirimkan pengakuan setelah menerima frame. Jika pengirim tidak menerima pengakuan dalam waktu tertentu, frame dianggap hilang, dan pengirim akan mengirim ulang frame tersebut.
   Kelebihan: *Stop-and-Wait* mudah diimplementasikan dan memastikan bahwa setiap frame diterima sebelum yang berikutnya dikirim.
   Kekurangan: Teknik ini tidak efisien, terutama dalam jaringan dengan latensi tinggi, karena pengirim harus menunggu pengakuan setiap kali mengirim frame.
2. Sliding Window adalah teknik kontrol aliran yang lebih kompleks dan efisien. Berikut adalah detail dari teknik ini:
   Cara Kerja: Pengirim dan penerima menegosiasikan "jendela" atau jumlah frame yang dapat dikirim sebelum memerlukan pengakuan. Pengirim dapat terus mengirim frame dalam jumlah ini tanpa perlu menunggu pengakuan setiap kali.
   Jendela Pengirim dan Penerima: Pengirim memiliki jendela yang menunjukkan frame mana yang diizinkan untuk dikirim, sedangkan penerima memiliki jendela yang menunjukkan frame mana yang diharapkan diterima. Jendela ini "meluncur" seiring dengan pengiriman dan penerimaan frame.

Pengakuan: Penerima mengirimkan pengakuan untuk frame yang diterima, dan pengirim menyesuaikan jendelanya berdasarkan pengakuan ini.
Kelebihan: Sliding Window memungkinkan pengiriman yang lebih cepat dan penggunaan bandwidth yang lebih efisien dibandingkan dengan Stop-and-Wait.
Kekurangan: Implementasi Sliding Window lebih kompleks, dan kesalahan dalam pengelolaan jendela dapat menyebabkan masalah dalam pengiriman.

6.7 Deteksi dan Koreksi Kesalahan di Data Link Layer

Seperti penjelasan sebelumnya bahwa lapisan Data Link bertanggung jawab untuk menciptakan koneksi yang handal antara dua perangkat yang berkomunikasi dalam jaringan. Pada lapisan ini, data yang dikirimkan dipecah menjadi frame dan diberikan informasi tambahan untuk memastikan bahwa data diterima dengan benar oleh penerima. Namun, dalam proses transmisi, data dapat mengalami berbagai gangguan yang menyebabkan kesalahan, seperti gangguan sinyal, kehilangan data, atau kerusakan data (Samuel, 2019).

Untuk mengatasi masalah ini, berbagai teknik deteksi dan koreksi kesalahan telah dikembangkan. Teknik-teknik ini bertujuan untuk mengidentifikasi dan, jika mungkin, memperbaiki kesalahan yang terjadi selama transmisi data. Dari teknik sederhana seperti Checksum dan Parity Bits hingga metode yang lebih canggih seperti *Cyclic Redundancy Check* (CRC) dan Hamming Code, berbagai pendekatan telah diaplikasikan untuk menjaga integritas data.

Pembahasan ini akan mengulas secara mendalam tentang Konsep Dasar Deteksi dan Koreksi Kesalahan, Teknik Deteksi Kesalahan seperti Checksum, Parity Bits, dan CRC, serta Teknik Koreksi Kesalahan termasuk Hamming Code dan

Forward Error Correction (FEC). Analisis ini ditujukan untuk mahasiswa, peneliti, dan profesional di bidang jaringan komputer yang ingin memahami lebih dalam tentang bagaimana teknologi modern menjaga keandalan komunikasi data dalam dunia yang semakin terkoneksi.

6.7.1 Konsep Dasar Deteksi dan Koreksi Kesalahan

Deteksi kesalahan adalah proses mengidentifikasi apakah ada kesalahan yang terjadi dalam transmisi data. Dalam komunikasi data, berbagai faktor seperti gangguan sinyal, kehilangan data, atau kerusakan perangkat dapat menyebabkan kesalahan dalam data yang diterima. Berikut adalah beberapa konsep dasar dalam deteksi kesalahan:

1. Redundansi: Untuk mendeteksi kesalahan, informasi tambahan (redundansi) sering ditambahkan ke data. Informasi ini memungkinkan penerima untuk memeriksa apakah ada kesalahan dalam data yang diterima.
2. Pengakuan dan Pengulangan: Jika penerima mendeteksi kesalahan dalam frame, ia dapat meminta pengirim untuk mengirim ulang frame tersebut. Ini adalah pendekatan sederhana tetapi efektif untuk memastikan integritas data.

Sementara deteksi kesalahan hanya mengidentifikasi adanya kesalahan, koreksi kesalahan adalah proses lebih lanjut yang mencoba memperbaiki kesalahan tersebut tanpa perlu pengulangan. Berikut adalah beberapa konsep dasar dalam koreksi kesalahan:

1. Kode Koreksi Kesalahan: Teknik koreksi kesalahan sering menggunakan kode khusus yang tidak hanya dapat mendeteksi kesalahan tetapi juga menentukan di mana kesalahan terjadi dan bagaimana memperbaikinya.
2. Penggunaan Redundansi: Seperti dalam deteksi kesalahan, redundansi juga digunakan dalam koreksi kesalahan. Namun, lebih banyak informasi redundan diperlukan untuk

memungkinkan sistem tidak hanya mendeteksi kesalahan tetapi juga memperbaikinya.

Deteksi dan koreksi kesalahan adalah aspek penting dari komunikasi data yang handal. Tanpa mekanisme ini, kesalahan dalam transmisi dapat menyebabkan data yang diterima berbeda dari yang dikirim, yang dapat mengakibatkan masalah dalam aplikasi yang bergantung pada transmisi data yang akurat.

Konsep dasar deteksi dan koreksi kesalahan melibatkan penggunaan informasi redundan untuk mengidentifikasi dan, jika mungkin, memperbaiki kesalahan dalam data yang diterima. Teknik-teknik ini adalah bagian integral dari banyak protokol komunikasi dan memiliki peran penting dalam memastikan integritas dan keandalan komunikasi data dalam jaringan komputer.

6.7.2 Teknik Deteksi Kesalahan*: Checksum, Parity Bits, Cyclic Redundancy Check* (CRC)

Teknik-teknik ini bertujuan untuk mengidentifikasi kesalahan dalam transmisi data, sehingga tindakan korektif dapat diambil untuk memastikan integritas data. Dalam pembahasan berikut, kita akan mengulas tiga teknik deteksi kesalahan yang umum digunakan, yaitu *Checksum, Parity Bits, dan Cyclic Redundancy Check* (CRC), serta memahami bagaimana masing-masing teknik ini berfungsi dalam mendeteksi kesalahan dalam komunikasi data.

1. Checksum

   Checksum adalah teknik yang sederhana namun efektif untuk mendeteksi kesalahan dalam blok data.

   Cara Kerja: Pengirim menghitung jumlah total dari semua bit dalam blok data dan menyimpan hasilnya sebagai nilai checksum. Nilai ini dikirim bersama dengan data. Penerima melakukan perhitungan yang sama pada data yang diterima

dan membandingkan hasilnya dengan checksum yang dikirim. Jika keduanya cocok, data dianggap bebas dari kesalahan.

Kelebihan: Checksum mudah dihitung dan tidak memerlukan banyak pemrosesan.

Kekurangan: Tidak efektif dalam mendeteksi kesalahan yang saling mengimbangi, seperti jika dua bit berubah dalam cara yang saling mengimbangi.

Penerapan: Checksum sering digunakan dalam protokol komunikasi tingkat tinggi seperti TCP dan IP.

2. *Parity Bits*

   Parity Bits adalah teknik deteksi kesalahan yang menambahkan satu bit ekstra ke data.

   Cara Kerja: Pengirim menambahkan bit ekstra (bit paritas) sehingga jumlah total bit 1 dalam data adalah genap (paritas genap) atau ganjil (paritas ganjil). Penerima memeriksa bit paritas untuk mendeteksi kesalahan.

   Kelebihan: Metode yang sangat sederhana dan efisien.

   Kekurangan: Hanya dapat mendeteksi kesalahan ganjil, sehingga tidak efektif jika ada jumlah bit yang salah dalam kelipatan dua.

   Penerapan: Parity Bits sering digunakan dalam komunikasi serial dan penyimpanan data.

3. *Cyclic Redundancy Check* (CRC)

   CRC adalah teknik yang lebih canggih yang menggunakan operasi matematika polinomial.

   Cara Kerja: Pengirim menggunakan polinomial pembagi yang telah disepakati untuk membagi data dan mengirim sisa pembagian (CRC) bersama dengan data. Penerima melakukan pembagian yang sama dan membandingkan CRC untuk mendeteksi kesalahan.

   Kelebihan: Sangat efektif dalam mendeteksi banyak jenis kesalahan, termasuk perubahan dalam urutan bit.

Kekurangan: Lebih kompleks untuk dihitung dibandingkan dengan Checksum dan Parity Bits.
Penerapan: CRC digunakan dalam berbagai protokol jaringan seperti Ethernet.

Teknik deteksi kesalahan seperti Checksum, Parity Bits, dan CRC adalah bagian penting dari komunikasi data yang handal. Masing-masing teknik ini memiliki kelebihan dan kekurangan yang membuatnya cocok untuk aplikasi yang berbeda. Checksum dan Parity Bits adalah metode yang lebih sederhana dan cepat, sedangkan CRC menawarkan deteksi kesalahan yang lebih kuat tetapi lebih kompleks. Pemilihan teknik yang tepat tergantung pada kebutuhan dan karakteristik jaringan yang spesifik, dengan pertimbangan terhadap efisiensi, keandalan, dan kompleksitas.

6.7.3 Teknik Koreksi Kesalahan: *Hamming Code, Forward Error Correction* (FEC)

1. *Hamming Code*
   Hamming Code adalah teknik koreksi kesalahan yang ditemukan oleh Richard Hamming. Teknik ini memungkinkan deteksi dan koreksi otomatis dari kesalahan tunggal-bit.
   Cara Kerja: Hamming Code menambahkan bit paritas pada posisi yang merupakan pangkat dari dua (1, 2, 4, 8, dll.) dalam data. Bit paritas ini dihitung sehingga mereka dan bit data yang mereka lindungi membentuk paritas genap atau ganjil. Jika ada kesalahan dalam transmisi, kombinasi bit paritas yang salah menunjukkan posisi bit yang salah.
   Kelebihan: Hamming Code efektif dalam mendeteksi dan mengoreksi kesalahan tunggal-bit dan mendeteksi kesalahan ganda-bit.
   Kekurangan: Tidak dapat mengoreksi kesalahan ganda-bit atau lebih.

Penerapan: Hamming Code digunakan dalam sistem komunikasi komputer dan aplikasi penyimpanan data.

2. *Forward Error Correction* (FEC)
   Forward Error Correction adalah teknik yang memungkinkan penerima untuk mengoreksi kesalahan tanpa perlu pengulangan dari pengirim.
   Cara Kerja: FEC menggunakan algoritma untuk menambahkan bit redundan ke data. Ini memungkinkan penerima untuk mendeteksi dan mengoreksi sejumlah kesalahan tanpa perlu berkomunikasi kembali dengan pengirim. Ada banyak skema FEC, termasuk kode blok, kode convolutional, dan kode turbo.
   Kelebihan: FEC sangat efektif dalam lingkungan di mana pengulangan tidak praktis, seperti transmisi satelit atau siaran langsung.
   Kekurangan: Menambahkan redundansi ekstra dapat meningkatkan kebutuhan bandwidth.
   Penerapan: FEC digunakan dalam berbagai aplikasi, termasuk transmisi data nirkabel, siaran televisi digital, dan komunikasi satelit.

Teknik koreksi kesalahan seperti *Hamming Code* dan *Forward Error Correction* memainkan peran penting dalam memastikan integritas data dalam komunikasi jaringan. Sementara Hamming Code menawarkan pendekatan yang lebih sederhana untuk mendeteksi dan mengoreksi kesalahan tunggal-bit, FEC menyediakan solusi yang lebih kuat dan fleksibel untuk mengoreksi sejumlah kesalahan tanpa perlu pengulangan. Pemilihan teknik yang tepat tergantung pada kebutuhan spesifik dari aplikasi dan karakteristik jaringan, termasuk keandalan yang diinginkan, latensi, dan bandwidth yang tersedia.

6.8 Kontrol Akses Media di Data Link Layer

Di balik kemudahan komunikasi yang terjadi pada Jaringan Komputer, terdapat serangkaian proses kompleks yang memastikan bahwa data dapat ditransmisikan dengan efisien dan akurat antara perangkat yang berbeda dalam jaringan. Salah satu aspek krusial dalam transmisi data ini adalah Kontrol Akses Media (*Media Access Control* - MAC) yang berada pada lapisan Data Link dalam model referensi OSI.

Kontrol Akses Media adalah mekanisme yang mengatur bagaimana perangkat dalam jaringan berkomunikasi di media bersama. Tanpa kontrol yang tepat, jika dua perangkat atau lebih mencoba mengirim data secara bersamaan, akan terjadi tabrakan yang mengakibatkan kegagalan dalam transmisi data. Oleh karena itu, berbagai protokol Kontrol Akses Media telah dikembangkan untuk mengatur akses ke media transmisi dan memastikan bahwa data dapat ditransmisikan dengan lancar dan tanpa tabrakan.

Dalam pembahasan berikut, kita akan mengulas lebih dalam tentang Konsep Dasar Kontrol Akses Media dan beberapa protokol utama yang digunakan dalam praktek, termasuk CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*), CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*), dan Token Passing. Analisis ini akan memberikan pemahaman yang mendalam tentang bagaimana perangkat dalam jaringan berkoordinasi untuk berbagi media transmisi, serta bagaimana teknologi modern telah mengoptimalkan proses ini untuk efisiensi dan keandalan.

6.8.1 Konsep Dasar Kontrol Akses Media

Kontrol Akses Media adalah elemen krusial dalam jaringan komputer yang mengatur bagaimana perangkat-perangkat dalam jaringan dapat mengakses media transmisi untuk mengirim dan menerima data. Dalam jaringan yang menggunakan media bersama, kontrol akses media bertujuan untuk mencegah tabrakan

data yang dapat terjadi ketika dua perangkat atau lebih mencoba mengirim data secara bersamaan.

Ada beberapa metode dasar yang digunakan untuk mengontrol akses media, termasuk:

1. Akses Terkontrol: Dalam metode ini, perangkat harus mendapatkan izin sebelum mengakses media. Ini membantu mencegah tabrakan tetapi bisa menjadi proses yang lambat.
2. Akses Bersamaan (*Contention*): Perangkat bersaing untuk mengakses media dan menggunakan algoritma khusus untuk menentukan kapan mengirim data.
3. Akses Terbagi: Media dibagi berdasarkan waktu atau saluran, dan setiap perangkat diberikan slot atau saluran khusus. Contohnya adalah *Time Division Multiple Access* (TDMA) dan *Frequency Division Multiple Access* (FDMA).

Kontrol Akses Media memiliki peran penting dalam memastikan transmisi data yang efisien dan handal. Tanpa kontrol yang tepat, tabrakan data dapat terjadi dengan mudah, yang mengakibatkan penurunan kinerja jaringan dan potensi kehilangan data. Dengan mengatur bagaimana perangkat berkomunikasi di media bersama, Kontrol Akses Media memungkinkan berbagai aplikasi dan layanan jaringan berfungsi dengan lancar dan efisien.

6.8.2 Protokol Kontrol Akses Media: CSMA/CD, CSMA/CA, Token Passing

Protokol Kontrol Akses Media, seperti CSMA/CD, CSMA/CA, dan Token Passing, adalah mekanisme yang mengatur bagaimana perangkat dalam jaringan berkomunikasi di media bersama, mencegah tabrakan, dan memastikan transmisi data yang handal.

1. CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*)

   CSMA/CD adalah protokol yang digunakan terutama dalam jaringan Ethernet.

Cara Kerja: Perangkat mendengarkan media untuk memastikan tidak ada transmisi lain yang sedang berlangsung. Jika media bebas, perangkat mengirim data. Jika terjadi tabrakan, perangkat berhenti mengirim dan mencoba lagi setelah waktu tunggu acak.

Kelebihan: CSMA/CD efisien dalam mengelola akses ke media bersama dan dapat menangani beban jaringan yang tinggi.

Kekurangan: Dalam jaringan dengan latensi tinggi, deteksi tabrakan mungkin tidak efektif.

Penerapan: Digunakan dalam Ethernet kabel tembaga.

2. CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*)

   CSMA/CA adalah protokol yang dirancang untuk menghindari tabrakan daripada mendeteksinya.

   Cara Kerja: Seperti CSMA/CD, perangkat mendengarkan media sebelum mengirim. Namun, CSMA/CA juga menggunakan pengakuan (*acknowledgments*) dan penundaan waktu (*backoff*) untuk mengurangi risiko tabrakan.

   Kelebihan: Lebih efektif daripada CSMA/CD dalam lingkungan nirkabel di mana deteksi tabrakan lebih sulit.

   Kekurangan: Penggunaan pengakuan dan penundaan waktu dapat menambah latensi.

   Penerapan: Digunakan dalam Wi-Fi.

3. Token Passing

   Token Passing adalah protokol yang menggunakan "token" atau izin khusus untuk mengontrol akses ke media.

   Cara Kerja: Token beredar dalam jaringan, dan hanya perangkat yang memiliki token yang dapat mengirim data. Setelah mengirim, perangkat melepaskan token untuk perangkat berikutnya.

Kelebihan: Menghindari tabrakan sepenuhnya dan menjamin akses yang adil ke media.
Kekurangan: Kehilangan token atau kegagalan perangkat dapat mengganggu operasi jaringan.
Penerapan: Digunakan dalam jaringan seperti Token Ring dan FDDI.

Protokol Kontrol Akses Media seperti CSMA/CD, CSMA/CA, dan Token Passing adalah teknologi kunci yang memungkinkan perangkat dalam jaringan untuk berkomunikasi tanpa tabrakan. Masing-masing protokol ini memiliki cara kerja, kelebihan, kekurangan, dan penerapan yang berbeda, yang mencerminkan kebutuhan dan tantangan yang berbeda dalam desain jaringan. Pemahaman mendalam tentang protokol ini adalah penting bagi siapa saja yang bekerja dalam bidang jaringan komputer, karena mereka mendukung komunikasi data yang efisien dan handal yang menjadi dasar dari banyak layanan dan aplikasi modern.

6.9 Protokol di Data Link Layer

Dalam arsitektur jaringan komputer, lapisan Data Link atau lapisan tautan data memegang peran penting dalam menjamin komunikasi data yang handal antara dua perangkat yang berdekatan dalam jaringan. Lapisan ini bertanggung jawab atas pengiriman data antara perangkat-perangkat dalam jaringan lokal dan mengatur bagaimana data dikemas, ditransmisikan, dan diterima.

Beberapa protokol yang paling umum dan penting dalam lapisan Data Link adalah Ethernet, Wi-Fi (IEEE 802.11), dan *Point-to-Point Protocol* (PPP). Masing-masing dari protokol ini memiliki karakteristik, kegunaan, dan implementasi yang berbeda, yang mencerminkan berbagai kebutuhan dan aplikasi dalam jaringan komputer.

Dalam pembahasan berikut, kita akan membahas lebih dalam tentang masing-masing protokol ini, memahami bagaimana mereka bekerja, serta bagaimana mereka berkontribusi terhadap efisiensi dan fleksibilitas dalam komunikasi jaringan.

6.9.1 Ethernet

Ethernet adalah teknologi jaringan yang paling umum digunakan untuk menghubungkan perangkat dalam *Local Area Network* (LAN). Ditemukan pada tahun 1970-an, Ethernet telah menjadi standar industri untuk jaringan kabel, menyediakan cara yang handal dan efisien untuk mengirim dan menerima data antar perangkat dalam jaringan lokal.

Ethernet bekerja dengan menggunakan protokol *Carrier Sense Multiple Access with Collision Detection* (CSMA/CD) untuk mengontrol akses ke media transmisi. Perangkat dalam jaringan mendengarkan media dan hanya mengirim data jika media bebas dari transmisi lain. Jika terjadi tabrakan, perangkat akan berhenti mengirim dan mencoba lagi setelah waktu tunggu acak.

Beberapa komponen utama dari Ethernet:

1. Kabel dan Konektor: Ethernet biasanya menggunakan kabel tembaga seperti kabel UTP (*Unshielded Twisted Pair*) dengan konektor RJ-45.
2. Switch Ethernet: Switch digunakan untuk menghubungkan perangkat dalam jaringan dan mengarahkan data ke tujuan yang tepat.
3. Kartu Jaringan (NIC): Setiap perangkat yang terhubung ke jaringan Ethernet memerlukan NIC untuk berinteraksi dengan jaringan.

Ethernet telah berkembang seiring waktu, dengan berbagai versi yang menawarkan kecepatan yang berbeda, mulai dari 10 Mbps (Ethernet asli) hingga 100 Gbps (100 Gigabit Ethernet). Versi yang umum digunakan adalah Fast Ethernet (100 Mbps) dan Gigabit Ethernet (1 Gbps).

Adapun kelebihan dari Ethernet, dimana Ethernet menawarkan kecepatan tinggi, keandalan, dan biaya yang relatif rendah. Sedangkan kekurangannya adalah terbatas oleh jarak dan memerlukan kabel fisik, yang mungkin tidak selalu praktis.

Ethernet adalah teknologi jaringan yang telah menjadi standar dalam banyak aplikasi LAN. Dengan berbagai versi dan kecepatan, Ethernet menyediakan solusi yang fleksibel dan handal untuk kebutuhan jaringan lokal. Pemahaman tentang cara kerja, komponen, dan karakteristik Ethernet adalah penting bagi siapa saja yang bekerja dalam bidang jaringan komputer.

6.9.2 Wi-Fi (IEEE 802.11)

Wi-Fi adalah teknologi jaringan nirkabel yang memungkinkan perangkat untuk terhubung ke jaringan lokal tanpa kabel. Berdasarkan standar IEEE 802.11, Wi-Fi telah menjadi salah satu cara paling populer untuk mengakses internet dan jaringan lokal, baik di rumah, kantor, maupun tempat umum lainnya.

Wi-Fi bekerja dengan menggunakan gelombang radio untuk mengirim dan menerima data antara perangkat nirkabel dan titik akses (*access point*) atau router. Protokol seperti CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*) digunakan untuk mengatur transmisi data dan menghindari tabrakan.

Wi-Fi menawarkan kenyamanan dan fleksibilitas dengan koneksi nirkabel, memungkinkan mobilitas dan akses mudah. Namun kekurangannya, rentan terhadap gangguan dan masalah keamanan jika tidak dikonfigurasi dengan benar.

Beberapa komponen utama Wi-Fi diantaranya :

1. Titik Akses (*Access Point*): Titik akses adalah perangkat yang menghubungkan perangkat nirkabel ke jaringan kabel, seperti internet.
2. Kartu Jaringan Nirkabel: Perangkat seperti laptop, smartphone, dan tablet memiliki kartu jaringan nirkabel untuk berinteraksi dengan jaringan Wi-Fi.

Versi dan Kecepatan Wi-Fi sangat beragam. Ada beberapa versi standar IEEE 802.11, termasuk 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, dan 802.11ax. Masing-masing menawarkan kecepatan dan fitur yang berbeda, dengan 802.11ax (Wi-Fi 6) sebagai versi terbaru yang menawarkan kecepatan hingga 10 Gbps. Keamanan adalah pertimbangan penting dalam Wi-Fi. Protokol keamanan seperti WEP, WPA, dan WPA2 digunakan untuk mengenkripsi data dan melindungi jaringan dari akses yang tidak sah.

Wi-Fi (IEEE 802.11) adalah teknologi yang revolusioner yang telah mengubah cara kita mengakses dan berinteraksi dengan jaringan. Dengan berbagai versi dan fitur, Wi-Fi menyediakan solusi nirkabel yang handal dan nyaman untuk berbagai kebutuhan jaringan. Pemahaman tentang cara kerja, komponen, versi, dan keamanan Wi-Fi adalah penting bagi siapa saja yang bekerja dalam bidang jaringan komputer atau menggunakan teknologi ini dalam kehidupan sehari-hari.

6.9.3 Point-to-Point Protocol (PPP)

Point-to-Point Protocol (PPP) adalah protokol komunikasi data yang digunakan untuk menghubungkan dua perangkat secara langsung melalui jalur komunikasi serial. PPP sering digunakan dalam koneksi internet dial-up, serta dalam koneksi WAN (*Wide Area Network*) antara dua lokasi yang berbeda.

PPP bekerja dengan mengemas data ke dalam frame yang ditransmisikan antara dua perangkat melalui jalur komunikasi point-to-point. Protokol ini menyediakan fitur untuk otentikasi, negosiasi opsi, dan pengawasan koneksi.

PPP menyediakan koneksi yang sederhana dan efisien antara dua titik, dengan dukungan untuk otentikasi dan negosiasi opsi. Namun terbatas pada koneksi antara dua perangkat dan mungkin tidak sesuai untuk jaringan yang lebih kompleks
PPP beroperasi dalam beberapa fase, termasuk:

1. Fase Pembentukan Tautan (*Link Establishment*): Perangkat menegosiasikan opsi dan membentuk koneksi.
2. Fase Otentikasi (*Authentication*): Jika diperlukan, perangkat dapat mengautentikasi satu sama lain.
3. Fase Penghubungan Jaringan (*Network Layer Connection*): Perangkat menegosiasikan opsi untuk protokol lapisan jaringan yang digunakan (misalnya, IP).
4. Fase Terputus (*Termination*): Koneksi ditutup.

Komponen utama dari PPP, diantaranya:

1. Frame PPP: Data dikemas dalam frame PPP yang memiliki header dan trailer untuk mengidentifikasi dan mengontrol transmisi.
2. Protokol Otentikasi: PPP mendukung beberapa protokol otentikasi, termasuk PAP (*Password Authentication Protocol*) dan CHAP (*Challenge Handshake Authentication Protocol*).

Point-to-Point Protocol (PPP) adalah protokol yang penting dalam komunikasi data *point-to-point*, terutama dalam koneksi internet dan WAN. Dengan fitur-fitur seperti otentikasi dan negosiasi opsi, PPP menyediakan solusi yang fleksibel dan handal untuk koneksi langsung antara dua perangkat. Pemahaman tentang cara kerja, komponen, dan karakteristik PPP adalah penting bagi siapa saja yang bekerja dalam bidang jaringan komputer atau terlibat dalam pengaturan dan pemeliharaan koneksi *point-to-point*.

6.10 Ringkasan dan Masa Depan Data Link Layer

Lapisan Data Link atau lapisan tautan data merupakan salah satu komponen krusial dalam arsitektur jaringan komputer. Berfungsi sebagai penghubung antara lapisan fisik yang mengatur perangkat keras dan lapisan jaringan yang mengatur aliran data,

lapisan Data Link memainkan peran penting dalam mengendalikan cara data dikemas, ditransmisikan, dan diterima dalam jaringan.

Lapisan Data Link adalah lapisan kedua dalam model referensi OSI yang bertanggung jawab atas pengiriman data yang handal antara dua perangkat yang berdekatan dalam jaringan. Berikut adalah ringkasan dari komponen utama dan teknologi yang terkait dengan lapisan Data Link:

1. Framing: Data dikemas dalam frame yang berisi informasi kontrol dan alamat.
2. Protokol Kontrol Akses Media: Seperti CSMA/CD dalam Ethernet dan CSMA/CA dalam Wi-Fi.
3. Deteksi dan Koreksi Kesalahan: Teknik seperti Parity Bits, CRC, dan Hamming Code.
4. Kontrol Aliran: Teknik seperti Stop-and-Wait dan Sliding Window.
5. Protokol Utama: Termasuk Ethernet, Wi-Fi (IEEE 802.11), dan *Point-to-Point Protocol* (PPP).

Dalam beberapa dekade terakhir, teknologi dan protokol yang terkait dengan lapisan Data Link telah mengalami perkembangan yang signifikan. Dari Ethernet yang telah menjadi standar industri, Wi-Fi yang mengubah cara kita terhubung, hingga protokol point-to-point yang memungkinkan koneksi yang lebih spesifik, lapisan Data Link telah menjadi fondasi dari banyak inovasi dalam teknologi jaringan.

Dalam era teknologi yang terus berkembang, lapisan Data Link menghadapi beberapa tantangan:

1. Keamanan: Perlindungan terhadap serangan dan akses yang tidak sah menjadi semakin penting.
2. Integrasi dengan Teknologi Baru: Seperti IoT, 5G, dan teknologi nirkabel generasi berikutnya.
3. Skalabilitas: Kemampuan untuk mendukung jumlah perangkat yang semakin banyak dalam jaringan.

4. Efisiensi Energi: Penting dalam konteks perangkat mobile dan IoT.

Bersama dengan tantangan, ada juga peluang yang menarik:

1. Inovasi dalam Protokol Nirkabel: Dengan pertumbuhan teknologi nirkabel, ada ruang untuk inovasi dalam protokol dan standar.
2. Integrasi dengan Teknologi Cloud dan Edge Computing: Memungkinkan komputasi yang lebih efisien dan responsif.
3. Pengembangan Teknologi Green Networking: Fokus pada efisiensi energi dan dampak lingkungan.

Terakhir, lapisan Data Link adalah komponen kunci dalam arsitektur jaringan komputer, yang telah mengalami perkembangan signifikan seiring waktu. Dari teknologi kabel hingga nirkabel, dari LAN hingga WAN, lapisan Data Link telah beradaptasi untuk memenuhi kebutuhan yang terus berubah.

DAFTAR PUSTAKA

Forouzan, B.A. 2007. *Data Communications and Networking*. 4th Editio. The McGraw-Hill Companies, Inc.

Kurose, J. and Ross, K. 2016. *Computer Networking: A Top-Down Approach*. 7th edn. Pearson.

Samuel. 2019. 'Packet Loss Prevention System Failover Incident on Network Infrastructure', in *5Th International Conference On New Media Studies (CONMEDIA 2019)*. Universitas Multimedia Nusantara, STIKI Indonesia.

Stallings, W. 2013. *Data and Computer Communications*. 10th edn. Pearson.

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

Tanenbaum, A. and Wetherall, D. 2010. *Computer Networks*. 5th edn. Pearson.

Yusuf, G.N. and Gunawan, D. 2021. 'Smote and Random Forest Algorithm for Detecting DOS Attacks in Wireless Sensor Networks', in *15th International Conference on Innovative Computing, Information and Control (ICICIC2021)*. ICIC International.

BAB 7
ETHERNET SWITCHING

Oleh Arief Yanto Rukmana

7.1 Pendahuluan

Ethernet switching adalah teknologi dasar yang digunakan dalam jaringan komputer untuk memfasilitasi transmisi data dalam jaringan area lokal (LAN) (Vakharkar & Sakhare, 2022). Ini berfungsi sebagai jembatan antara perangkat, seperti komputer, server, printer, dan peralatan yang mendukung jaringan lainnya, memungkinkan untuk berkomunikasi satu sama lain secara efisien (Sujana, 2022). Tujuan utama dari switch Ethernet adalah untuk mengarahkan paket data dari sumber ke perangkat tujuan sambil mengoptimalkan kinerja jaringan dan meminimalkan tabrakan (George et al., 2022).

Inti dari Ethernet switching terletak pada konsep alamat *Media Access Control* (MAC). Setiap perangkat yang terhubung ke jaringan memiliki alamat MAC yang unik, yang ditetapkan ke kartu antarmuka jaringan (NIC). Ketika bingkai data memasuki sakelar Ethernet, ia memeriksa alamat MAC sumber bingkai dan memperbarui tabel alamat MAC-nya, menghubungkan alamat MAC dengan port sakelar yang sesuai. Proses ini dikenal sebagai pembelajaran alamat MAC. Semakin banyak frame tiba, switch membangun database alamat MAC dan port yang sesuai, yang memungkinkannya membuat keputusan penerusan data dengan lebih efisien (Kyriakakis et al., 2019; Painuly, n.d.).

Setelah menerima bingkai data, sakelar Ethernet menggunakan alamat MAC tujuan untuk menentukan port keluaran yang sesuai untuk meneruskan bingkai. Tidak seperti hub jaringan yang menyiarkan data ke semua perangkat yang

terhubung, sakelar Ethernet menggunakan pemfilteran bingkai. Itu hanya meneruskan frame ke port yang terkait dengan alamat MAC tujuan, secara signifikan mengurangi lalu lintas jaringan yang tidak perlu dan meningkatkan keamanan (Tokmakov et al., 2019).

Pergantian Ethernet juga membantu dalam segmentasi jaringan, memisahkan LAN menjadi domain tabrakan yang lebih kecil. Setiap port switch mewakili domain tabrakan individu, memungkinkan perangkat yang terhubung ke port ini untuk berkomunikasi tanpa mengalami tabrakan dengan perangkat di port lain (Alani & Al-Sadi, 2023). Selain itu, domain siaran ditentukan oleh sakelar, memastikan bahwa lalu lintas siaran hanya terbatas pada port tempat perangkat milik domain siaran yang sama terhubung.

Switch Ethernet beroperasi menggunakan berbagai metode switching, masing-masing dengan kelebihan dan keterbatasannya. Metode yang paling umum adalah store-and-forward switching. Dalam metode ini, sakelar memverifikasi integritas bingkai yang diterima sebelum meneruskannya (Mathew & Prabhu, 2017). Mekanisme pengecekan error ini memastikan bahwa hanya frame bebas error yang ditransmisikan, menjaga integritas data di seluruh jaringan. Namun, pengalihan store-and-forward memperkenalkan beberapa latensi karena pemrosesan yang terlibat (Gentile et al., 2021).

Metode alternatif adalah cut-through switching, di mana switch meneruskan frame segera setelah alamat MAC tujuan dikenali. Pendekatan ini mengurangi latensi dibandingkan dengan pengalihan store-and-forward tetapi tidak melakukan pemeriksaan kesalahan, yang dapat mengakibatkan frame yang rusak diteruskan (Csikor et al., 2020).

Untuk mengatasi trade-off antara latensi dan pemeriksaan kesalahan, pendekatan hibrid yang disebut pengalihan bebas fragmen, atau pengalihan cut-through yang dimodifikasi, diperkenalkan. Peralihan bebas fragmen memeriksa 64 byte

pertama dari bingkai untuk memverifikasi integritasnya sebelum meneruskan, memberikan keseimbangan antara pengurangan latensi dan deteksi kesalahan dasar (Halsall, 1995).

Ethernet switching adalah teknologi dasar dalam jaringan komputer, penting untuk transmisi data yang efisien dalam LAN. Dengan menggunakan pembelajaran alamat MAC, penerusan bingkai, dan metode switching seperti store-and-forward, cut-through, dan fragment-free, switch Ethernet memungkinkan komunikasi tanpa batas antar perangkat sambil mempertahankan segmentasi jaringan dan meningkatkan integritas dan kinerja data. Pergantian Ethernet adalah landasan jaringan modern, memastikan konektivitas yang andal dan efisien untuk berbagai aplikasi (Rukmana, Rahman, et al., 2023).

7.2 Konsep Dasar Ethernet Switching

Pergantian Ethernet adalah konsep dasar dalam jaringan komputer, berfungsi sebagai mekanisme penting untuk transmisi data dalam jaringan area lokal (LAN). Pada intinya, switch Ethernet beroperasi sebagai jembatan antara perangkat yang berbeda, seperti komputer, server, dan printer, di dalam jaringan (Sujana, 2022). Tujuan utama dari switch Ethernet adalah untuk secara efisien mengarahkan paket data dari sumber ke tujuan, meningkatkan kinerja jaringan dan mengurangi tabrakan, sekaligus memungkinkan perangkat untuk berkomunikasi dengan lancer (Adhikari et al., 2022).

Salah satu elemen kunci dalam pengalihan Ethernet adalah alamat *Media Access Control* (MAC), pengidentifikasi unik yang ditetapkan untuk setiap kartu antarmuka jaringan (NIC) perangkat yang terhubung ke jaringan. Ketika bingkai data memasuki sakelar, ia memeriksa alamat MAC sumber dan menyimpannya dalam tabel alamat MAC bersama dengan port yang sesuai di mana bingkai diterima. Proses ini dikenal sebagai pembelajaran alamat MAC. Saat lebih banyak frame tiba, switch memperbarui tabel MAC-nya,

memungkinkannya membuat keputusan penerusan data dengan lebih efisien (Rashid & Chaturvedi, 2019).

Setelah menerima bingkai data, sakelar Ethernet menggunakan alamat MAC tujuan untuk menentukan port keluaran yang sesuai untuk meneruskan bingkai. Tidak seperti hub jaringan tradisional, yang menyiarkan data ke semua perangkat yang terhubung, sakelar Ethernet menggunakan pemfilteran bingkai, memungkinkannya mengirim bingkai hanya ke port penerima yang dituju. Ini menghasilkan pengurangan lalu lintas yang tidak perlu, meningkatkan keamanan jaringan dan kinerja (Rukmana, 2023).

Pergantian Ethernet juga membantu segmentasi jaringan, memisahkannya menjadi domain tabrakan. Setiap port pada switch mewakili domain tabrakan individu, memungkinkan perangkat yang terhubung ke port ini untuk berkomunikasi tanpa mengalami tabrakan dengan perangkat lain di port yang berbeda. Selain itu, domain siaran juga ditentukan oleh sakelar, memastikan bahwa lalu lintas siaran hanya terbatas pada port tempat perangkat milik domain siaran yang sama terhubung (Cao et al., 2020).

Ada berbagai metode switching yang digunakan oleh switch Ethernet, masing-masing dengan kelebihan dan keterbatasannya. Metode yang paling umum adalah store-and-forward switching, dimana switch memverifikasi integritas frame yang diterima sebelum meneruskannya. Ini membantu dalam deteksi kesalahan dan memastikan bahwa hanya frame bebas kesalahan yang ditransmisikan. Namun, metode ini menimbulkan beberapa latensi karena pemrosesan yang terlibat (Thangaramya et al., 2019).

Alternatifnya, pengalihan cut-through melibatkan penerusan frame segera setelah alamat MAC tujuan dikenali, mengurangi latensi. Namun, cut-through switching tidak melakukan pemeriksaan error dan mungkin meneruskan frame yang rusak. Untuk mengatasinya, ada pendekatan hibrid yang disebut fragment-free switching, juga dikenal sebagai modified cut-

through switching, yang memeriksa 64 byte pertama dari frame untuk memverifikasi integritasnya sebelum diteruskan.

Aspek penting lainnya dari switching Ethernet adalah penerapan LAN Virtual (VLAN). VLAN memungkinkan administrator jaringan untuk secara logis mengelompokkan LAN fisik menjadi beberapa LAN virtual, mengisolasi perangkat berdasarkan persyaratan fungsional, pertimbangan keamanan, atau afiliasi departemen. VLAN dapat dikonfigurasi berdasarkan port (VLAN berbasis port) atau dengan menggunakan teknik penandaan seperti IEEE 802.1Q (VLAN berbasis tag).

Switching Ethernet adalah landasan jaringan komputer modern, menyediakan transmisi data yang efisien, meningkatkan kinerja jaringan, dan meningkatkan keamanan. Dengan menggunakan tabel alamat MAC, penerusan bingkai, dan mekanisme pemfilteran, sakelar Ethernet memungkinkan perangkat berkomunikasi dengan mulus sambil mempertahankan segmentasi jaringan untuk aliran data yang optimal. Fleksibilitas VLAN semakin meningkatkan organisasi dan keamanan jaringan, menjadikan peralihan Ethernet sebagai teknologi yang sangat diperlukan dalam dunia jaringan komputer (Kyriakakis et al., 2019).

7.3 Operasi Switching Ethernet

Operasi switching Ethernet adalah proses mendasar yang terletak di jantung jaringan komputer modern. Ini melibatkan penerusan bingkai data yang efisien dalam jaringan area lokal (LAN) menggunakan sakelar Ethernet. Pengoperasian switch Ethernet didasarkan pada interaksi antara komponen perangkat kerasnya dan algoritma switching yang mendasarinya (Gentile et al., 2021).

Inti dari Ethernet switching adalah alamat Media Access Control (MAC). Setiap perangkat yang terhubung ke jaringan memiliki alamat MAC unik yang ditetapkan ke kartu antarmuka

jaringan (NIC). Ketika bingkai data memasuki sakelar Ethernet, ia memeriksa alamat MAC sumber bingkai dan memperbarui tabel alamat MAC-nya. Proses ini dikenal sebagai pembelajaran alamat MAC. Dengan mempertahankan tabel ini, switch membuat database yang mengaitkan alamat MAC dengan port switch yang sesuai melalui mana frame diterima (Yang et al., 2019).

Saat sakelar menerima bingkai data, ia menggunakan alamat MAC tujuan untuk membuat keputusan penerusan. Switch mencari alamat MAC tujuan di tabel alamat MAC untuk menentukan port output yang sesuai untuk frame. Jika alamat MAC ditemukan di tabel, sakelar meneruskan bingkai hanya ke port yang terkait dengan alamat MAC tujuan. Proses ini dikenal sebagai penerusan bingkai dan memungkinkan peralihan untuk mengarahkan lalu lintas secara efisien (Tokmakov et al., 2019).

Ada berbagai metode penerusan bingkai yang digunakan oleh sakelar Ethernet. Metode yang paling umum adalah store-and-forward switching. Dalam pendekatan ini, sakelar terlebih dahulu memverifikasi integritas bingkai yang diterima sebelum meneruskannya. Ini memeriksa kesalahan, memastikan bahwa hanya frame bebas kesalahan yang ditransmisikan, yang membantu menjaga integritas data di seluruh jaringan. Namun, metode ini menimbulkan beberapa latensi karena waktu yang diperlukan untuk pemeriksaan kesalahan sebelum meneruskan.

Pendekatan lain adalah cut-through switching, dimana switch meneruskan frame segera setelah mengenali alamat MAC tujuan. Ini mengurangi latensi dibandingkan dengan store-and-forward, karena sakelar tidak menunggu seluruh frame diterima sebelum meneruskan. Namun, cut-through switching tidak melakukan pemeriksaan kesalahan, yang dapat menyebabkan frame yang rusak diteruskan (Hiltz, 1994).

Untuk mengatasi masalah latensi dan pemeriksaan kesalahan, pendekatan hibrid yang disebut pengalihan bebas fragmen, atau pengalihan cut-through yang dimodifikasi,

diperkenalkan. Dalam metode ini, switch memeriksa 64 byte pertama dari frame, yang dikenal sebagai preamble dan pembatas frame mulai, untuk memeriksa kesalahan. Jika frame bebas dari kesalahan, frame akan meneruskannya. Ini memberikan keseimbangan antara pengurangan latensi dan deteksi kesalahan dasar (Quarterman & Hoskins, 1986).

Algoritme switching adaptif juga digunakan dalam switch Ethernet modern untuk secara dinamis menyesuaikan metode penerusannya berdasarkan kondisi jaringan. Algoritme ini dapat beralih antara mode simpan-dan-maju, cut-through, atau bebas fragmen tergantung pada jenis bingkai, tingkat kesalahan, dan tingkat kemacetan di jaringan, sehingga mengoptimalkan kinerja.

Operasi switching Ethernet adalah proses penting yang memungkinkan frame data diteruskan secara efisien dalam LAN. Dengan menggunakan pembelajaran alamat MAC, penerusan bingkai, dan algoritme pengalihan seperti store-and-forward, cut-through, dan bebas fragmen, sakelar Ethernet memastikan komunikasi yang mulus antar perangkat dengan tetap menjaga integritas data dan meminimalkan latensi. Teknik switching ini memainkan peran penting dalam keberhasilan dan efisiensi jaringan komputer modern (Zhang et al., 2019).

7.4 Virtual LAN (VLAN) dan Trunking

Virtual LAN (VLAN) dan Trunking (Gentile et al., 2021) adalah konsep penting dalam jaringan komputer modern, memberikan administrator jaringan alat yang ampuh untuk melakukan segmentasi dan mengelola jaringan secara efisien (Poularakis et al., 2019).

VLAN, kependekan dari Virtual LAN, adalah metode yang secara logis membagi jaringan area lokal (LAN) fisik menjadi beberapa domain siaran. Segmentasi logis ini memungkinkan administrator jaringan untuk mengelompokkan perangkat berdasarkan faktor-faktor seperti departemen, fungsi, atau

persyaratan keamanan, bahkan jika perangkat ini secara fisik terletak di sakelar yang berbeda. Dengan mengimplementasikan VLAN, lalu lintas siaran dalam setiap VLAN diisolasi, mengurangi lalu lintas jaringan yang tidak perlu dan meningkatkan keamanan (Long, 2022).

VLAN dapat dikonfigurasi dengan dua cara utama: VLAN berbasis port dan VLAN berbasis tag (IEEE 802.1Q). Dalam VLAN berbasis port, setiap port switch ditetapkan ke VLAN tertentu, artinya perangkat yang terhubung ke port yang sama milik VLAN yang sama. Metode ini sederhana untuk disiapkan dan dikelola tetapi kurang fleksibel, karena perangkat harus terhubung secara fisik ke port VLAN yang sesuai (Gentile et al., 2021; Long, 2022).

VLAN berbasis tag, di sisi lain, menggunakan penandaan untuk mengidentifikasi keanggotaan VLAN. Ketika sebuah frame memasuki switch, itu ditandai dengan pengidentifikasi VLAN, yang memungkinkan switch untuk membedakan VLAN mana yang menjadi milik frame. Hal ini memungkinkan administrator jaringan untuk secara fleksibel menetapkan keanggotaan VLAN ke perangkat terlepas dari lokasi port fisiknya, menawarkan opsi skalabilitas dan organisasi jaringan yang lebih besar.

Di jaringan besar, mengelola konfigurasi VLAN di beberapa sakelar bisa menjadi tantangan. Di sinilah VLAN Trunking berperan. Trunking memungkinkan beberapa VLAN dibawa melalui satu tautan fisik antar sakelar, menyederhanakan desain jaringan dan mengurangi jumlah koneksi yang diperlukan. Protokol trunking yang paling umum digunakan adalah IEEE 802.1Q, yang memasukkan tag VLAN ke setiap frame untuk menunjukkan keanggotaan VLAN-nya (Rahmanzi et al., 2020).

Trunking memastikan bahwa frame milik VLAN yang berbeda tetap terpisah saat diangkut melalui tautan yang sama. Pemisahan ini dicapai melalui penggunaan tag VLAN. Ketika frame diteruskan dari satu switch ke switch lainnya melalui link trunk, switch penerima memeriksa tag VLAN untuk menentukan VLAN

yang sesuai dengan frame tersebut. Proses ini memastikan bahwa frame dikirimkan hanya ke VLAN yang dimaksud dan tidak mengganggu yang lain (Robertazzi, 2000).

VLAN Trunking Protocol (VTP) adalah protokol penting yang digunakan untuk mengelola konfigurasi VLAN dalam jaringan dengan banyak sakelar. VTP memungkinkan switch untuk bertukar informasi VLAN, memastikan konsistensi di seluruh jaringan dan menyederhanakan manajemen VLAN. Hal ini memungkinkan untuk pembuatan, penghapusan, dan modifikasi VLAN pada satu switch, yang kemudian disebarkan ke switch lain dalam domain VTP, mengurangi beban administratif untuk mengonfigurasi VLAN satu per satu pada setiap switch.

Keutamaan VLAN dan Trunking merupakan komponen penting dari jaringan modern, menawarkan administrator jaringan kemampuan untuk membagi dan mengelola jaringan secara efektif. VLAN memberikan pemisahan logis dari domain siaran, meningkatkan keamanan dan kinerja, sementara trunking memungkinkan beberapa VLAN dibawa melalui satu tautan fisik, menyederhanakan desain dan manajemen jaringan. Dengan menggunakan teknologi ini, administrator jaringan dapat membuat arsitektur jaringan yang terukur, fleksibel, dan aman untuk memenuhi beragam kebutuhan organisasi modern (Rahmanzi et al., 2020).

7.5 Spanning Tree Protocol (STP)

Spanning Tree Protocol (STP) adalah protokol jaringan penting yang dirancang untuk mencegah loop dalam jaringan Ethernet dan memastikan stabilitas dan redundansi jalur jaringan. Ini beroperasi pada Lapisan Data Link (Lapisan 2) dari model OSI dan sangat penting dalam lingkungan di mana banyak sakelar saling terhubung untuk membuat topologi jaringan yang berlebihan (Zhang et al., 2019).

Kebutuhan akan STP muncul karena adanya potensi loop jaringan. Loop jaringan terjadi ketika beberapa jalur antara switch membuat rute alternatif untuk paket data, yang menyebabkan duplikasi dan banjir paket, yang dapat sangat menurunkan kinerja jaringan dan bahkan menyebabkan pemadaman jaringan (Poularakis et al., 2019).

STP mengatasi masalah ini dengan memilih satu "jembatan akar" dari semua sakelar yang saling terhubung dalam jaringan. Jembatan akar bertindak sebagai titik referensi pusat untuk seluruh jaringan. Setelah root bridge dipilih, STP menghitung jalur terpendek dari root bridge ke setiap switch dalam jaringan, yang dikenal sebagai "biaya jalur root". Biaya jalur root menentukan jalur yang paling efisien untuk transmisi data, menghindari loop.

STP mencapai pencegahan loop dengan secara selektif memblokir jalur redundan tertentu. Ini menunjuk satu port pada setiap switch sebagai "port root", yang merupakan port dengan biaya jalur root terendah, yang mengarah ke jembatan root. Semua port lain pada setiap sakelar kemudian ditempatkan di salah satu dari beberapa status: "ditunjuk", "bergantian", atau "dinonaktifkan".

"Port yang ditunjuk" pada sakelar adalah port dengan biaya jalur akar terendah yang mengarah ke jembatan akar untuk segmen jaringan tertentu. Hanya port yang ditunjuk yang diizinkan untuk secara aktif meneruskan lalu lintas di segmen tersebut. Semua port lain di segmen itu, termasuk yang ada di sakelar lain, ditempatkan dalam status pemblokiran untuk mencegah loop.

"Port alternatif" adalah port cadangan yang dapat menjadi port yang ditunjuk jika port yang ditunjuk saat ini gagal. Port alternatif disimpan dalam keadaan dibuang tetapi siap untuk diambil alih jika diperlukan.

"Port yang dinonaktifkan" adalah port yang telah ditentukan oleh STP sebagai redundan dan sepenuhnya

dinonaktifkan untuk mencegah transmisi data melalui port tersebut.

STP juga menggunakan proses yang dikenal sebagai fase "mendengarkan" dan "belajar" ketika port bertransisi dari status pemblokiran ke status penerusan. Proses ini memungkinkan STP untuk menetapkan jalur bebas loop sebelum mengizinkan penerusan data aktif pada port, sehingga mencegah potensi gangguan jaringan selama konvergensi.

Jika terjadi perubahan jaringan, seperti kegagalan tautan atau penambahan sakelar baru, STP akan secara otomatis mengonfigurasi ulang jaringan untuk beradaptasi dengan perubahan sambil mempertahankan topologi bebas loop. Waktu konvergensi jaringan dapat bervariasi berdasarkan versi STP yang digunakan dan ukuran jaringan tetapi biasanya dalam beberapa detik (Havinal et al., 2015).

Spanning Tree Protocol (STP) adalah mekanisme penting dalam jaringan Ethernet untuk mencegah loop, memastikan stabilitas jaringan, dan memelihara redundansi. Dengan memilih root bridge, menghitung biaya root path, dan memblokir redundant path secara selektif, STP menciptakan topologi loop-free dan memungkinkan transmisi data yang efisien melalui switch yang saling terhubung. Kemampuan STP untuk beradaptasi secara dinamis terhadap perubahan jaringan memastikan infrastruktur jaringan yang andal dan kuat (Csikor et al., 2020).

7.6 Link Aggregation (EtherChannel)

Agregasi Tautan, juga dikenal sebagai EtherChannel atau Bundling Tautan, adalah teknologi jaringan yang menggabungkan beberapa tautan Ethernet fisik menjadi satu tautan logis (Qiu et al., 2020). Tautan logis ini muncul sebagai satu koneksi bandwidth tinggi antara dua perangkat, seperti sakelar atau router, yang memungkinkan peningkatan kecepatan transfer data dan peningkatan toleransi kesalahan (Sadiku & Akujuobi, 2022).

Tujuan utama dari Agregasi Tautan adalah untuk mengumpulkan bandwidth tautan individu untuk membuat koneksi berkapasitas lebih tinggi, sehingga mencapai throughput data yang lebih tinggi dan meningkatkan kinerja jaringan (Gerovitch, 2008). Ini sangat berguna dalam skenario di mana satu tautan mungkin tidak cukup untuk menangani permintaan lalu lintas jaringan, atau dalam situasi di mana redundansi dan ketersediaan tinggi diperlukan (Pióro & Medhi, 2004).

Proses Agregasi Tautan melibatkan pembuatan antarmuka logis, yang dikenal sebagai EtherChannel, yang dikonfigurasi di kedua ujung tautan agregat (Cononelos & Oliva, 1993). EtherChannel ini bertindak sebagai antarmuka virtual, menyatukan tautan fisik menjadi satu koneksi agregat. Perangkat di kedua ujung EtherChannel menegosiasikan konfigurasi agregasi menggunakan protokol seperti *Link Aggregation Control Protocol* (LACP) atau *Port Aggregation Protocol* (PAgP).

LACP dan PAgP memfasilitasi negosiasi dinamis Agregasi Tautan antara perangkat yang kompatibel. Protokol ini memungkinkan perangkat untuk bertukar informasi tentang kemampuannya dan menyepakati jumlah tautan yang akan digabungkan, mode operasional, dan parameter lainnya. Dengan membentuk dan mengelola EtherChannel secara dinamis, protokol-protokol ini memastikan operasi optimal tautan agregat dan kemampuan beradaptasi terhadap perubahan jaringan.

Proses Link Aggregation dapat beroperasi dalam dua mode utama: mode statis dan mode dinamis. Dalam mode statis, administrator secara manual mengonfigurasi parameter agregasi, menentukan tautan mana yang harus menjadi bagian dari EtherChannel dan algoritme penyeimbangan beban yang akan digunakan. Mode statis lebih mudah untuk dikonfigurasi tetapi tidak memiliki fleksibilitas untuk beradaptasi dengan perubahan jaringan secara dinamis (Strinati & Barbarossa, 2021).

Mode dinamis, menggunakan LACP atau PAgP, lebih umum digunakan karena menyediakan negosiasi tautan otomatis dan beradaptasi dengan perubahan jaringan. Dalam mode dinamis, perangkat bertukar paket protokol untuk menentukan apakah akan membentuk EtherChannel dan bagaimana menyeimbangkan lalu lintas lintas tautan agregat secara efektif (Salih et al., 2020).

Penyeimbangan muatan adalah aspek penting dari Agregasi Tautan, karena mendistribusikan lalu lintas data ke seluruh tautan agregat untuk memaksimalkan pemanfaatannya. Algoritme penyeimbangan muatan yang berbeda, seperti alamat IP tujuan-sumber, alamat MAC tujuan-sumber, atau port TCP/UDP tujuan-sumber, dapat digunakan untuk mencapai distribusi beban yang efisien (Halsall, 1995).

Jika terjadi kegagalan tautan di EtherChannel, Agregasi Tautan memberikan toleransi kesalahan dengan mengalihkan lalu lintas secara cepat ke tautan operasional yang tersisa. Deteksi kegagalan dan mekanisme pemulihan link di LACP atau PAgP memfasilitasi failover link yang lancar, meminimalkan gangguan jaringan.

Agregasi Tautan (EtherChannel) adalah teknologi jaringan yang kuat yang menggabungkan beberapa tautan Ethernet fisik ke dalam koneksi bandwidth tinggi yang logis. Dengan menggabungkan link, Link Aggregation meningkatkan throughput data, meningkatkan kinerja jaringan, dan menyediakan redundansi dan toleransi kesalahan (George et al., 2022). Penggunaan protokol seperti LACP atau PAgP memastikan negosiasi tautan dinamis dan kemampuan beradaptasi, menjadikan Agregasi Tautan alat yang berharga dalam desain jaringan modern (Hammond & O'Reilly, 1986).

7.7 Operasi Switching Ethernet

Keamanan switch Ethernet adalah aspek penting dari manajemen jaringan dan memainkan peran penting dalam menjaga data, mencegah akses tidak sah, dan melindungi dari potensi ancaman dunia maya (Piqueira et al., 2005). Mengonfigurasi dan mengelola sakelar dengan aman sangat penting untuk menjaga integritas dan kerahasiaan jaringan (Bishop, 2004).

Salah satu langkah keamanan mendasar untuk sakelar Ethernet adalah keamanan port. Keamanan port memungkinkan administrator jaringan untuk mengontrol perangkat mana yang dapat terhubung ke port switch tertentu. Administrator dapat mengonfigurasi sakelar untuk menerima lalu lintas hanya dari alamat MAC tertentu, yang secara efektif membatasi akses ke perangkat resmi. Ini mencegah perangkat yang tidak sah terhubung ke jaringan dan membantu mengurangi potensi risiko keamanan (Govindan et al., 2019).

Serangan melompat VLAN merupakan masalah keamanan potensial di lingkungan VLAN. Serangan ini terjadi ketika penyerang memperoleh akses tidak sah ke VLAN selain dari yang awalnya ditugaskan. Untuk mencegah lompatan VLAN, administrator jaringan dapat menerapkan teknik seperti daftar kontrol akses VLAN (VACL) atau VLAN pribadi (PVLAN). VACL memungkinkan pemfilteran lalu lintas antar VLAN, sementara PVLAN menyediakan lapisan isolasi tambahan, membatasi komunikasi antar perangkat dalam VLAN yang sama.

Sakelar Ethernet rentan terhadap berbagai serangan *Spanning Tree Protocol* (STP), yang dapat menyebabkan gangguan jaringan dan pelanggaran keamanan. Untuk melindungi dari serangan STP, administrator jaringan dapat mengimplementasikan fitur keamanan STP seperti BPDU Guard dan Root Guard. Penjaga BPDU mencegah sakelar yang tidak sah berpartisipasi dalam STP dengan menonaktifkan port yang menerima paket Unit Data

Protokol Jembatan (BPDU). Root Guard, di sisi lain, melindungi dari switch tidak sah yang mencoba menjadi root bridge dengan memblokir port yang tidak ditunjuk sebagai root port.

Pertimbangan keamanan penting lainnya untuk sakelar Ethernet adalah pembaruan firmware dan perangkat lunak. Memperbarui firmware sakelar secara teratur dengan tambalan keamanan terbaru membantu mengatasi kerentanan yang diketahui dan memastikan bahwa sakelar dilindungi dari ancaman yang muncul.

Langkah-langkah keamanan fisik juga penting dalam melindungi sakelar Ethernet dari akses fisik yang tidak sah. Administrator jaringan harus menempatkan sakelar di lokasi yang aman, seperti ruang server yang terkunci, dan membatasi akses fisik hanya untuk personel yang berwenang. Selain itu, mengaktifkan fitur keamanan port seperti penguncian alamat MAC dapat mencegah penyerang memasukkan perangkat yang tidak sah ke port switch.

Keamanan switch Ethernet adalah pendekatan multifaset yang melibatkan konfigurasi kontrol akses, mencegah lompatan VLAN, melindungi dari serangan STP, dan memelihara firmware terkini. Menerapkan langkah-langkah keamanan ini meningkatkan ketahanan jaringan dan membantu melindungi data sensitif dari akses tidak sah dan potensi ancaman. Dengan mengatasi masalah keamanan secara proaktif, administrator jaringan dapat memastikan integritas dan kerahasiaan jaringan Ethernet (Grigorjew et al., 2021).

7.8 Operasi Switching Ethernet

Memecahkan masalah pengalihan Ethernet adalah keterampilan penting bagi administrator jaringan untuk memastikan kelancaran fungsi jaringan area lokal (LAN). Saat menghadapi masalah dengan sakelar Ethernet, ada beberapa

masalah dan alat umum yang dapat membantu dalam proses pemecahan masalah (West, 2022).

Salah satu masalah utama dalam switching Ethernet adalah masalah konektivitas jaringan. Ketika perangkat tidak dapat berkomunikasi satu sama lain atau mengakses sumber daya di jaringan, administrator perlu mengidentifikasi akar masalahnya. Penyebab umum masalah konektivitas meliputi konfigurasi VLAN yang salah, port sakelar yang salah konfigurasi, atau kesalahan kabel fisik. Dengan memverifikasi pengaturan VLAN, memeriksa konfigurasi port, dan menguji kabel, administrator dapat mengisolasi masalah dan mengambil tindakan korektif yang sesuai (Sadiku & Akujuobi, 2022).

Masalah lain yang sering ditemui adalah broadcast storms atau network loops. Ini dapat menyebabkan lalu lintas siaran yang berlebihan, membanjiri jaringan dan menyebabkan gangguan komunikasi. Untuk mengatasi masalah tersebut, administrator dapat menggunakan Spanning Tree Protocol (STP) untuk mencegah loop dan mengonfigurasi pengaturan STP, seperti prioritas port dan biaya jalur, untuk memastikan arus lalu lintas dan redundansi yang efisien (Foley et al., 1994).

Performa jaringan yang lambat adalah masalah lain yang mungkin muncul. Waktu respons yang lambat antar perangkat dapat disebabkan oleh lalu lintas jaringan yang berlebihan, hambatan dalam jaringan, atau penyeimbangan muatan yang tidak efisien. Administrator dapat menggunakan alat pemantauan jaringan untuk mengidentifikasi area dengan lalu lintas tinggi dan melakukan penyesuaian keseimbangan muatan, seperti menyesuaikan pengaturan agregasi tautan, untuk mengoptimalkan distribusi data (Bishop, 2004).

Duplikasi alamat MAC di jaringan adalah masalah umum lainnya yang dapat menyebabkan konflik komunikasi dan ketidakstabilan jaringan. Administrator dapat menggunakan tabel alamat MAC pada sakelar untuk menemukan alamat MAC duplikat

dan kemudian melacak perangkat yang bermasalah untuk mengatasi masalah tersebut (Qiu et al., 2020).

Dalam beberapa kasus, port switch tidak responsif atau kegagalan switch lengkap dapat terjadi. Pemecahan masalah seperti itu memerlukan pemeriksaan konektivitas fisik sakelar, verifikasi daya dan indikator status tautan, dan pengujian dengan kabel dan perangkat yang dikenal baik (Puspita et al., 2022).

Administrator jaringan dapat menggunakan berbagai alat untuk membantu memecahkan masalah pengalihan Ethernet. Alat pemantauan jaringan, seperti SNMP (Simple Network Management Protocol) atau packet sniffer, membantu mengidentifikasi kemacetan jaringan, memantau pola lalu lintas, dan menunjukkan potensi masalah. Alat baris perintah, seperti ping dan traceroute, dapat digunakan untuk menguji konektivitas jaringan dan memverifikasi jalur perutean (Cononelos & Oliva, 1993).

Dokumentasi dan pencatatan sangat penting dalam proses pemecahan masalah (Sari et al., 2023). Menyimpan catatan terperinci tentang konfigurasi jaringan, perubahan, dan masalah masa lalu dapat membantu administrator dalam mengidentifikasi pola dan menyelesaikan masalah berulang secara efektif.

Pemecahan masalah pengalihan Ethernet memerlukan pendekatan metodis dan berbagai alat. Mengidentifikasi dan menyelesaikan masalah konektivitas jaringan, badai siaran, kinerja jaringan yang lambat, konflik alamat MAC, dan kegagalan sakelar sangat penting untuk memelihara jaringan yang stabil dan efisien. Administrator jaringan harus mengandalkan pengetahuan tentang prinsip-prinsip jaringan dan menggunakan alat yang tepat untuk mendiagnosis dan mengatasi masalah dengan segera, memastikan kinerja dan keandalan jaringan Ethernet yang optimal (Gerovitch, 2008).

7.9 Tren masa depan dalam switching Ethernet

Tren masa depan (Wakil et al., 2022) dalam switching Ethernet diperkirakan akan didorong oleh permintaan jaringan modern yang terus meningkat, didorong oleh teknologi baru dan arsitektur jaringan yang berkembang (Setiawan et al., 2023). Beberapa tren utama cenderung membentuk masa depan peralihan Ethernet dan berkontribusi pada jaringan yang lebih efisien, fleksibel, dan Tangguh (Robertazzi, 2000).

Salah satu tren menonjol dalam switching Ethernet adalah dorongan terus menerus untuk kecepatan data yang lebih tinggi. Karena lalu lintas jaringan terus meningkat secara eksponensial, permintaan untuk koneksi yang lebih cepat menjadi yang terpenting. Sakelar Ethernet cenderung melihat kemajuan dalam kecepatan transmisi data, dengan kapasitas yang lebih tinggi seperti 100 Gigabit Ethernet (100 Gbps) menjadi lebih umum, dan bahkan kecepatan yang lebih cepat seperti 400 Gigabit Ethernet (400 Gbps) mendapatkan daya tarik. Kecepatan yang lebih cepat ini akan mengakomodasi kebutuhan bandwidth aplikasi intensif data dan mendukung volume data yang terus berkembang yang mengalir melalui jaringan modern (Sadiku & Akujuobi, 2022).

Pergerakan menuju jaringan yang ditentukan perangkat lunak (SDN) dan kemampuan program jaringan adalah tren signifikan lainnya yang membentuk masa depan switching Ethernet. SDN memungkinkan administrator jaringan untuk memusatkan dan abstrak kontrol jaringan, membuatnya lebih gesit dan responsif terhadap tuntutan perubahan. Dengan SDN, sakelar dapat dikonfigurasi ulang dan disediakan secara dinamis, mengoptimalkan aliran lalu lintas dan alokasi sumber daya. Programabilitas jaringan memungkinkan pengembangan aplikasi khusus yang dapat berinteraksi dengan infrastruktur jaringan, memungkinkan pengelolaan dan otomatisasi tugas jaringan yang lebih efisien (Qiu et al., 2020).

Pergantian Ethernet juga diharapkan memainkan peran penting dalam pusat data dan jaringan cloud. Saat pusat data berevolusi untuk mengakomodasi beban kerja yang masif dan meningkatkan virtualisasi, sakelar Ethernet akan menjadi penting dalam menyediakan komunikasi kinerja tinggi dan latensi rendah di antara server dan sistem penyimpanan. Selain itu, kemajuan teknologi seperti *Data Center Bridging* (DCB) dan *Transparent Interconnection of Lots of Links* (TRILL) akan meningkatkan skalabilitas dan efisiensi jaringan pusat data (Cao et al., 2020).

Tren masa depan lainnya dalam peralihan Ethernet adalah integrasi kemampuan kecerdasan buatan (AI) (Harto et al., 2022) dan pembelajaran mesin (ML) (Andriana & Zulkarnain, 2018). Sakelar Ethernet yang digerakkan oleh AI dapat dengan cerdas menganalisis pola lalu lintas jaringan, memprediksi potensi masalah, dan secara proaktif menyesuaikan konfigurasinya untuk mengoptimalkan kinerja dan keamanan. Algoritme ML dapat membantu deteksi anomali dan pencegahan intrusi, meningkatkan pertahanan jaringan terhadap ancaman dunia maya (Xue & Calabretta, 2022).

Efisiensi dan keberlanjutan energi akan terus menjadi pertimbangan penting di masa depan switching Ethernet. Saat skala jaringan meningkat, mengurangi konsumsi daya menjadi lebih penting. Sakelar Ethernet cenderung menggabungkan fitur hemat energi dan manajemen daya cerdas untuk meminimalkan dampak lingkungan dan biaya operasionalnya (Khattak et al., 2020).

Implementasi switching Ethernet dalam aplikasi Industrial *Internet of Things* (IIoT) akan mendapatkan momentum. Karena lingkungan industri menjadi lebih terhubung dan membutuhkan komunikasi yang andal dan aman, sakelar Ethernet akan menjadi penting dalam menyediakan infrastruktur jaringan yang kuat untuk otomasi industri dan sistem kontrol (Kim et al., 2021).

Masa depan switching Ethernet ditandai dengan kecepatan data yang lebih tinggi, kemajuan dalam SDN dan programabilitas jaringan, pusat data dan inovasi jaringan cloud, integrasi kemampuan AI dan ML, efisiensi energi, dan perluasan ke aplikasi IIoT. Dengan merangkul tren ini, sakelar Ethernet akan terus berkembang untuk memenuhi permintaan jaringan modern yang terus meningkat (Rukmana, Zebua, et al., 2023), memungkinkan infrastruktur komunikasi yang lebih efisien, aman, dan dapat diskalakan (Olumuyiwa & Chen, 2022).

DAFTAR PUSTAKA

Adhikari, N., Logeshwaran, J., & Kiruthiga, T. 2022. The Artificially Intelligent Switching Framework for Terminal Access Provides Smart Routing in Modern Computer Networks. *BOHR International Journal of Smart Computing and Information Technology*, *3*(1), 45–50.

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

Andriana, A., & Zulkarnain, Z. 2018. Speech Recognition System with Linear Predictive Coding Method and Hidden Markov Model Using Matlab to Identify Speakers. *Jurnal Tiarsie*, *14*(1), 27–32.

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

Cao, K., Liu, Y., Meng, G., & Sun, Q. 2020. An overview on edge computing research. *IEEE Access*, *8*, 85714–85728.

Cononelos, T., & Oliva, M. 1993. Using computer networks to enhance foreign language/culture education. *Foreign Language Annals*, *26*(4), 527–534.

Csikor, L., Szalay, M., Rétvári, G., Pongrácz, G., Pezaros, D. P., & Toka, L. 2020. Transition to SDN is HARMLESS: Hybrid architecture for migrating legacy ethernet switches to SDN. *IEEE/ACM Transactions On Networking*, *28*(1), 275–288.

Foley, J. D., Van Dam, A., Feiner, S. K., Hughes, J. F., & Phillips, R. L. 1994. *Introduction to computer graphics* (Vol. 55). Addison-Wesley Reading.

Gentile, A. F., Fazio, P., & Miceli, G. 2021. A Survey on the Implementation and Management of Secure Virtual Private Networks (VPNs) and Virtual LANs (VLANs) in Static and Mobile Scenarios. *Telecom*, *2*(4), 430–445.

George, A. S., George, A. S. H., Baskar, T., & Pandey, D. 2022. The Transformation of the workspace using Multigigabit Ethernet. *Partners Universal International Research Journal*, *1*(3), 34–43.

Gerovitch, S. 2008. InterNyet: why the Soviet Union did not build a nationwide computer network. *History and Technology*, *24*(4), 335–350.

Govindan, V., Koteshwara, S., Das, A., Parhi, K. K., & Chakraborty, R. S. 2019. ProTro: a probabilistic counter based hardware trojan attack on FPGA based MACSec enabled ethernet switch. *Security, Privacy, and Applied Cryptography Engineering: 9th International Conference, SPACE 2019, Gandhinagar, India, December 3–7, 2019, Proceedings 9*, 159–175.

Grigorjew, A., Baier, C., Metzger, F., & Hoßfeld, T. 2021. Distributed Implementation of Deterministic Networking in Existing Non-TSN Ethernet Switches. *2021 IEEE International Conference on Communications Workshops (ICC Workshops)*, 1–6.

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

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

Harto, B., Saymsu, Y. L., Rukmana, A. Y., Komalasari, R., & Dwijayanti, A. 2022. Bibliometric Analysis of Transforming Leadership Education with Artificial Intelligence. In *1st Virtual Workshop on Writing Scientific Article for International Publication Indexed SCOPUS* (pp. 385–390). Sciendo. https://doi.org/10.2478/9788366675827-067

Havinal, R., Attimarad, G. V, & Prasad, M. N. G. 2015. Easr: Graph-based framework for energy efficient smart routing in manet using availability zones. *International Journal of*

Electrical and Computer Engineering (IJECE), *5*(6), 1381–1395.

Hiltz, S. R. 1994. *The virtual classroom: Learning without limits via computer networks*. Intellect Books.

Khattak, M. K., Tang, Y., Fahim, H., Rehman, E., & Majeed, M. F. 2020. Effective routing technique: Augmenting data center switch fabric performance. *IEEE Access*, *8*, 37372–37382.

Kim, H.-J., Choi, M.-H., Kim, M.-H., & Lee, S. 2021. Development of an ethernet-based heuristic time-sensitive networking scheduling algorithm for real-time in-vehicle data transmission. *Electronics*, *10*(2), 157.

Kyriakakis, E., Sparsø, J., & Schoeberl, M. 2019. Implementing time-triggered communication over a standard ethernet switch. *Proceedings of the Workshop on Fog Computing and the IoT*, 21–25.

Long, Z. 2022. Design for security configuration of remote management multi-VLAN switch based on VLAN trunking protocol. *5th International Conference on Computer Information Science and Application Technology (CISAT 2022)*, *12451*, 86–94.

Mathew, A., & Prabhu, B. 2017. A study on virtual local area network (Vlan) and inter-vlan routing. *International Journal of Current Engineering and Scientific Research (IJCESR)*, *4*(10).

Olumuyiwa, O., & Chen, Y. 2022. Virtual CANBUS and Ethernet Switching in Future Smart Cars Using Hybrid Architecture. *Electronics*, *11*(21), 3428.

Painuly, S. (n.d.). *QoS management for performance analysis of switched Ethernet networks*.

Pióro, M., & Medhi, D. 2004. *Routing, flow, and capacity design in communication and computer networks*. Elsevier.

Piqueira, J. R. C., Navarro, B. F., & Monteiro, L. H. A. 2005. Epidemiological models applied to viruses in computer networks. *Journal of Computer Science*, *1*(1), 31–34.

Poularakis, K., Llorca, J., Tulino, A. M., Taylor, I., & Tassiulas, L. 2019. Joint service placement and request routing in multi-cell mobile edge computing networks. *IEEE INFOCOM 2019-IEEE Conference on Computer Communications*, 10–18.

Puspita, H., Mulyana, A., Putro, H. P., Sihombing, F. A. H., Ikhram, F., Sutjiningtyas, S., Utomo, S., Andriani, A. D., Pratiwi, V., & Friadi, J. 2022. *Pengantar Teknologi Informasi*. Haura Utama.

Qiu, T., Chi, J., Zhou, X., Ning, Z., Atiquzzaman, M., & Wu, D. O. 2020. Edge computing in industrial internet of things: Architecture, advances and challenges. *IEEE Communications Surveys & Tutorials*, *22*(4), 2462–2488.

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

Rahmanzi, M. Z., Fitri, I., & Aningsih, A. 2020. Load Balancing Performance in Etherchannel Technology Using the VLAN Trunking Protocol (VTP) Method: Load Balancing Performance in Etherchannel Technology Using the VLAN Trunking Protocol (VTP) Method. *Jurnal Mantik*, *3*(4), 540–547.

Rashid, A., & Chaturvedi, A. 2019. Cloud computing characteristics and services: a brief review. *International Journal of Computer Sciences and Engineering*, *7*(2), 421–426.

Robertazzi, T. G. 2000. *Computer networks and systems: queueing theory and performance evaluation*. Springer Science & Business Media.

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

Rukmana, A. Y., Rahman, R., Afriyadi, H., Moeis, D., Setiawan, Z., Subchan, N., Magdalena, L., Singadji, M., El Rayeb, A., & Kusuma, A. T. A. P. 2023. *PENGANTAR SISTEM INFORMASI:*

Panduan Praktis Pengenalan Sistem Informasi & Penerapannya. PT. Sonpedia Publishing Indonesia.

Rukmana, A. Y., Zebua, R. S. Y., Aryanto, D., Nur'Aini, I., Ardiansyah, W., Adhicandra, I., & Setiawan, Z. 2023. *DUNIA MULTIMEDIA: Pengenalan dan Penerapannya*. PT. Sonpedia Publishing Indonesia.

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

Salih, Q. M., Rahman, M. A., Al-Turjman, F., & Azmi, Z. R. M. 2020. Smart routing management framework exploiting dynamic data resources of cross-layer design and machine learning approaches for mobile cognitive radio networks: A survey. *IEEE Access*, *8*, 67835–67867.

Sari, O. H., Rukmana, A. Y., Munizu, M., Novel, N. J. A., Salam, M. F., Hakim, R. M. A., Sukmadewi, R., & Purbasari, R. 2023. *DIGITAL MARKETING: Optimalisasi Strategi Pemasaran Digital*. PT. Sonpedia Publishing Indonesia.

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

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

Sujana, J. 2022. Implementasi Virtual Local Area Network Dengan Basis Inter-Vlan Routing Menggunakan Mikrotik: Implementasi Virtual Local Area Network Dengan Basis Inter-Vlan Routing Menggunakan Mikrotik. *Journal of Network and Computer Applications (ISSN: 2964-6669)*, *1*(1), 19–30.

Thangaramya, K., Kulothungan, K., Logambigai, R., Selvi, M., Ganapathy, S., & Kannan, A. 2019. Energy aware cluster and

neuro-fuzzy based routing algorithm for wireless sensor networks in IoT. *Computer Networks*, *151*, 211–223.

Tokmakov, K., Sarker, M., Domaschka, J., & Wesner, S. 2019. A case for data centre traffic management on software programmable ethernet switches. *2019 IEEE 8th International Conference on Cloud Networking (CloudNet)*, 1–6.

Vakharkar, S., & Sakhare, N. 2022. Critical analysis of virtual LAN and its advantages for the campus networks. *Mobile Computing and Sustainable Informatics: Proceedings of ICMCSI 2021*, 733–748.

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

West, J. 2022. *Data Communication and Computer Networks: A Business User's Approach*. Cengage Learning.

Xue, X., & Calabretta, N. 2022. Nanosecond optical switching and control system for data center networks. *Nature Communications*, *13*(1), 2257.

Yang, Z., Pan, C., Wang, K., & Shikh-Bahaei, M. 2019. Energy efficient resource allocation in UAV-enabled mobile edge computing networks. *IEEE Transactions on Wireless Communications*, *18*(9), 4576–4589.

Zhang, J., Guo, H., Liu, J., & Zhang, Y. 2019. Task offloading in vehicular edge computing networks: A load-balancing solution. *IEEE Transactions on Vehicular Technology*, *69*(2), 2092–2104.

BAB 8
NETWORK LAYER

Oleh Angga Aditya Permana

8.1 Pendahuluan

Gambar 8.1. Icon Network Layer
Sumber : www.istockphoto.com

Network layer merupakan salah satu komponen penting dalam model referensi OSI (*Open Systems Interconnection*) yang digunakan untuk menggambarkan dan mengatur bagaimana komunikasi data terjadi dalam jaringan komputer. Network layer berperan dalam mengatur rute pengiriman paket data dari sumber ke tujuan melalui berbagai jaringan yang berbeda, serta mengelola alamat-alamat logis yang dikenal sebagai alamat IP. Pada tingkat yang lebih mendalam, network layer berfungsi untuk menjaga efisiensi, kehandalan, dan skalabilitas komunikasi di dalam jaringan. (Sukaridhoto, 2014)

Salah satu tugas utama dari network layer adalah melakukan proses routing, di mana setiap paket data diberi informasi tentang rute yang harus diambil untuk mencapai tujuan akhirnya. Ini melibatkan pemilihan jalur terbaik berdasarkan berbagai faktor seperti jarak, beban jaringan, kondisi jaringan, dan lainnya. Protokol yang sering digunakan dalam tugas ini adalah protokol IP (*Internet Protocol*), yang memberikan alamat logis unik kepada setiap perangkat dalam jaringan dan memastikan pengiriman paket data yang tepat.

Selain itu, network layer juga bertanggung jawab atas fragmentasi dan reasemblasi paket data. Karena berbagai jaringan memiliki batasan ukuran paket yang berbeda-beda, network layer dapat memecah paket data besar menjadi bagian yang lebih kecil saat melewati jaringan dengan batasan ukuran tertentu. Di sisi penerima, network layer pada tujuan akan merakit kembali fragmen-fragmen tersebut menjadi paket data asli. Proses ini memastikan bahwa paket data dapat dikirim dan diterima dengan benar tanpa kehilangan informasi penting.

Secara keseluruhan, network layer berperan sebagai perantara antara lapisan-lapisan yang lebih tinggi dalam model OSI dengan fisik jaringan. Ini memberikan kemampuan untuk mengirimkan data melalui jaringan yang berbeda-beda dan mengatur rute serta alamat yang diperlukan untuk komunikasi yang efisien dan handal.

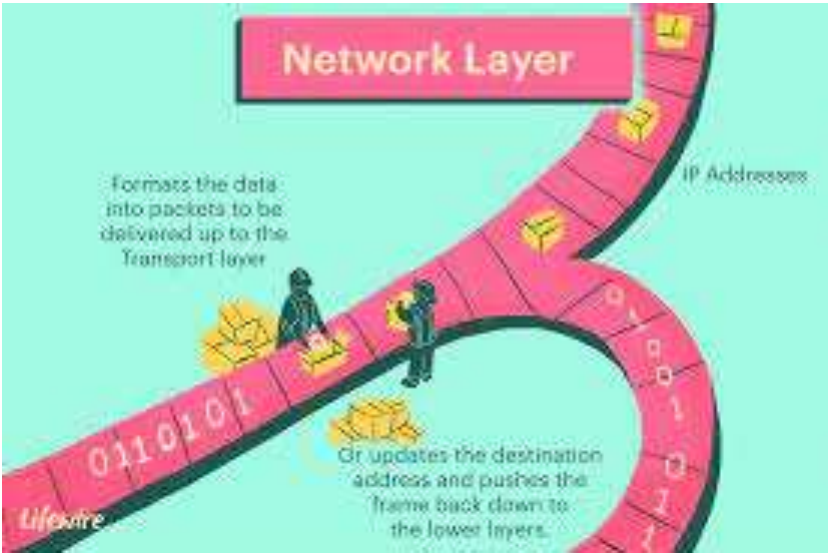
Selain fungsi-fungsi yang telah disebutkan sebelumnya, network layer juga memiliki peran penting dalam pengelolaan alamat-alamat IP. Setiap perangkat dalam jaringan diberikan alamat IP yang unik, baik itu alamat IPv4 yang terdiri dari empat oktet angka desimal atau alamat IPv6 yang lebih panjang dan kompleks. Network layer bertanggung jawab atas pemberian, pengelolaan, dan pelacakan alamat-alamat ini sehingga paket data dapat diteruskan dengan benar ke tujuan yang dituju.

Sebagai contoh, ketika sebuah paket data dikirimkan dari sumber ke tujuan, network layer pada sumber menambahkan alamat IP sumber dan alamat IP tujuan ke dalam header paket. Kemudian, paket ini akan melewati beberapa perangkat jaringan (seperti router) saat menuju tujuan. Setiap router akan menggunakan informasi alamat IP untuk memutuskan rute terbaik untuk meneruskan paket tersebut. Network layer pada setiap router melakukan proses pengambilan keputusan routing berdasarkan tabel routing yang diperbarui secara dinamis.

Network layer juga berperan dalam mengelola layanan-layanan khusus seperti *Quality of Service* (QoS) yang memungkinkan prioritas dan alokasi sumber daya yang berbeda untuk jenis-jenis layanan yang berbeda dalam jaringan. Misalnya, layanan VoIP (*Voice over Internet Protocol*) mungkin membutuhkan prioritas lebih tinggi daripada pengiriman data biasa untuk menjaga kualitas percakapan suara yang baik.

Penting untuk diingat bahwa network layer tidak hanya terbatas pada model OSI, tetapi juga ada dalam model jaringan lain seperti TCP/IP. Network layer adalah lapisan yang esensial dalam struktur komunikasi jaringan, memungkinkan berbagai jenis perangkat dan jaringan untuk saling berkomunikasi secara efisien dan teratur.

8.2 Fungsi Network Layer



Gambar 8.2. Ilustrasi Peran Network Layer
Sumber : smkadiluhur.sch.id

Network layer memiliki beberapa fungsi utama dalam jaringan komputer: (Sukaridhoto, 2014)

1. *Routing* (Pengalihan): Fungsi utama network layer adalah menentukan rute atau jalur terbaik yang harus diambil oleh paket data dari sumber ke tujuan melalui jaringan yang berbeda. Ini melibatkan pengambilan keputusan tentang bagaimana paket harus bergerak melalui jaringan dan melalui berbagai perangkat jaringan seperti router. Protokol routing digunakan untuk memutuskan rute ini berdasarkan berbagai faktor seperti jarak, beban jaringan, kondisi jaringan, dan lainnya.

2. Pemberian Alamat *(Addressing*): Network layer memberikan alamat logis kepada setiap perangkat dalam jaringan. Dalam dunia jaringan IP, alamat IP digunakan untuk mengidentifikasi setiap perangkat yang terhubung ke jaringan. Network layer memastikan bahwa setiap paket data yang dikirimkan memiliki informasi alamat IP tujuan dan sumber di dalam header paket. Ini memungkinkan perangkat di jaringan untuk mengarahkan paket data dengan benar ke tujuan yang diinginkan.
3. Fragmentasi dan Reasemblasi Paket: Network layer dapat memecah paket data besar menjadi fragmen-fragmen yang lebih kecil saat melintasi jaringan dengan batasan ukuran paket tertentu. Ini diperlukan karena berbagai jaringan mungkin memiliki batasan ukuran paket yang berbeda. Pada tujuan, network layer akan merakit kembali fragmen-fragmen ini menjadi paket data asli. Proses ini memastikan bahwa data dapat dikirim dan diterima dengan benar tanpa masalah.
4. Pengaturan *Quality of Service* (QoS): Network layer juga memungkinkan pengaturan kualitas layanan (QoS) dalam jaringan. Dengan menggunakan mekanisme QoS, jaringan dapat memberikan prioritas yang berbeda kepada jenis layanan yang berbeda. Misalnya, layanan suara dan video mungkin diberikan prioritas lebih tinggi daripada pengiriman data biasa untuk memastikan kualitas yang baik.
5. Pengalamatan Jaringan (*Network Address Translation* - NAT): Fungsi network layer ini digunakan dalam kasus di mana beberapa perangkat dalam jaringan lokal (LAN) berbagi satu alamat IP publik untuk mengakses Internet. NAT memetakan alamat-alamat IP lokal ke alamat IP publik yang sama saat data dikirim keluar dari jaringan lokal.

6. Pengiriman Paket Data:
    a. Network layer bertanggung jawab atas pengemasan paket data dengan menambahkan informasi header, termasuk alamat tujuan dan sumber.
    b. Layer ini juga mengatasi pengiriman paket data dari sumber ke tujuan dengan memutuskan rute yang tepat dan meneruskan paket melalui perangkat jaringan yang sesuai.

Secara keseluruhan, network layer berfungsi sebagai perantara antara lapisan-lapisan yang lebih tinggi dalam model jaringan dan lapisan fisik jaringan. Fungsi-fungsi ini memungkinkan komunikasi yang efisien dan handal antara perangkat dalam jaringan yang berbeda-beda.

8.3 Hindari Ini Pada Network Layer

Gambar 8.3. Ilustrasi Peringatan
Sumber : https://www.pngdownload.id/

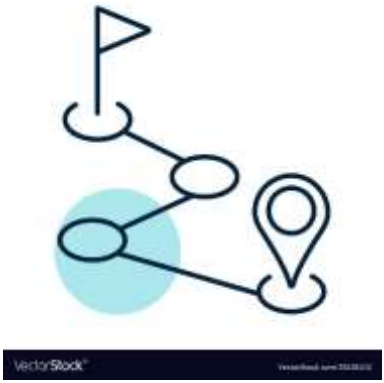
Ada beberapa hal yang sebaiknya dihindari atau tidak dilakukan pada network layer untuk menjaga kinerja, keamanan, dan stabilitas jaringan. Beberapa hal yang sebaiknya tidak dilakukan pada network layer antara lain: (Sukaridhoto, 2014)

1. Manipulasi Alamat IP dengan Sembarangan: Tidak seharusnya Anda secara sembarangan memanipulasi alamat IP pada network layer. Mengubah alamat IP tanpa alasan yang jelas atau melakukan spoofing alamat IP (mengirim paket dengan alamat IP palsu) dapat mengganggu komunikasi jaringan dan bahkan membahayakan keamanan jaringan.
2. Melakukan Perubahan Routing Tanpa Alasan yang Jelas: Mengubah konfigurasi routing atau tabel routing tanpa pemahaman yang cukup dapat menyebabkan gangguan pada aliran data dalam jaringan. Perubahan-perubahan ini harus direncanakan dan diuji dengan hati-hati untuk meminimalkan dampak negatif pada kinerja jaringan.
3. Tidak Mengamankan Jaringan: Tidak mengamankan jaringan dengan baik dapat mengakibatkan kerentanan dan risiko keamanan. Misalnya, tidak menerapkan firewall atau tidak membatasi akses yang tidak diinginkan dapat membuat jaringan rentan terhadap serangan dan akses tidak sah.
4. Tidak Memperhatikan Kebutuhan QoS: Tidak memperhatikan pengaturan *Quality of Service* (QoS) dapat mengakibatkan ketidaksetaraan dalam alokasi sumber daya jaringan. Jika tidak diberikan prioritas yang benar, layanan penting seperti suara dan video dapat mengalami masalah kualitas yang signifikan.
5. Mengabaikan Skalabilitas: Tidak merencanakan jaringan untuk pertumbuhan dan skalabilitas masa depan dapat mengakibatkan masalah ketika jaringan tumbuh dan menjadi lebih kompleks. Mengabaikan faktor-faktor skalabilitas seperti kebutuhan bandwidth, jumlah perangkat, dan volume lalu lintas dapat menyebabkan kinerja jaringan yang buruk.

6. Tidak Melakukan Monitoring dan Pemeliharaan Rutin: Tidak melakukan monitoring dan pemeliharaan rutin pada perangkat jaringan dan pengaturan routing dapat menyebabkan masalah tidak terdeteksi yang dapat mempengaruhi kinerja jaringan. Penting untuk memonitor lalu lintas jaringan, mengidentifikasi masalah, dan mengambil tindakan perbaikan jika diperlukan.
7. Mengabaikan Standar dan Protokol: Mengabaikan standar dan protokol yang berlaku dalam network layer dapat mengakibatkan inkompatibilitas dengan perangkat atau jaringan lain. Penting untuk memastikan bahwa perangkat dan konfigurasi mengikuti standar yang diakui untuk memastikan interoperabilitas yang baik.

Penting untuk memiliki pemahaman yang kuat tentang prinsip-prinsip jaringan dan operasi network layer serta menerapkan praktik terbaik untuk menjaga kinerja dan keamanan jaringan.

8.4 Routing



Gambar 8.4. Ilustrasi IoT
Sumber : www.vectorstock.com

Routing adalah proses pengiriman paket data dari sumber ke tujuan melalui jaringan yang terdiri dari berbagai perangkat jaringan seperti router. Tujuan utama routing adalah untuk menentukan rute terbaik yang harus diambil oleh paket data sehingga dapat sampai ke tujuan dengan efisien dan cepat. Proses routing melibatkan pengambilan keputusan tentang bagaimana paket data harus bergerak melalui jaringan dengan mempertimbangkan faktor-faktor seperti jarak, kondisi jaringan, beban lalu lintas, dan lainnya. (Sukaridhoto, 2014)

Contoh Sederhana Routing:

Misalkan ada dua perangkat komputer, A dan B, yang ingin saling berkomunikasi melalui jaringan. Mereka terhubung ke jaringan yang sama dan terhubung ke router A dan router B masing-masing.

1. Komputer A ingin mengirimkan paket data ke komputer B.
2. Ketika paket data diterima oleh router A, router ini akan melihat alamat tujuan paket (alamat IP B).
3. Router A akan melihat tabel routing yang telah dikonfigurasi sebelumnya. Dalam tabel routing ini, router A akan menemukan bahwa paket data harus diteruskan ke router B karena alamat tujuan adalah alamat di luar jaringan lokal.
4. Router A mengirimkan paket data ke router B berdasarkan keputusan routing yang diambil dari tabel routing.
5. Router B menerima paket data dan meneruskannya ke komputer B.

Dalam contoh ini, router A adalah node yang bertanggung jawab untuk melakukan routing. Router A mengambil keputusan routing berdasarkan tabel routing yang telah dikonfigurasi sebelumnya, yang berisi informasi tentang rute yang harus diambil untuk mencapai berbagai alamat tujuan.

Penting untuk diingat bahwa dalam jaringan yang lebih kompleks, ada banyak router dan perangkat jaringan lainnya yang terlibat dalam proses routing. Setiap router di jaringan akan bekerja sama untuk menentukan rute terbaik bagi paket data sehingga dapat mencapai tujuan dengan efisien dan tanpa masalah.

8.5 Addressing

Gambar 8.5. Ilustrasi Addressing
Sumber : www.pngwing.com

Addressing dalam konteks jaringan mengacu pada penggunaan alamat untuk mengidentifikasi dan membedakan setiap perangkat atau entitas dalam jaringan. Alamat ini digunakan untuk merujuk pada tujuan atau sumber informasi, memastikan bahwa data dikirimkan ke tempat yang tepat dalam jaringan. Addressing sangat penting dalam komunikasi jaringan, karena memungkinkan perangkat untuk mengenali dan berinteraksi satu sama lain. (Miller, 1984)

Contoh Addressing dalam Jaringan:

Dalam jaringan komputer, alamat IP (*Internet Protocol*) adalah salah satu bentuk addressing yang paling umum digunakan. Alamat IP adalah angka atau rangkaian angka yang unik yang diberikan kepada setiap perangkat yang terhubung ke jaringan. Ada dua jenis alamat IP utama yang digunakan:

1. IPv4 Address: Ini adalah alamat IP yang paling umum digunakan saat ini. Alamat IPv4 terdiri dari empat oktet angka desimal yang dipisahkan oleh titik. Misalnya, 192.168.1.1 adalah contoh alamat IPv4.
2. IPv6 Address: Sebagai respons atas semakin berkurangnya alamat IPv4 yang tersedia, IPv6 diperkenalkan. Alamat IPv6 jauh lebih panjang dan kompleks, terdiri dari delapan blok heksadesimal yang dipisahkan oleh titik dua-kolon. Contohnya adalah 2001:0db8:85a3:0000:0000:8a2e:0370:7334.

Pertimbangan Penting dalam Addressing:

1. Unik: Setiap alamat dalam jaringan harus unik, sehingga tidak ada konflik atau kebingungan dalam mengidentifikasi perangkat.
2. Hierarki: Alamat IP biasanya diatur dalam struktur hierarkis yang mencerminkan jaringan besar hingga sub-jaringan lebih kecil dan perangkat tunggal.
3. Subnetting: Dalam jaringan besar, konsep subnetting digunakan untuk membagi alamat IP menjadi sub-jaringan yang lebih kecil, memungkinkan penggunaan yang lebih efisien.
4. Penugasan Dinamis dan Statis: Alamat IP dapat diberikan secara statis (ditetapkan manual) atau secara dinamis (oleh server DHCP) kepada perangkat dalam jaringan.
5. Pemetaan DNS: Alamat IP sering kali dikaitkan dengan nama domain melalui layanan DNS (*Domain Name System*),

yang memungkinkan penggunaan alamat yang lebih mudah diingat.

Dalam konteks jaringan, addressing memainkan peran kunci dalam mengarahkan data ke tujuan yang tepat. Ini memungkinkan komunikasi yang efisien dan handal antara perangkat dalam jaringan yang luas dan beragam.

8.6 Fragmentasi dan Reasemblasi Paket

Gambar 8.6. Ilustrasi Fragmentasi
Sumber : https://www.vecteezy.com/

Fragmentasi dan reasemblasi paket adalah proses yang terjadi pada lapisan jaringan (*network layer*) dalam komunikasi data melalui jaringan komputer. Ini terjadi ketika paket data yang dikirimkan melewati jaringan dengan batasan ukuran paket yang berbeda-beda. Karena beberapa jaringan memiliki batasan ukuran maksimal paket yang lebih kecil daripada ukuran paket data asli, paket tersebut harus dipecah (difragmentasi) menjadi fragmen-fragmen yang lebih kecil sebelum dikirim. Di sisi tujuan, fragmen-

fragmen ini akan dirakit kembali menjadi paket data asli (reasemblasi) sebelum diproses lebih lanjut. (Miller, 1984)
Contoh Fragmentasi dan Reasemblasi Paket:

Misalkan Anda ingin mengirimkan sebuah file berukuran 6000 byte melalui jaringan. Namun, jaringan yang Anda gunakan memiliki batasan ukuran maksimal paket sebesar 1500 byte. Dalam hal ini, file tersebut harus dipecah menjadi fragmen-fragmen yang lebih kecil sebelum dikirim.

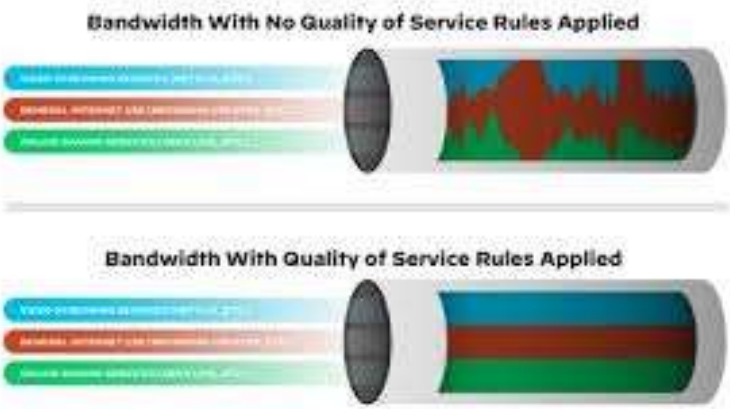
1. **Fragmentasi:**
    a. File 6000 byte dipecah menjadi fragmen-fragmen yang lebih kecil.
    b. Setiap fragmen memiliki header yang berisi informasi yang diperlukan, seperti alamat tujuan, alamat sumber, nomor urut fragmen, dan lain-lain.
    c. Fragmen-fragmen ini dikirimkan satu per satu melalui jaringan.

2. **Reasemblasi:**
    a. Di sisi tujuan, fragmen-fragmen yang diterima akan diidentifikasi melalui informasi header yang ada.
    b. Fragmen-fragmen ini akan dirakit kembali sesuai dengan urutan nomor fragmen yang benar.
    c. Setelah semua fragmen berhasil dirakit, file asli yang utuh dapat diperoleh kembali.

Dalam contoh ini, fragmentasi dan reasemblasi paket memastikan bahwa file yang besar dapat dikirimkan melalui jaringan yang memiliki batasan ukuran paket tertentu. Proses fragmentasi memungkinkan file asli untuk dipecah menjadi bagian-bagian yang lebih kecil yang sesuai dengan ukuran paket jaringan yang ada. Di sisi tujuan, reasemblasi memastikan bahwa bagian-bagian ini dirakit kembali dengan benar sehingga data dapat diambil dengan lengkap.

Penting untuk diingat bahwa fragmentasi dan reasemblasi paket berfungsi secara transparan bagi pengguna akhir. Proses ini diatur oleh protokol di lapisan jaringan dan tidak memerlukan interaksi atau campur tangan langsung dari pengguna.

8.7 Meningkatkan Qos



Gambar 8.7. Ilustrasi QoS
Sumber : www.paloaltonetworks.com

Meningkatkan *Quality of Service* (QoS) dalam jaringan komputer adalah suatu upaya untuk memberikan prioritas dan pengaturan sumber daya yang lebih baik kepada jenis layanan yang lebih penting atau kritis. Hal ini bertujuan untuk mengoptimalkan kinerja jaringan, mengurangi latensi, dan memastikan pengiriman data yang lebih handal untuk aplikasi dan layanan yang memerlukan kualitas yang lebih tinggi. Berikut adalah beberapa cara untuk meningkatkan QoS dalam jaringan: (Miller, 1984)

1. Pengaturan Prioritas: Identifikasi layanan yang paling penting dalam jaringan Anda, seperti layanan suara (VoIP) atau video streaming. Kemudian, atur pengaturan prioritas

untuk memberikan bandwitch dan penggunaan sumber daya yang lebih tinggi kepada layanan-layanan tersebut. Ini dapat dilakukan melalui konfigurasi pengaturan QoS di router dan perangkat jaringan.

2. Pembatasan Lalu Lintas (*Traffic Shaping*): Gunakan teknik pembatasan lalu lintas untuk mengendalikan dan mengatur aliran data dalam jaringan. Dengan cara ini, Anda dapat mencegah lalu lintas yang tidak kritis mengambil terlalu banyak sumber daya dan memberikan prioritas kepada layanan yang lebih penting.
3. Penjadwalan Paket (*Packet Scheduling*): Menggunakan algoritma penjadwalan paket yang tepat dapat membantu dalam mengatur pengiriman paket dengan lebih efisien dan meminimalkan latensi. Beberapa algoritma penjadwalan paket yang umum digunakan termasuk *Weighted Fair Queuing* (WFQ) dan *Deficit Round Robin* (DRR).
4. Pengaturan Batas (*Rate Limiting*): Batasi laju lalu lintas bagi layanan-layanan yang kurang kritis atau memiliki kebutuhan bandwidth yang lebih rendah. Dengan cara ini, Anda dapat menghindari satu layanan yang menguasai seluruh bandwidth dan mengganggu layanan lain.
5. Segmentasi Jaringan (*Network Segmentation*): Membagi jaringan menjadi segmen-segmen atau VLANs (*Virtual Local Area Networks*) dapat membantu dalam mengisolasi lalu lintas dan memberikan prioritas yang lebih baik pada setiap segmen sesuai kebutuhannya.
6. Penggunaan Protokol yang Sesuai: Pilih protokol yang tepat untuk aplikasi dan layanan yang digunakan. Beberapa protokol mungkin memiliki dukungan bawaan untuk QoS dan prioritas.
7. Monitoring dan Analisis: Lakukan pemantauan lalu lintas jaringan secara teratur untuk mengidentifikasi perubahan dalam lalu lintas dan masalah kinerja. Dengan memahami

pola lalu lintas, Anda dapat mengambil tindakan untuk meningkatkan QoS jika diperlukan.

8. **Investasi dalam Sumber Daya: ** Jika memungkinkan, meningkatkan kapasitas bandwidth dan sumber daya jaringan secara keseluruhan dapat membantu menjaga kualitas layanan yang baik.
9. Konfigurasi Prioritas Aplikasi: Beberapa perangkat dan aplikasi memiliki opsi untuk mengatur prioritas lalu lintas. Memastikan bahwa prioritas ini diatur dengan benar dapat membantu meningkatkan QoS.
10. Pembaruan dan Optimalisasi Perangkat: Pastikan perangkat jaringan, router, dan switch diperbarui dengan versi firmware terbaru, dan lakukan optimalisasi untuk meningkatkan kinerja mereka.

Penting untuk memahami kebutuhan spesifik jaringan Anda dan jenis layanan yang digunakan untuk merancang strategi QoS yang tepat. QoS yang baik dapat membantu memastikan pengalaman yang lebih baik bagi pengguna jaringan dan mencegah masalah kinerja yang tidak diinginkan.

8.8 Network Address Translation

Gambar 8.8. Ilustrasi NAT
Sumber : https://www.vecteezy.com/

Network Address Translation (NAT) adalah proses yang digunakan dalam jaringan komputer untuk mengubah alamat IP dalam header paket data saat melewati perangkat jaringan tertentu, seperti router. Tujuan utama NAT adalah untuk mengizinkan beberapa perangkat dalam jaringan lokal (LAN) untuk berbagi satu alamat IP publik yang unik untuk mengakses Internet. Dengan kata lain, NAT memungkinkan penggabungan alamat IP lokal menjadi satu alamat IP publik saat berkomunikasi di luar jaringan lokal. (Miller, 1984)

Contoh NAT:

Misalkan Anda memiliki jaringan rumah dengan beberapa perangkat yang terhubung ke router melalui jaringan lokal. Anda memiliki satu alamat IP publik yang diberikan oleh penyedia layanan Internet (ISP). Ketika perangkat-perangkat ini ingin mengakses Internet, mereka harus berbagi alamat IP publik yang sama.

1. Sebelum NAT:
    a. Perangkat A (192.168.1.10) ingin mengakses situs web.
    b. Perangkat B (192.168.1.20) ingin mengirim email.
    c. Keduanya berada dalam jaringan lokal dengan alamat IP yang dimulai dengan 192.168.1.x.

2. Setelah NAT:
    a. Ketika permintaan datang dari Perangkat A, router NAT akan mengubah alamat sumber dari paket menjadi alamat IP publik (misalnya, 203.0.113.1) sebelum dikirim ke tujuan di Internet.
    b. Begitu juga, saat Perangkat B mengirim email, router NAT akan mengubah alamat sumber paketnya menjadi alamat IP publik yang sama.
    c. Ketika respons datang dari server web atau server email di Internet, router NAT akan menggunakan tabel

translatif untuk mengarahkan respons tersebut kembali ke perangkat yang sesuai dalam jaringan lokal (misalnya, Perangkat A atau B).

Dengan menggunakan NAT, alamat IP lokal dalam jaringan lokal Anda menjadi "tersembunyi" di balik alamat IP publik tunggal. Ini membantu mengamankan jaringan lokal dan memperpanjang penggunaan alamat IP yang terbatas.

Selain dari penggunaan NAT untuk menghubungkan jaringan lokal ke Internet, NAT juga dapat digunakan dalam skenario jaringan lain, seperti dalam konfigurasi jaringan perusahaan yang kompleks atau dalam penggunaan layanan cloud.

8.9 Pengiriman Paket Data

Gambar 8.9. Ilustrasi Paked Data
Sumber : https://www.pngwing.com/

Pengiriman paket data adalah proses mentransfer informasi atau data dalam bentuk paket-paket kecil melalui jaringan komunikasi, seperti jaringan komputer atau Internet. Setiap paket data berisi sejumlah bit informasi, termasuk data pengirim, data tujuan, dan data aktual yang ingin dikirim. Proses pengiriman paket data melibatkan berbagai lapisan jaringan,

termasuk lapisan fisik (*physical layer*), lapisan data link (data link layer), dan lapisan jaringan (*network layer*) dalam model referensi OSI. (Miller, 1984)

Contoh Pengiriman Paket Data:

Misalkan Anda ingin mengirimkan pesan teks dari komputer A ke komputer B melalui jaringan lokal. Proses pengiriman paket data dapat dipecah menjadi langkah-langkah berikut:

1. Pembagian Data: Pesan teks yang ingin Anda kirim dipecah menjadi paket-paket data yang lebih kecil. Misalnya, "Halo, bagaimana kabarmu?" dapat dipecah menjadi beberapa paket data, seperti "Hal", "o, b", "aga", "ima", "na k", "aba", "rmu", dan "?".
2. Penambahan Header: Setiap paket data diberi header, yang berisi informasi tentang alamat pengirim, alamat tujuan, nomor urut paket, dan informasi pengendalian lainnya.
3. Transmisi melalui Jaringan: Setiap paket data dikirimkan melalui jaringan. Ini melibatkan konversi data menjadi sinyal listrik atau cahaya yang sesuai dengan medium transmisi jaringan, seperti kabel atau gelombang radio.
4. Routing dan Pengalihan: Paket-paket data melewati perangkat jaringan, seperti router, yang memutuskan rute terbaik untuk pengiriman paket-paket ini berdasarkan tabel routing.
5. Reasemblasi di Tujuan: Di sisi tujuan (komputer B), paket-paket data diterima dan dirakit kembali sesuai dengan nomor urutnya untuk membangun kembali pesan asli "Halo, bagaimana kabarmu?".
6. Pengiriman Balik (Jika Diperlukan): Jika ada respons dari komputer B, proses yang serupa terjadi di arah sebaliknya, yaitu pengiriman paket-paket data dari komputer B ke komputer A.

Penting untuk diingat bahwa proses pengiriman paket data ini terjadi dalam waktu sangat cepat dan berulang-ulang sampai seluruh pesan berhasil dikirim dan diterima. Pengiriman paket data menjadi dasar dari komunikasi dalam jaringan, termasuk komunikasi data, suara, video, dan lainnya.

8.10 Protokol Network Layer

Gambar 8.10. Ilustrasi Protokol
Sumber : www.pngwing.com

Protokol network layer adalah protokol yang beroperasi pada lapisan jaringan (*network layer*) dalam model referensi OSI. Protokol ini bertanggung jawab atas pengiriman paket data melalui jaringan, termasuk pengaturan rute, fragmentasi dan reasemblasi paket, serta pengiriman paket dari sumber ke tujuan. Beberapa protokol *network layer* yang penting termasuk: (Miller, 1984)

1. Internet Protocol (IP): IP adalah protokol paling mendasar dalam jaringan dan digunakan untuk mengirimkan paket data antar perangkat di jaringan. Ada dua versi utama: IPv4 (Internet Protocol versi 4) dan IPv6 (Internet Protocol versi 6).
2. *Internet Control Message Protocol* (ICMP): ICMP digunakan untuk mengirim pesan kesalahan dan informasi terkait jaringan, seperti pesan "ping" untuk menguji keterhubungan host.

3. *Internet Group Management Protocol* (IGMP): Protokol ini digunakan untuk mengelola dan mengontrol komunikasi multicast dalam jaringan IP, yang memungkinkan pengiriman data ke beberapa tujuan sekaligus.
4. *Routing Information Protocol* (RIP): RIP adalah protokol routing interior yang digunakan untuk mengatur tabel routing dalam jaringan kecil hingga menengah.
5. *Open Shortest Path First* (OSPF): OSPF adalah protokol routing interior yang lebih canggih dan skala lebih besar daripada RIP, biasanya digunakan dalam jaringan besar dan kompleks.
6. *Border Gateway Protocol* (BGP): BGP adalah protokol routing eksterior yang digunakan untuk mengatur routing antara berbagai sistem otonom (AS) dalam Internet.
7. *Interior Gateway Routing Protocol* (IGRP) dan *Enhanced Interior Gateway Routing Protocol* (EIGRP): Protokol-protokol ini juga digunakan untuk routing interior dan dikembangkan oleh Cisco untuk digunakan dalam jaringan Cisco.
8. *Packet Internet Groper* (PING): PING adalah utilitas yang menggunakan protokol ICMP untuk menguji koneksi jaringan dan mengukur latensi.
9. *Address Resolution Protocol* (ARP): ARP digunakan untuk mengaitkan alamat IP dengan alamat fisik (MAC address) dalam jaringan lokal.
10. *Reverse Address Resolution Protocol* (RARP): RARP digunakan untuk mengaitkan alamat fisik (MAC address) dengan alamat IP dalam jaringan lokal.
11. *Internet Group Management Protocol* (IGMP): IGMP digunakan untuk mengelola dan mengontrol komunikasi multicast dalam jaringan IP.

12. *Multicast Listener Discovery* (MLD): MLD adalah versi IPv6 dari protokol IGMP dan digunakan untuk mengelola dan mengontrol komunikasi multicast dalam jaringan IPv6.
13. *Internet Protocol version* 6 (IPv6): IPv6 adalah versi terbaru dari protokol Internet Protocol dan diperkenalkan sebagai respons atas semakin berkurangnya alamat IPv4 yang tersedia. IPv6 menggunakan format alamat yang lebih panjang dan kompleks untuk mengatasi keterbatasan alamat IPv4.
14. *Internet Group Management Protocol version* 3 (IGMPv3): IGMPv3 adalah versi lebih baru dari IGMP yang mendukung pengaturan yang lebih baik dalam komunikasi multicast dalam jaringan IP.
15. P*rotocol Independent Multicast* (PIM): PIM adalah sekumpulan protokol yang digunakan untuk mengatur komunikasi multicast di jaringan IP. Ini mencakup PIM Sparse Mode (PIM-SM) dan PIM Dense Mode (PIM-DM), serta varian lainnya.
16. *Hot Standby Router Protocol* (HSRP): HSRP adalah protokol yang digunakan untuk mengatur redundansi router dalam jaringan. Ini memungkinkan beberapa router berbagi satu alamat IP virtual untuk memberikan failover yang lebih baik.
17. V*irtual Router Redundancy Protocol* (VRRP): VRRP adalah protokol serupa dengan HSRP dan digunakan untuk menciptakan redundansi router dengan menggunakan alamat IP virtual.
18. *Internet Protocol Security* (IPsec): IPsec adalah rangkaian protokol yang digunakan untuk mengamankan komunikasi jaringan dengan mengenkripsi dan mengotentikasi lalu lintas data.

19. *Internet Control Message Protocol for* IPv6 (ICMPv6): Ini adalah versi IPv6 dari protokol ICMP dan digunakan untuk mengirim pesan kesalahan dan informasi terkait dalam jaringan IPv6.
20. *Multiprotocol Label Switching* (MPLS): MPLS adalah teknologi pengalihan paket yang digunakan untuk meningkatkan efisiensi dan kecepatan pengiriman paket data dalam jaringan.
21. *Shortest Path Bridging* (SPB): SPB adalah protokol pengalihan jaringan yang memungkinkan penyebaran jaringan skala besar dengan menggabungkan beberapa jaringan lokal ke dalam satu jaringan virtual.
22. *Generic Routing Encapsulation* (GRE): GRE adalah protokol tuneling yang digunakan untuk mengirimkan lalu lintas jaringan yang dienkapsulasi dalam lalu lintas jaringan lain.

Setiap protokol ini memiliki peran khusus dalam pengelolaan dan pengaturan komunikasi dalam jaringan, membantu memastikan pengiriman data yang efisien dan handal.

DAFTAR PUSTAKA

Miller, R.L. 1984. 'InfoSec Reading Room The OSI Model : An Overview , A ho ll r igh ts'.

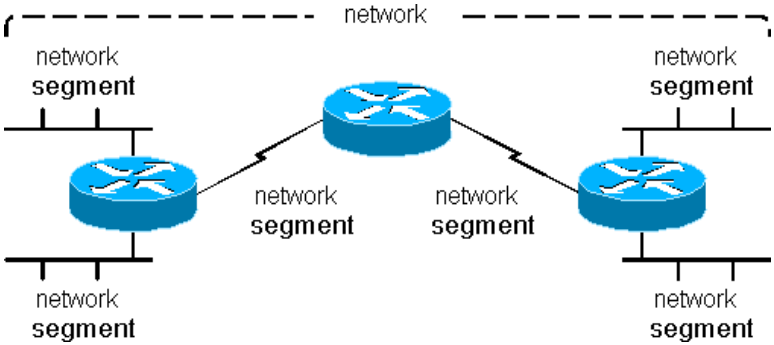
Sukaridhoto, S. 2014. 'Buku Jaringan Komputer I'. Available at: http://dhoto.lecturer.pens.ac.id/publications/book/2014/Dhoto-JaringanKomputer1.pdf.

BAB 9
RESOLUSI PENGALAMATAN

Oleh Abdurohim

9.1 Memahami Resolusi Alamat

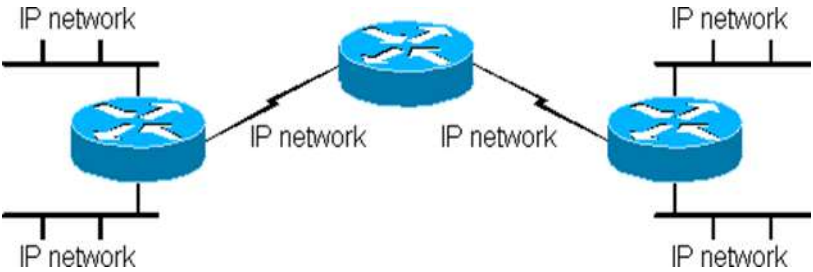
Resolusi alamat (Alani *et al.,* 2023) merupakan aktivitas yang dilakukan oleh komputer atas permintaan pengguna untuk memperoleh alamat fisik dari sebuah mesin atau alamat virtual yang telah dilakukan pengiriman oleh node komputer atau perangkat yang dipergunakan untuk kegiatan memperoleh sumber atau data, pengumuman yang diinginkan oleh pengirim untuk tujuan tertentu. Resolusi alamat ini sangat diperlukan oleh pihak pengelola komputer pengguna untuk mencari alamat suatu instansi atau bisnis, sehingga bisa tersambung ke alamat yang telah didaftarkan dari pengguna ke pengelola web, bisa mengakses sesuai dengan keinginannya seperti data yang telah disediakan untuk disebarluaskan kepada pengguna sesuai yang diinginkan (Abdurohim, 2022).



Gambar 9.1. Hubungan Fisik
Sumber: (Vaya, 2002)

Dalam hubungan fisik pada internet membutuhkan adanya kesesuaian antara satu dengan lainnya sebagaimana terurai pada gambar 9.1. Resolusi alamat ini dipergunakan oleh berbagai individu maupun group untuk menuju kearah alamat yang berbeda dalam satu jaringan komputer, bagi komputer dalam mencari pengalamatan, membutuhkan penyimpanan fisik atau alamat memori sehingga bila ditemukan alamat yang dikehendaki, maka mengirimkan data sebagaimana yang diinginkan oleh pengguna. Banyak yang meminta data ataupun pengiriman surat tidak tersampaikan disebabkan dalam mengetik pengalamatan tidak lengkap salah menulis ataupun alamat yang dituju, alamat sudah tidak aktif dipergunakan untuk kegiatan menyampaikan informasi kepada pelanggannya (Aski *et al.,* 2023).

Pengalamatan oleh pemilik, aksesnya bisa langsung dan berlangsung secara cepat tanpa ada kesalahan, pada jaringan TCP/IP maka pengguna internet yang berada di internal atau eksternal sudah bisa menikmati apa yang dibutuhkan seperti data yang dikelola oleh jaringan komputer untuk dibagikan ke seluruh pengguna yang membutuhkan, sehingga mereka merasa terbantukan maksud dan tujuannya (Ushakov *et al*., 2022).



Gambar 9.2. Keselarasan hubungan IP dan Host
Sumber: (Vaya, 2002)

Proses pengalamatan tidak hanya sebatas ketika mengetikan alamat maka data atau kedudukan secara virtual

ditemukan, prosesnya dengan terlebih dahulu untuk mendapatkan alamat IP dan MAC (Bandhaso & Sutanto, 2022) dari node yang diberi nama. Proses panjangnya adalah bahwa komputer yang dipergunakan untuk menerjemahkan dari bahasa manusia menjadi bahasa komputer/mesin. Kadangkala ada pencari alamat dari yang dituju menolak atas permintaan dari pengguna, hal ini bisa terjadi jika terjadi komunikasi yang dibutuhkan tidak stabil, ataupun dalam penulisan alamatnya tidak jelas atau kurang dalam pengetikan alamatnya, maka tidak bisa dilanjutkan .

Hal ini bisa terjadi karena bahasa komputer/mesin (Hermiati *et al.,* 2021) tidak bisa dinegosiasikan seperti bahasa manusia yang bisa dilakukan dengan basa basi, bahasa yang diinginkan oleh komputer/jaringan haruslah jelas dan tidak boleh kurang satu huruf maupun salah, sebab secara otomatis komputer jaringan yang menerima perintah untuk mengakses akan menolak permintaan.

Dalam penyusunan pengalamatan harus sesuai dengan protokol yang telah disusun oleh lembaga dunia, dan semua pembuat website haruslah mengikuti aturan yang telah disepakati secara internasional (Conrad *et al*., 2023). Beberapa pengaturan protokol resolusi alamat menyusun langkah-langkahnya, sebagai berikut:

1. Protokol resolusi alamat merupakan sebuah protokol pada TCP/IP protocol suite memiliki tanggung jawab pada resolusi alamat IP pada alamat MAC Address (*Media Access Control*).
2. Akses yang dilakukan oleh protokol TCP/IP melalui alamat IP, maka IP yang dimiliki oleh penampung.
3. Bila alamat yang dituju ternyata berada di luar jaringan lokal maka ARP maka komputer pengguna akan berupaya untuk memperoleh MAC address dan antarmuka router lokal, maka akan terus mencari lokasi komputer yang dituju berada.

Penggunaan *Address Resolution Protocol* ini dipergunakan dalam kegiatan pencarian alamat pengelola web (Shah et al., 2022), setiap pengiriman alamat kepada alamat pengelola terlebih dahulu. Misalnya komputer A (Node A) menanyakan kekomputer D (Node D), maka proses yang dilakukan adalah node A akan menanyakan terlebih dahulu alamat tersebut melalui ARP, dengan melakukan broadcast terlebih dahulu ke masing-masing node yang telah diberikan kode terlebih dahulu, sehingga bila ada node yang sesuai dengan pertanyaan yang telah dilontarkan tersebut, maka node yang sesuai dengan pertanyaan akan menyahut pertanyaan tersebut, sehingga bila sesuai dengan apa yang ditanyakan maka terjadi yang namanya hubungan komputer untuk memperoleh data yang diperlukan.

9.2 Pengembangan model TCP/IP

TCP/IP (*Transmission Control Protocol/Internet Protocol*) (Morawski & Ignacio, 2021) merupakan suatu model mencari pengalamatan yang dikembangkan oleh Department of Defence (DoD) Amerika Serikat untuk dipergunakan keperluan pengiriman paket kepada alamat yang dituju meskipun kondisinya tidak mendukung dari satu titik ke titik lainnya. Adanya TCP/IP tersebut memungkinkan masing-masing alamat bisa berhubungan satu sama lainnya melalui media LAN maupun WAN.

Untuk mendukung TCP P (Ha *et al*., 2023) bekerja dengan baik, sehingga operasi pengiriman alamat, data berjalan sesuai dengan yang dikehendaki oleh semua pengguna maupun penyedia, maka dilakukan pengaturan lapisan aplikasi yang terdiri dari:

1. Lapisan aplikasi pada tingkat 4

   Lapisan aplikasi pada tingkat 4 merupakan lapisan yang paling atas pada arsitektur protokol TCP/IP yang terdiri dari FTP (*File Transfer Protocol*), SMTP (*Simple Mail Transfer Protocol)* serta HTTP (*Hypertext Transfer Protocol*)

2. Lapisan aplikasi pada tingkat 3

   Lapisan ini memiliki tugas untuk mengatur komunikasi antara aplikasi, melalui pengaturan semua informasi yang masuk serta pemeriksaan kesalahan (error). Data yang masuk disalurkan pada lapisan internet melalui sebuah header. Dimana header memiliki alamat yang akan dituju, sumber serta checksum. Checksum yang masuk akan dilakukan pemeriksaan oleh mesin penerima untuk memastikan apakah paket tersebut tidak sesuai dengan rute.
3. Lapisan aplikasi pada tingkat 2

   Lapisan ini dipergunakan untuk saling mengirimkan informasi dengan network layer bila mengikuti model OSI, kegiatan pengiriman melalui pengalamatan logikal, serta untuk lapisan ini guna menentukan best path serta packet switching.
4. Lapisan aplikasi pada tingkat 1

   Melalui lapisan aplikasi ini untuk mengirimkan data ke device lain yang tercatat pada komputer, serta untuk dipergunakan untuk konversi IP Packet dengan demikian bisa dilakukan pengiriman melalui physical link.

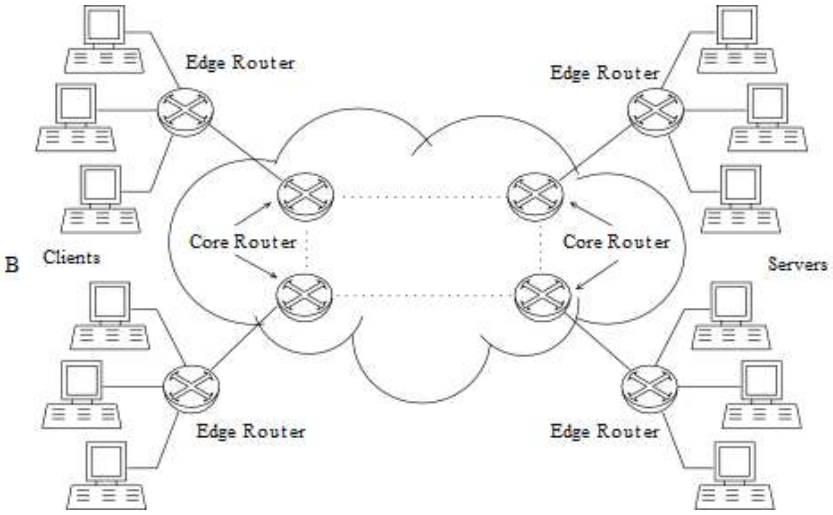
   Sedangkan untuk Internet Protocol merupakan protokol pada lapisan jaringan dalam rangka untuk memelihara sebuah hubungan, serta dalam pengiriman ini tidak menjamin akan diterima semuanya. Internet protocol dibangun untuk bisa melewati berbagai komunikasi yang beraneka ragam seperti kecepatan yang dimiliki ada yang cepat, sedang serta lambat. Hal ini sangat berpengaruh terhadap pengiriman data maupun pesan yang terkirim. Bila komunikasi nya stabil dan memiliki kecepatan yang tinggi maka dengan cepat internal protokol ini mengirimkan data/pesan juga cepat ke tujuan yang dimaksud, namun bila menghadapi komunikasi yang lambat disebabkan jaringannya terganggu karena hujan, atau ada halangan, maka proses pengirimannya juga menghadapi kendala yang harus bisa dipecahkan. Banyak pihak yang melakukan berbagai solusi

yang ditawarkan kepada pengelola komunikasi untuk melakukan penyesuaian-penyesuaian yang diperlukan. Sebab tidak bisa hanya mengandalkan jaringan komunikasi yang dipercayakan pada satu vendor, harus banyak dipersiapkan untuk mengatasi masalah komunikasi yang berlangsung .

Sedangkan untuk TCP merupakan komponen dalam aktivitas pengiriman data untuk keperluan menambang data (Morawski & Ignacio, 2021), merupakan protokol layer transport yang mengarah pada koneksi, kemampuan untuk memberikan jaminan yang stabil dan juga melalui orientasi yang terus menerus stabil dilakukan. Dalam TCP dikenal dengan Segment dipergunakan untuk membuat koneksi, pengiriman data, pengiriman ack, pemberitahuan ukuran window dan penutupan koneksi. Segmen tersebut akan dikirim melalui diagram IP.

9.3 Peranan IP dalam mensukseskan proses pengalamatan

Internet yang dibuat oleh pengembang meliputi jaringan fisik yang disambungkan dengan infrastruktur internetworking yang dikenal dalam istilah teknologi informasi adalah router. Data yang telah dikemas oleh pemilik akan dikirimkan ke pengguna yang meminta tentunya melewati berbagai jaringan yang berlainan dan pada akhirnya akan mencapai host yang dituju, secara teknologi proses ini hanya dalam beberapa detik, namun bila kita membaca secara teori seolah-olah melewati berbagai hubungan yang saling menjaga dan saling menghadang namun dengan kemampuan ilmu serta teori yang mampu memberikan kemudahan antara satu hubungan dengan lainnya. Bila telah sampai ke host tujuan, maka host dan router akan diterima jika terlebih dahulu dikenali melalui alamat logis yang telah ada.



Gambar 9.3. Jaringan pada Internet
Sumber: (Pióro & Dipankar, 2004)

Alamat logis dikenal dengan dengan istilah IP pada kegiatan yang dinamakan TCP/IP dengan panjang 32 bit (Shah *et al.,* 2022). Sedang Kan dikenal juga dalam jaringan selain alamat logis juga harus mempelajari alamat fisik atau dikenal dengan sebutan alamat lokal atau dikenal dengan sebutan jaringan lokal. Kegiatan pengiriman data akan menggunakan alamat logik ke alamat fisik. Karena itu perlu terlebih dahulu mematikannya, seperti:

1. Pemetaan statistic

   Pemetaan ini tentunya harus dibuatkan tabel yang bisa menghubungkan antara alamat logis dan alamat fisik. Dan kegunaan tabel untuk melihat apa yang tercantum dalam jaringan maka akan diarahkan pada tabel yang diperlukan.
2. Pemetaan Dinamis

   Pada pemetaan Dinamis maka setiap pengiriman data dari jaringan komputer lain sebagai alamat logis mesin lain. Untuk bisa memberikan fasilitas dalam pengiriman data, maka *Address*

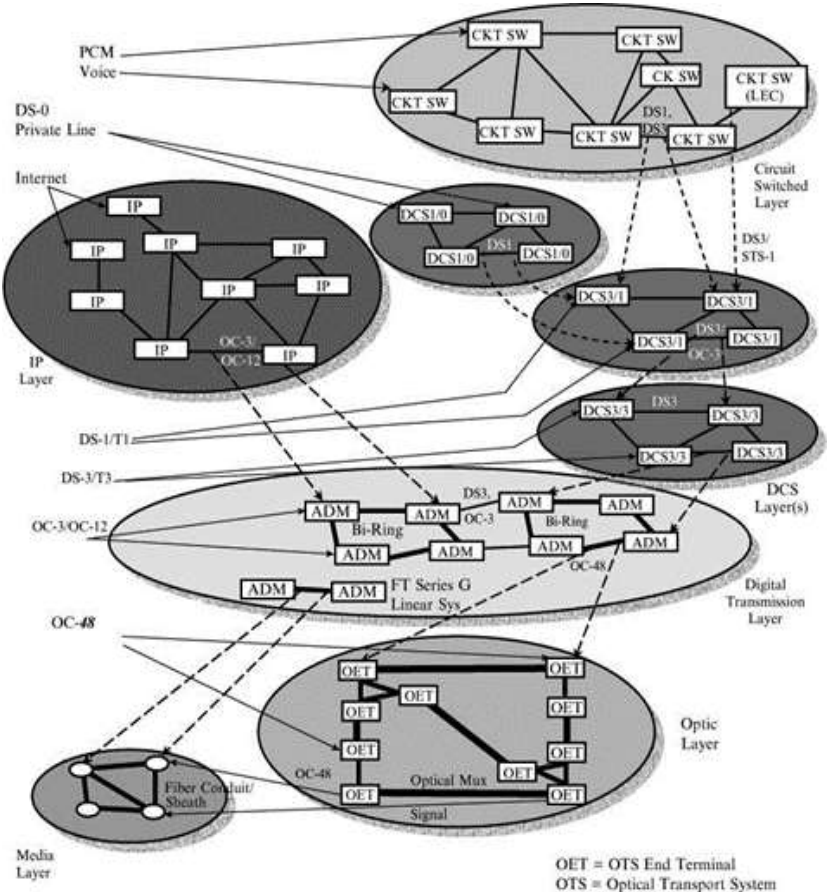
Resolution Protocol (ARP) serta *Reverse address Resolution Protocol* (ARP) telah disusun untuk mendukung kegiatan ini, dimana ARP akan memetakan alamat logis ke alamat fisik sedangkan tugas RARP lebih menitikberatkan pada pemetaan dari alamat fisik ke alamat logis (Girdler & Vassilakis, 2021).

9.4 Penamaan pada internet dan Pengalamatan

Pengalamatan sangatlah utama untuk individu maupun perusahaan yang memiliki internet, sehingga bisa dimasuki oleh pengguna, sehingga pengguna bisa melihat, mendownload data serta bisa memberikan saran dan perbaikan-perbaikan yang diperlukan oleh perusahaan maupun individual. Karena itu dalam membuat alamat haruslah benar-benar yang memiliki keamanan yang tinggi sehingga tidak bisa dimasuki oleh penyusup atau iklan yang mengganggu (Ghribi & Meddeb, 2023).

Pengalamatan harus benar-benar diperhatikan oleh pemilik website, sebab kegagalan dalam pengelolaan pengalamatan maka akan berdampak buruk pada pengembangan bisnis baik untuk perorangan maupun korporasi, karena itu untuk menyelenggarakan kegiatan melalui internet haruslah benar-benar sesuai dengan pengaturan yang telah ditetapkan, sehingga untuk hal tersebut tentunya dalam pengalamatan dan penamaan pada internet juga menyesuaikan apa yang digariskan oleh pengatur internet global (Pisarev Sky *et al*., 2022).

Penamaan untuk memudahkan pemakai menuju host yang dituju pada internet, dan ketika nama diketik oleh pemakai pada internet, maka secara langsung ditranslasikan pada alamat uniknya (*global internet address*) melalui media server yang telah disediakan oleh pengelola internet melalui name server (Yang et al., 2022). Alamat internet telah dilakukan penyusunan secara rapi mulai dari 32-bit (4-oket) terinci pada dua bagian [1, 2, 3, 37] yaitu alamat jaringan *(network address-netid*) dan alamat host (*host address-host id*) .



Gambar 9.4. Arsitektur hubungan Internet
Sumber: (Pióro & Dipankar, 2004)

DAFTAR PUSTAKA

Abdurohim. 2022. *BAB 8: Mobile Commerce* (S. S. E. , M. M. Acai, Ed.; 1st ed., Vol. 1). Media Sains Indonesia. www.penerbit.medsan.co.id

Alani, M. M., Awad, A. I., & Barka, E. 2023. ARP-PROBE: An ARP spoofing detector for Internet of Things networks using explainable deep learning. *Internet of Things*, *23*, 100861. https://doi.org/https://doi.org/10.1016/j.iot.2023.100861

Aski, V. J., Dhaka, V. S., Parashar, A., Kumar, S., & Rida, I. 2023. Internet of Things in healthcare: A survey on protocol standards, enabling technologies, WBAN architectures and open issues. *Physical Communication*, *60*, 102103. https://doi.org/https://doi.org/10.1016/j.phycom.2023.102103

Bandhaso, C. P., & Sutanto, Y. 2022. Analisis Dan Implementasi Metode Random Early Detection (Red) Pada Jaringan TCP/IP. *Respati*, *17*(2). https://doi.org/10.35842/jtir.v17i2.458

Conrad, E., Misenar, S., & Feldman, J. 2023. Chapter 5 - Domain 4: Communication and Network Security. In E. Conrad, S. Misenar, & J. Feldman (Eds.), *CISSP® Study Guide (Fourth Edition)* (pp. 225–293). Syngress. https://doi.org/https://doi.org/10.1016/B978-0-443-18734-6.00003-9

Ghribi, M., & Meddeb, A. 2023. A dual-mode MAC protocol with service differentiation for industrial IoT networks using wake-up radio. *Ad Hoc Networks*, *142*, 103111. https://doi.org/https://doi.org/10.1016/j.adhoc.2023.103111

Girdler, T., & Vassilakis, V. G. 2021. Implementing an intrusion detection and prevention system using Software-Defined Networking: Defending against ARP spoofing attacks and Blacklisted MAC Addresses. *Computers & Electrical Engineering*, *90*, 106990. https://doi.org/https://doi.org/10.1016/j.compeleceng.2021.106990

Ha, T., Masood, A., Na, W., & Cho, S. 2023. Intelligent Multi-Path TCP Congestion Control for video streaming in Internet of Deep Space Things communication. *ICT Express*. https://doi.org/https://doi.org/10.1016/j.icte.2023.02.006

Hermiati, R., Asnawati, A., & Kanedi, I. 2021. PEMBUATAN E-COMMERCE PADA RAJA KOMPUTER MENGGUNAKAN BAHASA PEMROGRAMAN PHP DAN DATABASE MYSQL. *JURNAL MEDIA INFOTAMA*, *17*(1). https://doi.org/10.37676/jmi.v17i1.1317

Morawski, M., & Ignaciuk, P. 2021. A green multipath TCP framework for industrial internet of things applications. *Computer Networks*, *187*, 107831. https://doi.org/https://doi.org/10.1016/j.comnet.2021.107831

Pióro, M., & Deepankar, M. 2004. *Routing, Flow, and Capacity Design in Communication and Computer Networks*. http://www.mkp.com

Pisarevsky, S. A., Li, Z. X., Tetley, M. G., Liu, Y., & Beardmore, J. P. 2022. An updated internet-based Global Paleomagnetic Database. *Earth-Science Reviews*, *235*, 104258. https://doi.org/https://doi.org/10.1016/j.earscirev.2022.104258

Shah, S. Q. A., Khan, F. Z., & Ahmad, M. 2022. Mitigating TCP SYN flooding based EDOS attack in cloud computing environment using binomial distribution in SDN. *Computer Communications*, *182*, 198–211. https://doi.org/https://doi.org/10.1016/j. comcom.2021.11.008

Ushakov, D., Dudukalov, E., Kozlova, E., & Shatila, K. 2022. The Internet of Things impact on smart public transportation. *Transportation Research Procedia*, *63*, 2392–2400. https://doi.org/https://doi.org/10.1016/j.trpro.2022.06.275

Vaya, L. 2002. *IP Addressing A Simplified Tutorial*. http://www1.avaya.com/enterprise/whitepapers/vlan-tutorial.pdf

Yang, W., Zhang, X., Chen, J., Miao, W., Zheng, C., Qian, X., & Geng, G. 2022. Effects of internet-based interventions on improvement of glycemic control and self-management in older adults with diabetes: Systematic review and meta-analysis. *Primary Care Diabetes*, *16*(4), 475–483. https://doi.org/https://doi.org/10.1016/j.pcd.2022.05.004

BAB 10
KONFIGURASI DASAR ROUTER

Oleh Raimon Efendi

10.1 Pendahuluan

Dalam konteks jaringan komputer, penting untuk memahami bahwa paket data yang dikirim tidak selalu dimulai dan berakhir di jaringan dengan ID yang sama. Faktanya, paket data dapat melakukan perjalanan melalui berbagai jaringan dengan ID yang berbeda-beda. Selama perjalanan ini, penting bahwa paket-paket data ini diarahkan melalui jaringan-jaringan ini untuk mencapai tujuan akhirnya (Hasrul Hasrul, 2020; Sujalwo, Bana Handaga and Heru Supriyono, 2020). Untuk melakukan ini, digunakan sebuah perangkat yang dikenal sebagai router . Tugas utama router adalah menghubungkan jaringan-jaringan dengan ID yang berbeda ini. Salah satu tanggung jawab penting dari router adalah menentukan rute terbaik (best path) yang harus diambil oleh setiap paket dan kemudian mengarahkannya menuju tujuan akhirnya. Seluruh proses ini dikenal dengan istilah "routing."

Saat ini, MikroTik telah banyak digunakan oleh berbagai penyedia layanan internet dan administrator sistem dalam berbagai lingkungan, seperti kafe internet, pusat permainan, kantor, sekolah, kampus, dan berbagai tempat lainnya. Sistem operasi MikroTik menjadikan komputer router menjadi handal dan efisien (Adhiwibowo and Mindatama, 2019). OS MikroTik menawarkan sejumlah fungsi dan alat yang beragam, membuatnya cocok untuk penggunaan di jaringan berbasis kabel maupun nirkabel. Routing, yang merupakan bagian penting dalam struktur jaringan, memainkan peran sentral dalam mengelola arus data dari satu komputer ke komputer lainnya (Sidik *et al.*, 2021). Router,

sebagai komponen utama yang bertugas mengelola perutean, memiliki tanggung jawab yang krusial dalam menjaga kelancaran dan efisiensi jaringan(Saragi *et al.*, 2021).

Perkembangan jaringan komputer telah menciptakan persaingan ketat di antara perusahaan-perusahaan yang berlomba-lomba untuk memberikan solusi terbaik bagi kebutuhan jaringan yang semakin kompleks. Dalam hal ini, MikroTik dan Cisco adalah dua perusahaan yang sering diperbincangkan, terutama dalam konteks jaringan komputer dan media transmisi. Kedua perusahaan ini telah berfokus pada pengembangan solusi jaringan yang efisien dan andal untuk berbagai keperluan. Mari kita telusuri lebih dalam tentang MikroTik, termasuk pengertian, sejarah, fitur, dan perbedaannya dengan Cisco serta router biasa.

10.1.1 Pengertian MikroTik:

MikroTik adalah perusahaan yang mengkhususkan diri dalam pengembangan perangkat keras dan perangkat lunak jaringan yang efisien, dengan fokus utama pada router dan sistem operasi jaringan. Solusi MikroTik digunakan secara luas dalam berbagai skenario, dari jaringan kecil hingga jaringan yang lebih besar dan kompleks.

10.1.2 Sejarah MikroTik

MikroTik dimulai pada tahun 1996 di Latvia, ketika pendiri John Trully mendirikan perusahaan ini dengan tekad untuk menciptakan solusi inovatif dalam industri jaringan. Pada awalnya, fokus perusahaan ini lebih pada perangkat keras nirkabel yang dapat memungkinkan koneksi jaringan tanpa kabel secara efisien. Dalam beberapa tahun pertama, MikroTik meraih popularitas sebagai penyedia perangkat keras nirkabel yang handal dan efektif dalam mengatasi tantangan konektivitas nirkabel.

Namun, visi dan komitmen MikroTik terhadap pengembangan teknologi jaringan tidak berhenti di situ. Menyadari bahwa tantangan dalam pengelolaan dan routing jaringan semakin

meningkat, MikroTik memutuskan untuk memperkenalkan sesuatu yang lebih: RouterOS. Pada titik ini, perusahaan mengambil langkah signifikan dengan merancang sistem operasi khusus untuk perangkat keras jaringan mereka.

RouterOS menjadi inti dari solusi MikroTik, memberikan fondasi yang kuat bagi perangkat keras mereka untuk menjadi lebih dari sekadar perangkat nirkabel (Oka *et al.*, 2022). Dengan penekanan pada fitur routing dan manajemen jaringan yang lebih canggih, RouterOS memungkinkan pengguna untuk mengelola lalu lintas data, mengarahkan koneksi, dan menjaga keamanan jaringan dengan lebih efisien dan efektif.

Pertumbuhan dan evolusi MikroTik tidak hanya terjadi dalam hal teknologi, tetapi juga dalam pengaruhnya di industri jaringan. Produk MikroTik semakin banyak digunakan oleh penyedia layanan internet (ISP), pengelola jaringan bisnis, serta individu yang ingin mengoptimalkan konektivitas dan manajemen jaringan mereka.

Dengan inovasi berkelanjutan, komitmen terhadap keunggulan, dan dedikasi untuk memenuhi kebutuhan pengguna, MikroTik terus memainkan peran penting dalam memajukan solusi jaringan yang efisien dan handal. Sejarah perusahaan ini merupakan kisah tentang bagaimana visi dan tekad seseorang dapat membentuk landasan teknologi yang memengaruhi cara kita terhubung dan berkomunikasi dalam dunia yang semakin terhubung ini.

Perbedaan mendasar antara MikroTik dan Cisco terletak pada skala penggunaan dan sasaran pasar solusi jaringan mereka. Meskipun keduanya berfungsi sebagai perangkat penghubung jaringan komputer (router), perbedaan utama muncul dalam rentang penggunaan yang dituju oleh masing-masing perusahaan. Cisco cenderung mengarahkan solusinya ke lingkungan jaringan berskala besar, sementara MikroTik lebih berfokus pada lingkungan jaringan berskala kecil hingga menengah.

Cisco dikenal sebagai pemimpin di industri jaringan dan umumnya digunakan oleh perusahaan besar, organisasi besar, dan penyedia layanan internet. Solusi jaringan Cisco mampu mengelola kompleksitas jaringan skala besar dengan fitur-fitur tingkat lanjut dan dukungan untuk lingkungan yang sangat terpusat. Di sisi lain, MikroTik lebih populer dalam lingkup bisnis kecil hingga menengah, serta pengguna individu. Produk MikroTik menawarkan solusi yang terjangkau dan fleksibel untuk pengelolaan jaringan yang lebih sederhana namun efektif.

10.2 Fitur-Fitur Router Mikrotik

Router MikroTik adalah perangkat jaringan yang dikenal dengan berbagai fitur dan kemampuan yang kuat. Berikut ini adalah beberapa fitur utama yang sering ditemukan pada router MikroTik:

10.2.1 Routing dan Forwarding:

Router MikroTik mendukung berbagai protokol routing, termasuk RIP, OSPF, BGP, dan static routing. Ini memungkinkan pengguna untuk mengatur dan mengelola aliran lalu lintas data di jaringan. Terkait fitur Routing dan Forwarding pada Router MikroTik, ini adalah komponen kunci yang memungkinkan perangkat untuk mengatur dan mengarahkan aliran lalu lintas data di jaringan dengan efisien. Dalam lingkup jaringan yang lebih besar, pengelolaan lalu lintas yang optimal menjadi sangat penting untuk memastikan koneksi yang stabil, keamanan data, dan efisiensi penggunaan sumber daya jaringan.

1. **Protokol Routing:**
   Router MikroTik mendukung beberapa protokol routing yang memungkinkan perangkat untuk berkomunikasi dengan router lain dan mengetahui rute terbaik untuk mengirimkan data. Ini mencakup:

a. RIP (*Routing Information Protocol*): Protokol routing sederhana yang menggunakan metrik hop count untuk menentukan jalur terbaik.
b. OSPF (*Open Shortest Path First*): Protokol routing yang lebih canggih, cocok untuk jaringan yang lebih besar, karena menghitung rute berdasarkan biaya berdasarkan bandwidth dan kecepatan.
c. BGP (*Border Gateway Protocol*): Protokol routing yang digunakan di internet untuk menghubungkan jaringan autonomus (AS). BGP membantu mengarahkan lalu lintas di antara jaringan yang berbeda secara efisien.
d. *Static Routing*: Pengaturan manual dari tabel routing yang memungkinkan administrator untuk secara langsung menentukan rute tujuan.

2. **Load Balancing**:
   Salah satu aspek penting dari routing adalah kemampuan untuk membagi lalu lintas secara merata melalui jalur yang tersedia. Router MikroTik memungkinkan load balancing, di mana lalu lintas diarahkan melalui jalur yang berbeda berdasarkan berbagai faktor seperti beban lalu lintas, kecepatan, atau jenis layanan.
3. **Redundansi dan Failover:**
   Routing juga berperan dalam menciptakan sistem jaringan yang tahan bencana. Router MikroTik memungkinkan konfigurasi redundansi, di mana jika satu jalur mati atau bermasalah, lalu lintas dapat diarahkan melalui jalur alternatif.
4. **Quality of Service (QoS):**
   Salah satu tantangan dalam routing adalah mengelola lalu lintas yang berbeda dengan prioritas yang berbeda. Router MikroTik mendukung fitur QoS yang memungkinkan administrator mengatur prioritas lalu lintas berdasarkan jenis layanan atau kepentingan.

5. **Pemantauan dan Pengelolaan:**
   Untuk mengelola aliran lalu lintas, router perlu memiliki alat untuk memantau kinerja jaringan. Router MikroTik menyediakan alat pemantauan yang membantu administrator memantau kesehatan jaringan, memeriksa penggunaan bandwidth, dan mengidentifikasi potensi masalah. Fitur Router MikroTik memungkinkan administrator jaringan untuk merancang, mengimplementasikan, dan mengelola arus lalu lintas dengan lebih efisien dan efektif, sesuai dengan ukuran dan kompleksitas jaringan yang berbeda.

10.2.2 Firewall dan Security:

MikroTik memiliki fitur firewall yang kuat, termasuk filter packet, NAT, dan stateful inspection. Ini membantu melindungi jaringan dari ancaman dan serangan. Dalam era digital yang terhubung, keamanan jaringan menjadi sangat penting untuk melindungi data, perangkat, dan sumber daya jaringan dari ancaman yang beragam. MikroTik mengakui pentingnya keamanan ini dan telah melengkapi perangkat mereka dengan fitur firewall yang kuat untuk melindungi jaringan dari serangan dan ancaman yang mungkin terjadi.

1. **Filter Packet**
   Fitur ini memungkinkan administrator untuk mengontrol lalu lintas yang masuk dan keluar dari jaringan berdasarkan berbagai kriteria, seperti alamat IP, port, protokol, dan lainnya. Dengan mengatur aturan-aturan khusus, administrator dapat mengizinkan atau memblokir lalu lintas tertentu, memberikan tingkat kontrol yang tinggi terhadap apa yang diperbolehkan masuk atau keluar dari jaringan.
2. **Network Address Translation (NAT):**
   NAT adalah teknik yang umum digunakan untuk mengubah alamat IP dan port dalam header packet. MikroTik mendukung NAT yang membantu mengamankan jaringan

dengan menyembunyikan alamat IP internal dari jaringan publik, sehingga mengurangi potensi serangan langsung pada perangkat internal.

3. **Stateful Inspection**
   Stateful inspection adalah metode pemeriksaan lalu lintas yang memahami hubungan antara paket-paket dalam sesi. Ini memungkinkan firewall untuk membuat keputusan yang lebih cerdas berdasarkan status sesi, sehingga dapat mengidentifikasi lalu lintas yang sebenarnya diharapkan dan memblokir yang tidak diinginkan.
4. **Intrusion Detection and Prevention**
   Beberapa perangkat MikroTik memiliki kemampuan deteksi dan pencegahan intrusi (IDS/IPS). Ini memungkinkan perangkat untuk mendeteksi aktivitas mencurigakan atau berbahaya dalam lalu lintas jaringan dan mengambil tindakan untuk mencegahnya.
5. **Application Layer Filtering**
   Firewall MikroTik juga mendukung filtering lapisan aplikasi, yang memungkinkan deteksi dan pengendalian lalu lintas berdasarkan jenis aplikasi. Ini membantu mengurangi risiko dari aplikasi berbahaya atau tidak diinginkan.
6. **VPN and Encrypted Communication**
   MikroTik mendukung berbagai protokol VPN untuk memastikan komunikasi yang aman di antara lokasi dan perangkat yang berbeda. Ini penting dalam melindungi data yang dikirim melalui jaringan publik.
7. **Logging dan Monitoring**
   Firewall MikroTik memiliki kemampuan untuk mencatat dan memantau aktivitas lalu lintas. Ini memungkinkan administrator untuk memantau potensi ancaman, menganalisis pola serangan, dan mengambil tindakan yang sesuai.

10.3 Konfigurasi Dasar Router Mikrotik

Saat mengatur router MikroTik yang baru, terkadang kita merasakan kesulitan dalam mengakses interface ether1 secara remote. Setelah berhasil melakukan remote ke router, konfigurasi yang terdapat di dalamnya bisa terlihat tidak begitu akrab. Namun, ini bukan disebabkan oleh adanya masalah pada router MikroTik itu sendiri, melainkan karena adanya konfigurasi default. Bagi beberapa orang, memulai konfigurasi dari awal tanpa adanya konfigurasi awal lebih disukai. Namun, bagi mereka yang masih belajar mengenai konfigurasi MikroTik, adanya konfigurasi default justru sangat membantu.

Proses mengakses atau meremote perangkat router MikroTik menjadi langkah penting saat melakukan konfigurasi pada perangkat tersebut. Dalam materi ini, kita akan menjelaskan metode untuk mengakses MikroTik. Sebelum melakukan remote pada router MikroTik, langkah awal yang perlu dilakukan adalah mempersiapkan koneksi fisik melalui kabel LAN atau menghubungkan perangkat ke jaringan Wi-Fi yang disediakan oleh routerboard MikroTik.

Persiapan Koneksi Fisik:

Sebelum dapat mengakses atau meremote router MikroTik, Anda perlu memastikan bahwa perangkat komputer atau laptop Anda terhubung secara fisik ke perangkat router tersebut. Anda dapat menggunakan kabel LAN untuk menghubungkan perangkat komputer langsung ke salah satu port Ethernet pada router MikroTik. Alternatifnya, jika router MikroTik menyediakan jaringan Wi-Fi, Anda dapat menghubungkan perangkat komputer ke jaringan tersebut menggunakan koneksi nirkabel.

Setelah koneksi fisik terjalin, Anda dapat melanjutkan untuk mengakses router MikroTik dan melakukan konfigurasi sesuai kebutuhan Anda. Dalam beberapa kasus, Anda mungkin perlu menggunakan perangkat tambahan seperti kabel LAN atau

mengkonfigurasi pengaturan Wi-Fi pada perangkat komputer Anda untuk terhubung ke jaringan Wi-Fi router MikroTik.

Tabel 10.1. Akses Mikrotik Routerboard

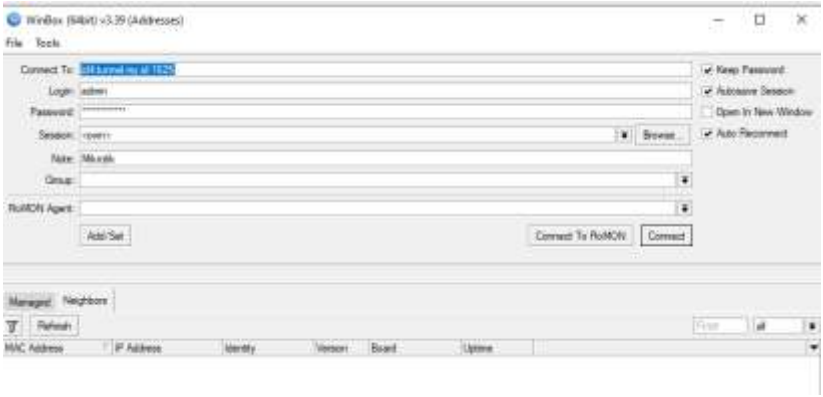
Akses via	Koneksi	Text Base	GUI	Need IP
Keyboard	Langsung ke PC	yes		
Serial Console	Konektor kabel serial	yes		
Telnet & SSh	Layer 3	yes		yes
Winbox	Menggunakan OS windows / Linux (wine)	yes	yes	
FTP	Layer 3	yes		yes
API	Socket Programming			yes
Web	Layer 3		yes	yes
MAC-Telnet	Layer 2	yes		

Salah satu cara paling umum dan sederhana yang digunakan oleh administrator jaringan dalam mengakses dan mengkonfigurasi perangkat MikroTik adalah dengan menggunakan alat bernama Winbox. Winbox merupakan sebuah alat konfigurasi yang memungkinkan administrator untuk terhubung dengan router menggunakan alamat MAC atau IP dengan antarmuka tampilan grafis (GUI), yang sangat mempermudah dalam menjalankan konfigurasi pada perangkat Router MikroTik. Untuk mengakses Winbox, Anda dapat mengunduhnya dari situs resmi MikroTik di www.mikrotik.com.

Winbox sebagai alat utama untuk melakukan konfigurasi pada Router MikroTik. Sebelum memulai proses konfigurasi, sangat dianjurkan untuk mengenal antarmuka dan tampilan yang disediakan oleh Winbox, yang akan menjadi alat utama Anda dalam berinteraksi dengan Router MikroTik.

Secara default, setiap Router MikroTik dikonfigurasi dengan alamat IP 192.168.88.1/24 pada port ether1. Username yang biasanya digunakan adalah "admin", dan awalnya tidak memerlukan kata sandi. Dengan memanfaatkan Winbox, Anda akan dapat dengan mudah terhubung dengan router, mengelola pengaturan, dan menjalankan konfigurasi yang diperlukan.

Winbox telah menjadi pilihan populer dalam dunia administrasi jaringan karena antarmuka yang intuitif dan penggunaannya yang mudah. Dengan tampilan GUI yang sederhana, administrator jaringan dapat lebih fokus pada mengatur dan mengelola konfigurasi Router MikroTik tanpa harus menghadapi kompleksitas teknis yang lebih mendalam. Dengan demikian, penggunaan Winbox menjadi langkah awal yang sangat nyaman dan efisien dalam menjalankan konfigurasi pada perangkat MikroTik Anda.

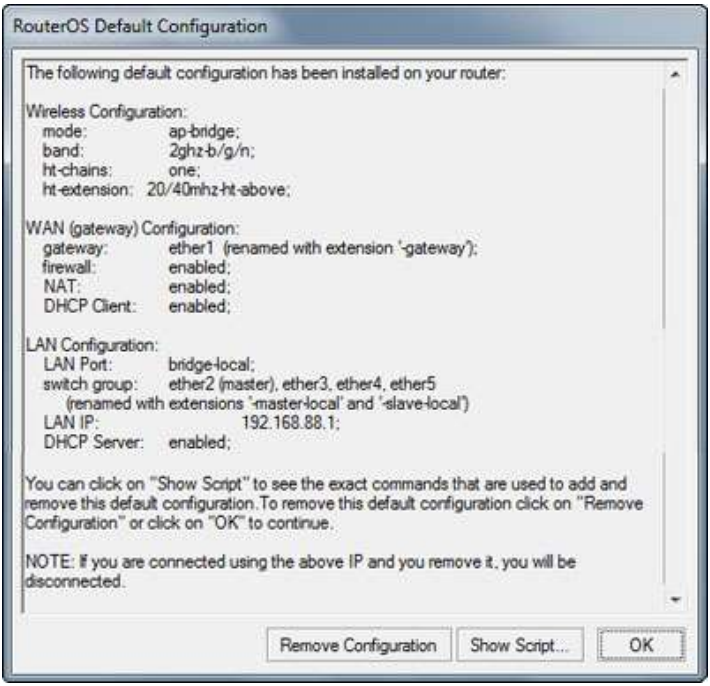


Gambar 10.1. Akses Mikrotik menggunakan winbox

Winbox memiliki kemampuan untuk secara otomatis mendeteksi perangkat MikroTik yang sudah terpasang dalam jaringan yang sama. Proses ini dilakukan dengan cara mengidentifikasi alamat MAC dari antarmuka Ethernet yang terhubung ke perangkat MikroTik. Pengguna dapat mengakses

perangkat MikroTik menggunakan Winbox baik melalui IP Address atau MAC Address yang terkait dengan perangkat tersebut.

Pada router yang memiliki konfigurasi default, seringkali informasi mengenai keberadaan konfigurasi default tersebut akan ditampilkan setelah Anda login melalui konsol atau akan muncul kotak dialog saat Anda melakukan remote menggunakan Winbox. Gambar 10.1 merupakan kotak dialog pada saat diremote dengan winbox :

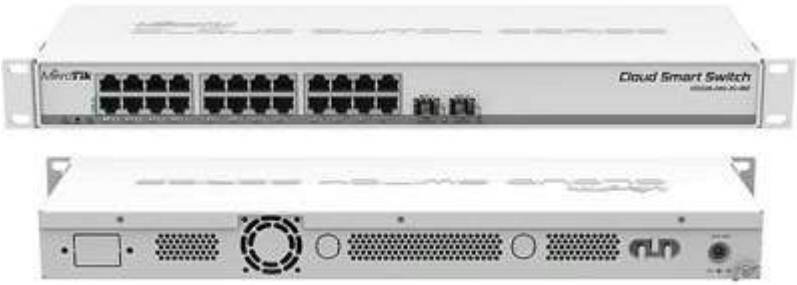


Gambar 10.2. Notifikasi Awal Remote Mikrotik

Kotak dialog ini memberikan tiga opsi yang berbeda. "*Remove Configuration*" akan menghapus konfigurasi default sehingga router akan menjadi bersih tanpa adanya konfigurasi apapun. Opsi "*Show Script*" akan menampilkan skrip konfigurasi

default dalam bentuk script. Sedangkan opsi "OK" akan menerapkan konfigurasi default ke router tersebut.

Setiap jenis router memiliki konfigurasi default yang unik tergantung pada kondisi perangkat kerasnya. Anda dapat menampilkan skrip konfigurasi default dengan menggunakan perintah "*/system default-configuration print*".



Gambar 10.3. Hardware Mikrotik

Default konfigurasi Dasar Router secara umum.

1. **Konfigurasi Ethernet**

   Default konfigurasi memberikan nama yang jelas pada setiap *interface* (*interface*) yang ada pada router. Hal ini bertujuan untuk membantu pengguna dalam menentukan di mana sebaiknya kabel disambungkan.

   a. Interface "ether1" akan secara otomatis diberi nama "**ether1-WAN**". Nama ini dipilih dengan asumsi bahwa pengguna akan menghubungkan kabel yang terhubung ke sumber internet langsung ke interface ini. Sehingga, pengguna dapat dengan mudah mengidentifikasi bahwa interface tersebut digunakan sebagai gerbang (*gateway*) ke dunia luar.
   b. Interface "ether2" akan diberi nama "**etherx-master**". Ini dirancang dengan tujuan memberikan pemahaman

bahwa interface ini memiliki peran sebagai interface utama (master) di dalam jaringan lokal.

c. Sementara itu, interface "ether3" hingga interface terakhir akan diberi nama "**ether3-LAN**" dan seterusnya. Pada interface-interface ini, konfigurasi "master-port" akan diarahkan ke "ether2". Dengan demikian, interface-interface ini akan berada dalam segmen jaringan yang sama dengan "ether2" dan dapat membentuk bagian dari jaringan lokal.

Pengguna memiliki fleksibilitas untuk menghubungkan perangkat jaringan lokal ke interface "ether2", "ether3", dan seterusnya. Namun, penting untuk dicatat bahwa interface "ether1" tidak digunakan untuk koneksi jaringan lokal. Segmen jaringan lokal juga harus berada dalam segmen yang sama untuk memungkinkan komunikasi yang efektif antara interface-interface tersebut. Dengan demikian, default konfigurasi tidak hanya memberikan nama yang jelas pada setiap interface, tetapi juga membantu pengguna dalam merencanakan dan menghubungkan perangkat dengan lebih baik dalam jaringan mereka.

2. IP Address

Konfigurasi default pada router MikroTik juga melibatkan pemberian alamat IP pada interface yang terhubung ke jaringan lokal. Misalnya, dalam banyak kasus, konfigurasi default akan mengatur alamat IP "192.168.88.1/24" pada interface yang relevan. Sebagai hasilnya, jaringan lokal akan menggunakan segmen alamat IP "192.168.88.0/24".

Namun, penting untuk dicatat bahwa ada pengecualian pada produk-produk tertentu yang hanya memiliki satu interface Ethernet. Contohnya termasuk seri produk seperti RB411, RB433, RB435, RB800, CCR, dan RB1000. Pada produk-produk ini, alamat IP tetap akan diatur pada interface "**ether1**".

3. **DHCP**

   Dalam konteks konfigurasi default, router MikroTik menghadirkan beberapa fitur yang secara otomatis mempermudah pengguna dalam mengatur alamat IP dan mengelola koneksi internet. Salah satu fitur utama yang mendukung hal ini adalah pengaturan DHCP Server dan DHCP Client. Mari kita melanjutkan dan mengeksplorasi lebih mendalam mengenai bagaimana kedua fitur ini berkontribusi untuk membuat konfigurasi awal menjadi lebih mudah dan efisien.

4. **DHCP Server untuk Jaringan Lokal**:

   Pada interface yang terhubung ke jaringan lokal, router MikroTik secara default menjalankan layanan DHCP Server. Hal ini memungkinkan klien, seperti perangkat komputer atau ponsel, yang terhubung ke interface ethernet tertentu (selain "ether1"), untuk secara otomatis mendapatkan alamat IP. Dengan menggunakan DHCP, proses pengaturan alamat IP, subnet mask, gateway, dan DNS dilakukan secara otomatis. Ini sangat bermanfaat karena mengurangi kebutuhan untuk mengonfigurasi setiap perangkat secara manual.

5. **DHCP Client untuk Koneksi Internet:**

   Interface "ether1" pada router MikroTik juga diatur sebagai DHCP Client. Ini berarti bahwa ketika Anda menyambungkan interface "ether1" ke sumber internet atau ISP melalui modem, router secara otomatis akan meminta dan menerima alamat IP dinamis dari ISP. Dengan demikian, router akan langsung terhubung ke internet tanpa perlu pengaturan manual yang rumit. Fitur ini sangat mengurangi kerumitan dalam mengatur koneksi internet.

6. **Efisiensi dalam Pengaturan Awal:**

   Kombinasi fitur DHCP Server dan DHCP Client dalam konfigurasi default menghasilkan pengalaman pengguna yang lebih efisien saat mengatur router MikroTik pertama kali.

Pengguna tidak perlu khawatir tentang mengatur alamat IP secara manual di jaringan lokal atau menghadapi rintangan dalam menghubungkan ke internet. Fitur ini juga sangat bermanfaat dalam lingkungan yang lebih besar, di mana jumlah perangkat dan klien yang terhubung dapat berjumlah besar.

Dengan demikian, router MikroTik memberikan konfigurasi yang lebih user-friendly bagi pengguna dengan secara otomatis mengelola alamat IP untuk jaringan lokal dan menerima alamat IP dinamis dari ISP. Ini berarti konfigurasi awal menjadi lebih sederhana dan mengurangi tugas administratif, memungkinkan pengguna untuk lebih fokus pada pengelolaan jaringan secara keseluruhan.

7. Wireless

Pengaturan Wireless dalam Default Konfigurasi Router MikroTik

Pada router MikroTik yang memiliki interface wireless terintegrasi, Anda akan menemukan default konfigurasi yang telah disesuaikan dengan kondisi perangkat keras tertentu. Setiap pengaturan dirancang untuk memberikan pengalaman yang optimal dalam menggunakan jaringan nirkabel, dan ini mencakup berbagai aspek, dari mode hingga keamanan.

Mode Operasi:

Konfigurasi default akan menyesuaikan mode operasi berdasarkan lisensi yang dimiliki oleh router. Untuk router dengan lisensi Level 4 ke atas, mode "AP Bridge" akan digunakan sebagai default. Sedangkan pada router dengan lisensi Level 3, mode "Station" akan diatur sebagai default. Mode "AP Bridge" memungkinkan router berperan sebagai titik akses (access point), sementara mode "Station" digunakan saat router terhubung ke titik akses lain.

Band dan Frekuensi:

Router yang mendukung 2,4 GHz dan MIMO akan menggunakan band "2,4 GHz b/g/n" sebagai default, sementara router yang mendukung 5 GHz dan MIMO akan menggunakan band "5 GHz a/n". Frekuensi default untuk router 2,4 GHz adalah 2412, sedangkan untuk router 5 GHz adalah 5300.

Chain (Rantai):

Konfigurasi default akan mengaktifkan dual chain pada router yang mendukungnya, dengan mengatur chain 0 dan 1. Pada router yang masih menggunakan single chain, hanya chain 0 yang diaktifkan.

Profil Keamanan:

Profil keamanan akan dibuat oleh konfigurasi default dengan menggunakan nomor seri router sebagai kunci WPA dan WPA2. Ini memastikan bahwa koneksi nirkabel dienkripsi secara aman dengan menggunakan kunci yang unik untuk setiap router.

SSID (*Service Set Identifier*):

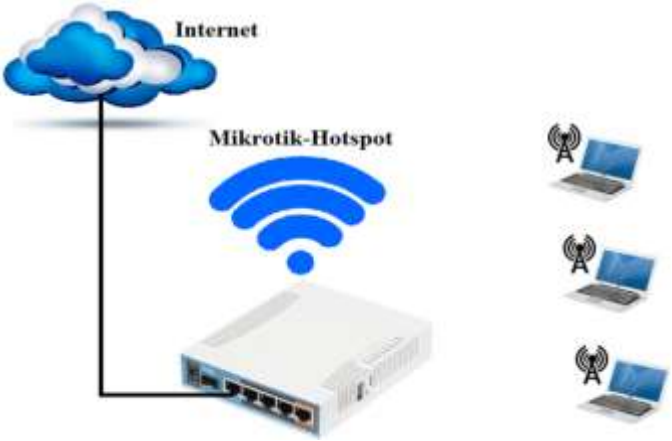
SSID akan ditentukan berdasarkan alamat MAC *interface wireless*. Biasanya, SSID akan diatur sebagai "MikroTik-[Enam Digit Terakhir MAC-Address]". Hal ini membantu mengidentifikasi jaringan nirkabel secara unik berdasarkan alamat MAC.

Dengan pengaturan ini, pengguna mengalami kenyamanan dan keamanan saat menggunakan jaringan nirkabel pada router MikroTik. Pengaturan default yang disesuaikan dengan fitur perangkat keras mengurangi kompleksitas dalam mengonfigurasi jaringan nirkabel. Namun, untuk pengguna yang ingin melakukan penyesuaian lebih lanjut, MikroTik juga memberikan fleksibilitas untuk mengubah dan mengatur setiap pengaturan sesuai kebutuhan mereka.

10.4 Konfigurasi Access Point Menggunakan Router Mikrotik (Studi Kasus)

Beberapa Tipe perangkat MikroTik menawarkan fitur wireless, salah satunya adalah MikroTik RB951-2n. Dalam situasi seperti pada contoh perangkat tersebut, kita akan melakukan konfigurasi agar perangkat terhubung ke internet atau ke *Access Point* (AP) melalui perangkat MikroTik.

Dalam skenario lab ini, Router yang digunakan adalah versi MikroTik RB951-2n. Proses konfigurasi dilakukan melalui aplikasi Winbox, yang menyediakan antarmuka grafis yang memudahkan pengguna dalam mengatur perangkat MikroTik. Nantinya, kita akan melakukan konfigurasi pada perangkat MikroTik RB951-2n agar dapat terhubung ke internet atau AP. Dengan menggunakan aplikasi Winbox, pengguna dapat mengakses perangkat MikroTik dengan mudah dan mengatur pengaturan jaringan sesuai kebutuhan.

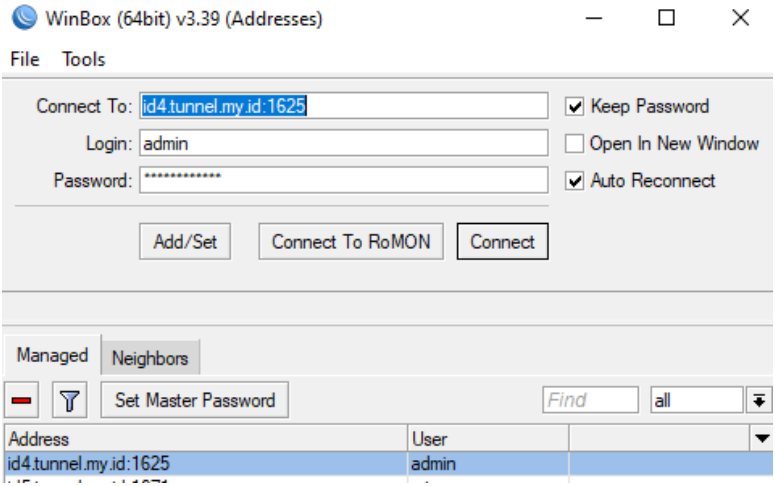


Gambar 10.4. Topologi Jaringan Access Point Router Mikrotik

Pada gambar 10.4 terlihat bahwa mikrotik bertindak selain sebagai hotspot server juga sebagai wireless hotspot. Pada beberapa mikrotik sudah di lengkapi dengan wlan yang dapat di

gunakan sebagai media access point ataupun station. Berikut beberapa langkah sederhana konfigurasi dasar accesspoint menggunakan mikrotik.

1. Pertama kita harus masuk ke Winbox-nya:

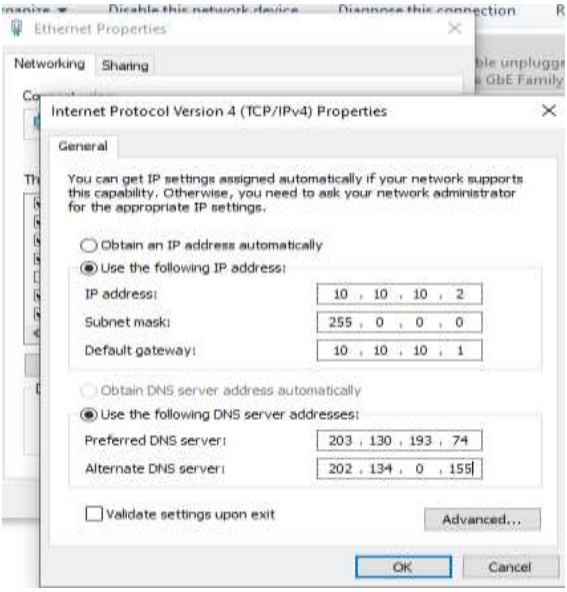


2. Setelah masuk, lalu konfigurasikan IP yang terhubung dari PC ke Port Mikrotik. Dengan perintah:

3. Untuk menghubungkan komputer ke antarmuka Ether2 pada Router MikroTik dengan IP 10.10.10.1/24 (kelas C), Anda perlu mengkonfigurasi alamat IP pada komputer sesuai dengan jaringan yang diatur pada Router MikroTik.
   Buka Pengaturan Jaringan di Komputer:
   - Klik kanan pada ikon jaringan di area notifikasi atau buka "Control Panel" dan pilih "*Network and Sharing Center*."
   - Pilih "Change adapter settings."

   Konfigurasi Lokal Area Connection:
   - Klik kanan pada "*Local Area Connection*" yang terhubung ke router MikroTik dan pilih "Properties."
   - Cari dan klik dua kali pada protokol "Internet Protocol Version 4 (TCP/IPv4)."

   Konfigurasi Alamat IP pada Komputer:
   - Pilih opsi "Use the following IP address."
   - Isikan alamat IP pada kolom "IP address." Misalnya, 10.10.10.2.
   - Isikan subnet mask 255.255.255.0 (kelas C).
   - Isikan alamat IP Gateway dengan 10.10.10.1 (IP antarmuka Ether2 pada router MikroTik).
   - Isikan DNS Server sesuai preferensi Anda atau biarkan kosong jika ingin menggunakan DNS default dari ISP.
     Klik OK dan Selesai:



Setelah mengkonfigurasi alamat IP, klik OK untuk menyimpan pengaturan. Komputer sekarang akan memiliki alamat IP yang sesuai dengan jaringan yang diatur pada Router MikroTik. Dengan melakukan langkah-langkah di atas, Anda telah mengkonfigurasi komputer untuk berada dalam satu jaringan dengan antarmuka Ether2 pada Router MikroTik. Pastikan untuk mengonfigurasi alamat IP pada komputer sesuai dengan rentang yang diatur pada router MikroTik (10.10.10.1-10.10.10.254).

4. Langkah-langkah untuk mengaktifkan fitur wireless pada Router MikroTik menggunakan antarmuka grafis (GUI) melalui aplikasi Winbox:

   Buka Menu Wireless:

   - Buka aplikasi Winbox dan terhubung ke perangkat MikroTik.
   - Pada jendela utama Winbox, pilih menu "Wireless."

Pilih Interface Wlan1 dan Aktifkan:

- Dalam menu "Wireless," pilih antarmuka "wlan1."
- Aktifkan antarmuka dengan mencentang kotak "Enable."

Konfigurasi Band dan Pengaturan Lain:

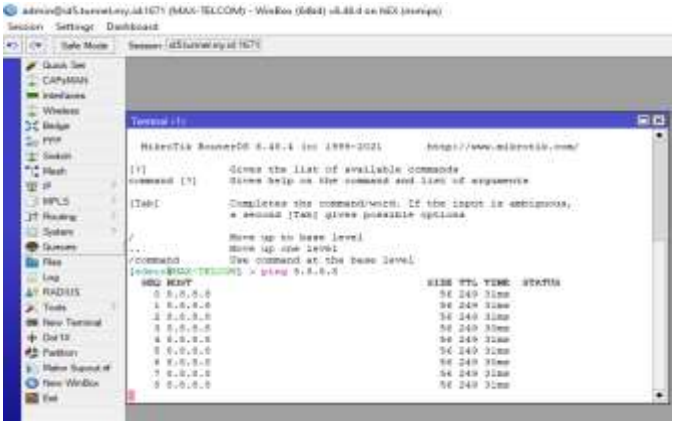
- Klik dua kali pada antarmuka "wlan1" untuk membuka jendela pengaturan.
- Pada tab "Wireless," pilih band "2GHz B/G/N" dari drop-down menu "Band."
- Klik tombol "Apply" untuk menyimpan pengaturan.

Lakukan Pencarian Access Point:

- Di jendela pengaturan antarmuka "wlan1," pilih tab "Wireless."
- Klik tombol "Scan" untuk mencari Access Point yang ada di sekitar.
- Setelah daftar Access Point muncul, pilih Access Point yang ingin Anda hubungkan.

Hubungkan ke Access Point:

- Setelah memilih Access Point, klik tombol "Connect."
- Setelah terhubung, klik tombol "Apply" dan kemudian "OK" untuk menyimpan pengaturan.



Dengan mengikuti langkah-langkah di atas, Anda telah berhasil mengaktifkan fitur wireless pada Router MikroTik. Pastikan untuk mengatur band dan pengaturan lainnya sesuai dengan preferensi Anda dan menghubungkan ke Access Point yang diinginkan. Nah, kalau sudah, coba test Ping via Mikrotik Di Menu New Terminal, ketik Ping 8.8.8.8, jika Reply lalu test ping melalui CMD ke 8.8.8.8, jika berhasil, maka PC sudah bisa Akses Internet melalui Router.

DAFTAR PUSTAKA

Adhiwibowo, W. and Mindatama, W. 2019. 'IMPLEMENTASI SISTEM VOUCHER DENGAN ROUTER MIKROTIK', *Jurnal Pengembangan Rekayasa dan Teknologi*, 15(2). Available at: https://doi.org/10.26623/jprt.v15i2.1766.

Hasrul Hasrul, A.M.L. 2020. 'Pengembangan Jaringan Wireless Menggunakan Mikrotik Router Os Rb750 Pada Pt. Amanah Finance Palu', *Jurnal Elektronik Sistem Informasi dan Komputer*, 3(1).

Oka, P.G. *et al.* 2022. 'Implementasi Bandwidth Management Menggunakan Mikrotik Router Os (Studi Kasus Di Pt. Rejeki Maha Bumi Lestari)', *RESI : Jurnal Riset Sistem Informasi*, 1(1).

Saragi, D.R. *et al.* 2021. 'Implementasi Konfigurasi Hotspot Server Untuk Akses Internet Menggunakan Mikrotik Router Pada Dinas Lingkungan Hidup Pematangsiantar', *Device*, 11(2). Available at: https://doi.org/10.32699/device.v11i2.2090.

Sidik, S. *et al.* 2021. 'Implementasi VPN Berbasis Point To Point Tunneling Protocol (PPTP) Menggunakan Mikrotik Router Board', *Jurnal Infortech*, 3(1). Available at: https://doi.org/10.31294/infortech.v3i1.10400.

Sujalwo, Bana Handaga and Heru Supriyono. 2020. 'Manajemen Jaringan Komputer dengan Menggunakan Mikrotik Router', *Jurnal Komunikasi dan Teknologi Informasi*, 2(2).

BAB 11
PENGALAMATAN IPv4

Oleh Bambang Suprayogi

11.1 Internet Protocol Address

Internet Protocol Address merupakan identifikasi berupa nilai angka dengan nilai unik di setiap *device* seperti komputer, ponsel, atau gadget pintar lainnya yang merupakan penomoran sebagai pengenal atau identifikasi satu sama lainya dalam jaringan komputer lokal maupun internet.

Fungsi *Internet Protocol Address* selain sebagai identitas alamat atau kode unik dari perangkat yang terhubung satu dengan lainya dalam jaringan internet dan berfungsi sebagai *node* atau alamat pengiriman data ke perangkat lainya sebagai alat untuk mengidentifikasi *host* atau antarmuka jaringan dimana alamat IP dianalogikan sebagai alamat rumah agar paket data yang dikirim dapat sampai tujuan (perangkat) yang tepat dapat menjalin komunikasi satu sama lainnya melalui perangkat dapat berkomunikasi, mengirim serta mengambil data melalui protokol TCP/IP.

Internet Protocol Address sekumpulan angka yang bernilai 4 okta untuk setiap kelompok dan setiap kelompok mempunyai rentang nilai angka antara 0-255, memiliki 2 bagian yaitu *NetworkID* sebagai identitas dalam suatu jaringan dan *HostID* yang merupakan identitas *device* dalam suatu jaringan.

Internet Protocol merupakan sebuah protokol yang mendefinisikan sebuah model TCP/IP *(Transmission Control Protocol/Internet Protocol)* berfungsi mengirimkan sebuah paket dari *device* sumber ke *device* tujuan dalam suatu jaringan komputer berdasarkan nomor IP. Protokol IP menyediakan layanan tanpa

koneksi yang menggunakan dua protokol transport yaitu *Transmission Control Protocol/Internet Protocol* dan *User Datagram Protocol*, dalam skema pengalamatan *(IP Address)* untuk menghubungkan sistem-sistem berbeda yang heterogen dan bersifat *routable* dalam suatu jaringan komputer.
Keunggulan *Transmission Control Protocol/Internet Protocol* ialah :

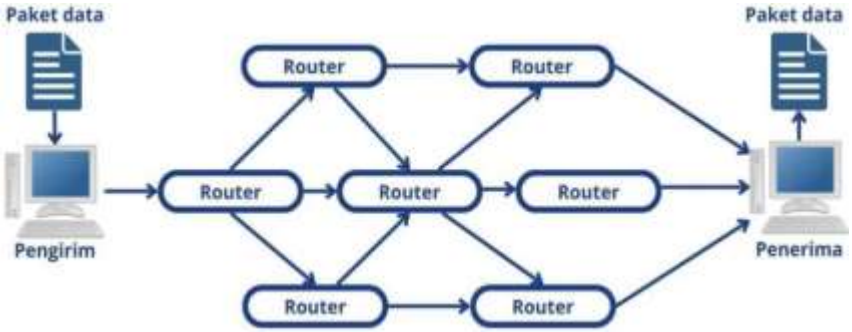
1. *Open Protocol Standard*
   TCP/IP dapat menghubungkan bermacam hardware dan software dan dikembangkan secara independen.
2. *Independen physical network hardware*
   Berfungsi menghubungkan dan berkomunikasi melalui *token ring, dial-up, protokol X.25/AX.25, ethernet* dan media transmisi lainnya dengan berbagai macam *network*.

Fungsi *Transmission Control Protocol/Internet Protocol (TCP/IP)* sebagai berikut :

1. Mengirim file atau berkas terenkripsi dari *node* ke *node* lainya.
2. Pengguna dapat melakukan *remote log in* komputer dari jarak jauh.
3. Dapat mengirim dan menerima mailing dari komputer lain.
4. Dapat menggunakan fitur *network file system* dalam melakukan *sharing file*
5. Dapat melakukan fitur *name server*
6. Menjalankan perintah secara multi pada saat pengiriman paket yamg sama di semua perangkat yang tergabung dalam jaringan, atau *remote execution*.

Cara Kerja TCP/IP dalam melakukan pengiriman paket data sebuah perangkat yang kemudian dikirimkan ke perangkat tujuan melalui jaringan sebagai berikut :

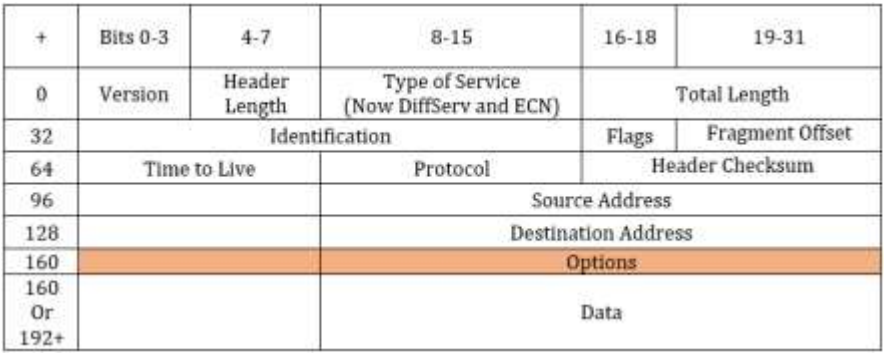
1. Memecah data menjadi paket kecil
   Untuk mempercepat transmisi pengiriman data dan menjaga keamanan maka data yang dikirim diubah menjadi paket-paket kecil dengan memberikan label yang berbeda beserta alamat tujuan data yang akan dikirim.
2. Paket dikirimkan melalui *router*
   Pengiriman paket data dan rute pengiriman paket tersebut ditentukan oleh router, data yang dikirim melalui router ke router lainnya yang terdekat hingga akhirnya sampai di tujuan tergantung besar kecilnya jaringan tersebut.
3. Paket berhasil dikirim ke tujuan
   Layer TCP/IP akan menjalankan fungsinya mulai dari penerjemahan sinyal menjadi data, hingga akhirnya disusun menjadi sebuah *file* utuh saat paket sudah terkirim dan sampai di alamat tujuan.



Gambar 11.1. Cara Kerja TCP/IP
Sumber : https://www.dewaweb.com/blog/pengertian-tcp-ip/

RFC (Request for Comments) merupakan dokumen berisi informasi standarisasi penomoran *internet* yang digunakan oleh suatu *device* dalam suatu jaringan komputer, *Internet* maupun sistem operasi jaringan lainya seperti *Unix*, *Windows*, dan *Novell*

NetWare. *Request for Comments (RFC)* yang diterbitkan oleh *Internet Engineering Task Force (IETF) dan Internet Society (ISO)* salah satunya *Internet Protocol (RFC 791)*, berdasarkan (Forouzan, 2010) : paket-paket data dalam protokol IP dikirim dalam bentuk datagram terdiri atas header dan data, ukuran *header IP* mulai dari 20 sampai dengan 60 *byte* yang berisi *field- field version*, *internet header length, type of service, total length, identification, flags, fragment offset, time to live, protocol, header checksum, source ip address, destinantion ip address, dan ip option* sebagai berikut :



+	Bits 0-3	4-7	8-15	16-18	19-31
0	Version	Header Length	Type of Service (Now DiffServ and ECN)	Total Length	
32	Identification			Flags	Fragment Offset
64	Time to Live		Protocol	Header Checksum	
96			Source Address		
128			Destination Address		
160			Options		
160 Or 192+			Data		

Gambar 11.2. Struktur Header IP4
Sumber : https://www.baeldung.com/cs/popular-network-protocols

Keterangan :

1. *Version*
   Field mulai dari oktet 0 sampai 3 dan berukuran 4 bit, berisi versi format *internet header IPv4*.
2. *Internet Header Length*
   Dimulai dari oktet 4 sampai 7 dan berukuran 4 bit yang berfungsi mengidentifikasi nilai *header IP* dalam bilangan 32 bit (4 *byte*), menunjukan nilai terkecil adalah 20-60 byte yang dinyatakan dalam nilai 5-15.

3. *Type of Service*
   Berfungsi untuk mengarahkan *selection* dari suatu parameter yang mengirimkan datagram ke jaringan lokal dengan ukuran 8 bit yang berfungsi mengidentifikasikan parameter abstrak dari kualitas servis yang diinginkan mulai dari oktet 8 sampai 15. Tiga type of service ini antara lain *low-delay, high-reliability dan high-throughput* dalam jaringan dengan menyediakan *service precedence* untuk pengiriman data yang berprioritas tinggi berikut ini menjelaskan dari *Type of Service*.

Field Type of Service	
Bit 0-2	Precedence
Bit 3	0=Normal Delay, 1=Low Delay
Bit 4	0 = Normal Throughput, 1 = High Throughput
Bit 5	0 = Normal Relibility, 1 = High Relibility
Bit 6-7	Reserved for Future Use
Precedence Code	
111	Network Control
110	Internetwork Control
101	CRITIC/ECP
100	Flash Override
011	Flash
010	Immediate
001	Priority
000	Routine

Gambar 11.3. Field Type of Service and Precedence Code
Sumber : https://notes.shichao.io/tcpv1/ch5/

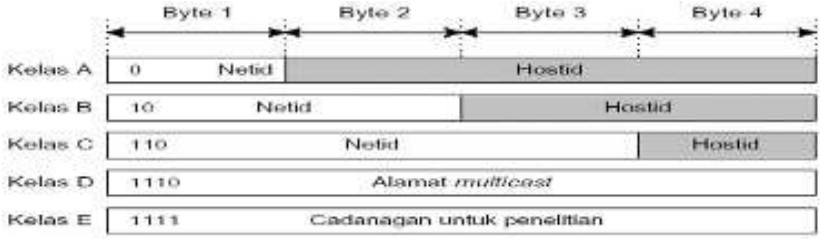
4. *Total Length*
   Field yang dimulai dari oktet ke 16-31 dengan ukuran 16 bit merupakan ukuran dari suatu datagram dengan nilai maksimum 65.535 byte.

5. *Identification*
   Field yang dimulai dari oktet 32-47 (16 bit) yang berfungsi mengidentifikasi pengiriman data dari IP tertentu untuk mengenali *fragment-fragment* sebuah datagram IP dimana *Host* pengirim berfungsi memberi nilai field dan menambahkan nilainya pada datagram IP selanjutnya.
6. *Flags*
   Field yang dimulai dari 48-50 dengan ukuran 3 bit berisi dua buah *flag* dimana sebuah datagram IP mengalami fragmentasi atau tidak.
7. *Fragment Offset*
   Yang dimulai dari ke 51-63 dengan berukuran 13 bit, yang menyatakan pecahan data *(fragment)* posisi dalam datagram, setiap datagram berukuran 65.536 *byte* dengan *fragment offset* dalam ukuran 8 *byte* (64 bit).
8. *Time to Live*
   Field yang dimulai dari oktet ke 64-71 dengan berukuran 8 bit, yang berisi waktu maksimum dalam datagram suatu sistem jaringan, jika bernilai nol maka datagram diabaikan dan *field* tersebut diubah dalam memproses *header* dalam satuan detik.
9. *Protocol*
   Field yang dimulai dari oktet 72-79 dengan ukuran 8 bit, *field* tersebut menyatakan protokol yang digunakan selanjutnya, nilai dari *field* tersebut ICMP bernilai 1(0x01), TCP bernilai 6 (0x06), dan UDP bernilai 17 (0x11) sebagai *multiplex identifier*.
10. *Header Checksum*
    Field yang dimulai dari 80-95 dengan ukuran 16 bit berfungsi melakukan pemeriksaan keberadaan *IP header*.

11. *Source Address*
    Field yang dimulai dari 96-127 dengan ukuran 32 bit digunakan *router* untuk memilih jalur yang tepat / terbaik untuk mengirimkan data tersebut oleh *intermediate*.
12. *Destination Address*
    Field yang berisi alamat IP tujuan mulai dari oktet 128-159 dengan ukuran sama dengan *source address*.
13. *IP Option*
    Field yang berisikan nilai atau *null* dengan ukuran bervariasi dalam sebuah datagram

11.2 Pembagian Kelas IPv4

Menurut (Forouzan, 2013), RCF 791 membagi kelas IPv4 menjadi beberapa kelas, setiap kelas dibedakan berdasarkan nilai oktet pertama dengan nilai angka biner 0 sebagai *high-order* bit, yang reprensentasi dalam decimal. Kelas Ipv4 dibagi menjadi lima kelas yang mempunyai fungsi yang berbeda seperti berikut :

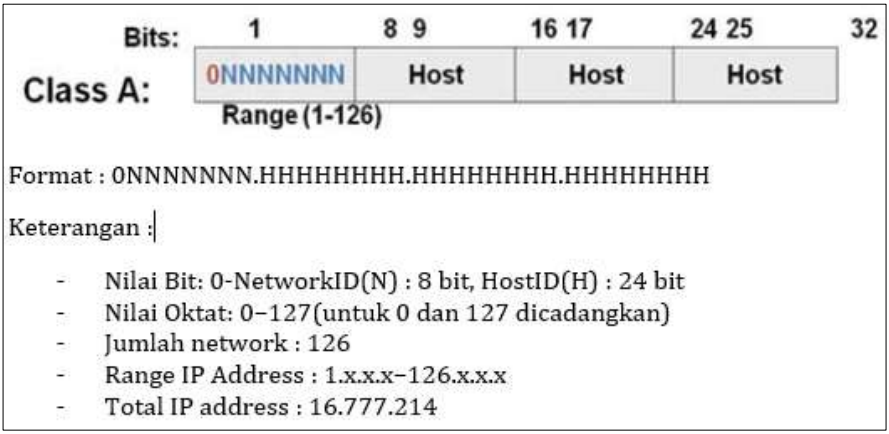


Gambar 11.4. Kelas Ipv4
Sumber : http://solutions24h.com/ip-addressing-schemes/

1. Jaringan IPv4 Kelas A

Jaringan komputer yang memiliki 126 *network* dan setiap *network* bisa menampung sekitar 16.777.214 *host* yang mencakup jaringan komputer yang berskala besar. Jaringan IPv4 kelas A yang mempunyai ukuran 8 bit sebagai alamat

jaringan atau *NetworkID* dan 24-bit sebagai alamat HostID. *Most Signification Bit(MSB)* memiliki nilai biner 0 berada di posisi paling kiri dan nilai selanjutnya untuk *NetID*, nilai oktat berikutnya untuk *HostID* yang disebut *Least Signifacation Bit(LSB)* sebesar 24-bit jadi jumlah alamat IP yang dialokasikan sebanyak 16.777.214 *host* dengan range *IP Address* 1.xxx.xxx.xxx-126.xxx.xxx.xxx.

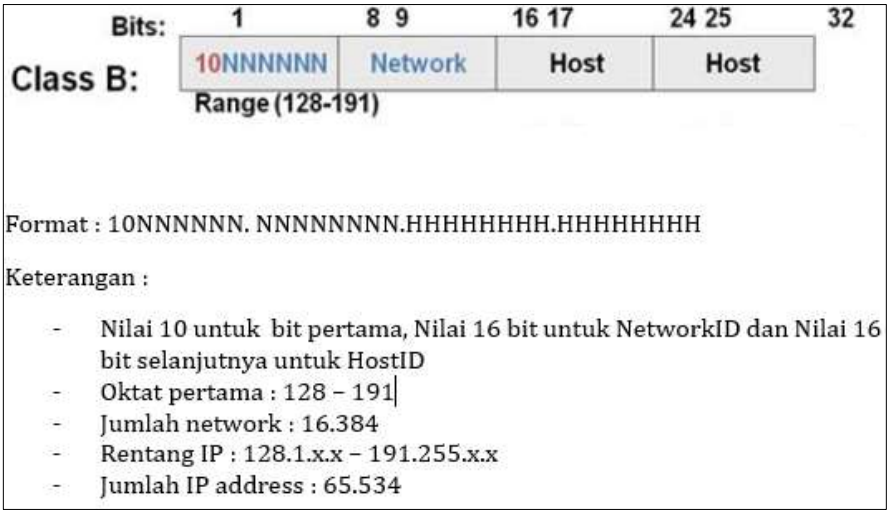


Gambar 11.5. IP Address Kelas A
Sumber : https://basobasri.wordpress.com/

Penerapan dalam Jaringan IPv4 kelas A dengan alamat sebagai berikut 120.31.45.18 maka *IP address* tersebut memiliki *NetworkID* = 120 dan *HostID*=31.45.18

2. Jaringan IPv4 Kelas B

Jaringan Komputer yang memiliki 16,384 *network* dan 65,534 *host* untuk setiap *network*nya yang mencakup jaringan dengan skala menengah sampai besar, Jangkauan jaringan IPv4kelas B dimulai dari 128.0.xxx.xxx-191.255.xxx.xxx.



Gambar 11.6. IP Address Kelas B
Sumber : https://basobasri.wordpress.com/

Penerapan dalam Jaringan IPv4 kelas B dengan alamat sebagai berikut 150.70.60.56 maka *IP address* tersebut memiliki *NetworkID* = 150.70 dan *HostID*=60.56

3. Jaringan IPv4 Kelas C

Jaringan komputer yang memiliki 2,097,152 *network* dan 254 *host* untuk setiap *network*nya, jaringan IPv4 Kelas C skala kecil atau jaringan komputer *Local Area Network(LAN).* Jaringan IPv4 kelas C mulai dari 192.0.0.xxx-255.255.255.xxx.

Format : 110NNNNN.NNNNNNNN. NNNNNNNN.HHHHHHHH

Keterangan :

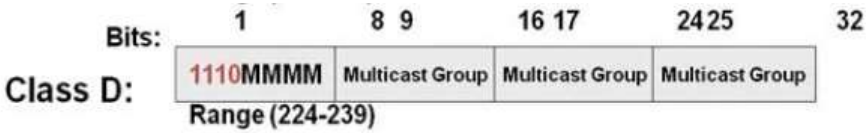
- Nilai 110 untuk bit pertama, Nilai 26 bit untuk NetworkID dan Nilai 8 bit selanjutnya untuk HostID
- Oktat pertama : 192 – 223
- Jumlah network : 2.097.152
- Rentang IP : 192.0.0.x – 223.255.225.x
- Jumlah IP address : 254

Gambar 11.7. IP Address Kelas C
Sumber : https://basobasri.wordpress.com/

Penerapan dalam Jaringan IPv4 kelas C dengan alamat sebagai berikut 192.168.1.1 maka *IP address* tersebut memiliki *NetworkID* = 192.168.1 dan *HostID*=1

4. Jaringan IPv4 Kelas D

Jaringan komputer digunakan untuk multicast, memiliki 4 bit pertama pada bilangan biner oktet pertama bernilai 1110 sebagai *NetworkID* dan 28 bit sebagai *HostID*. Jaringan IPv4 kelas D mulai dari 224.0.0.0-239.255.255.255.



Gambar 11.8. IP Address Kelas D
Sumber : https://basobasri.wordpress.com/

5. Jaringan IPv4 Kelas E

Jaringan komputer untuk eksperimen yang memiliki 4 bit pertama pada bilangan biner oktet pertama dengan nilai 1111 sebagai *NetworkID* dan 28 bit untuk *HostID*. Jaringan IPv4 kelas E mulai dari 240.0.0.0-254.255.255.255.

Kelas	Oktet pertama dalam desimal	Oktet pertama dalam biner	Jumlah jaringan	Jumlah Host Jaringan	Penggunaan
Kelas A	1 - 126	0xxx xxxx	128	16.777.216	Jaringan komputer berskala besar
Kelas B	128–191	10xx xxxx	16.384	1.048.576	Jaringan komputer berskala menengah sampai besar
Kelas C	192–223	110x xxxx	65.534	2.097.152	Jaringan komputer berskala kecil
Kelas D	224–239	1110 xxxx	Tidak didefinisikan	Tidak didefinisikan	Alamat multicast
Kelas E	240–255	1111 xxxx	Tidak didefinisikan	Tidak didefinisikan	Alamat percobaan atau eksperimen

Gambar 11.9. IP Address Kelas A, B, C, D Dan E
Sumber : https://www.diaryconfig.com/

IP Address dikhususkan tidak digunakan secara umum antara lain:

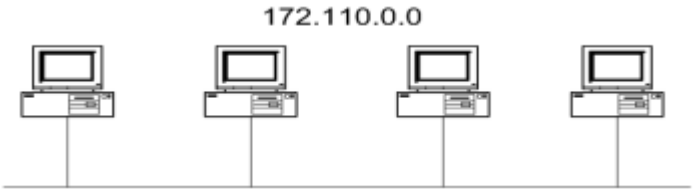
1. Jaringan *IP Address* untuk menunjukkan *Host* digunakan 0.0.0.0.
2. Jaringan *IP Address* yang menunjukkan *broadcast* suatu jaringan digunakan 255.255.255.255.
3. Alamat 127.0.0.1 digunakan untuk *host (lookback).*
4. Jaringan *IP Address* untuk multicasting digunakan 224.0.0.0–239.255.255.255.
5. Untuk *IP Address* yang dicadangkan digunakan 240.0.0.0–247.255.255.255.
6. Untuk alamat *Host* tidak diperbolehkan dengan nilai 0 semua atau nilai 1 semua bit dengan nilai 0 semua akan menunjuk kepada alamat *broadcast.*

11.3 Subnetting IPv4

Proses menentukan atau membagi berapa banyak jumlah *host* dalam sebuah jaringan menjadi beberapa *network* yang lebih kecil untuk lebih efisien dengan batasan *host* yang realistis sesuai kebutuhan. *IP Address* Kelas A yang menyediakan ukuran 8 bit, kelas B dengan ukuran 16 bit, dan C dengan ukuran 24 bit yang sudah yang mewakili *network ID* dan *hostID.*

Fungsi *Subnetting* antar lain :

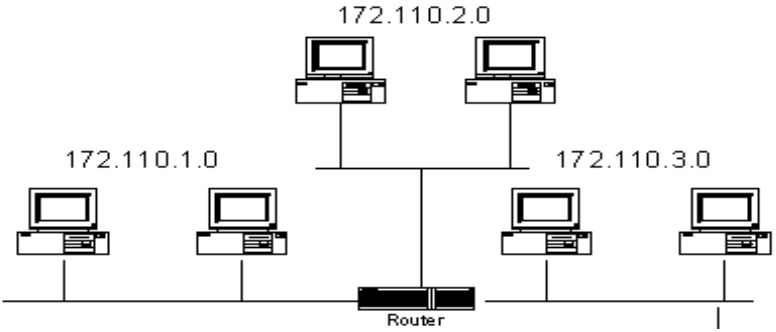
1. Penghematan Alamat IP dan Mereduksi *traffic* jaringan
   IP Address dalam sebuah jaringan akan membagi-bagi alamat IP untuk mengurangi beban *host* secara optimal guna memaksimalkan penggunaan *IP Address* agar alokasi *IP address* lebih efisien.
2. Mengoptimalisasi Jaringan
   Untuk meningkatkan optimalisai jaringan untuk lingkungan tertentu maka pembagian subnetting harus sesuai dengan prosedur yang sistimatik.
3. Memudahkan manajemen Jaringan
   Dengan *subnetting* dapat mempermudah manajemen jaringan sehingga akan menambah efisiensi kinerja suatu jaringan tersebut dan membatasi jumlah *host* yang terhubung dalam suatu subnet.



Gambar 11.10. Jaringan Tunggal
Sumber : https://romisatriawahono.net/

Dengan *subnetting* untuk membagi jaringan besar menjadi bagian yang lebih kecil dengan istilah ***s**ubnetworks* atau subnet

untuk lebih fleksibilitas *addressing* dalam sebuah jaringan seperti berikut :



Gambar 11.11. Proses subnetting dalam Jaringan
Sumber : https://romisatriawahono.net/

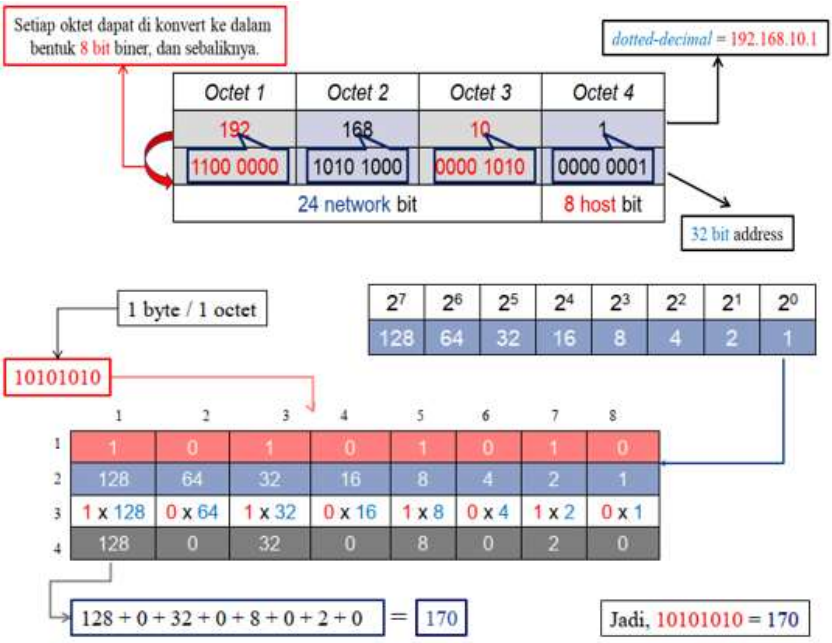
Dalam mengirim paket data melalui *router* dalam jaringan non lokal maka TCP/IP berfungsi dalam *subnet mask* yang memisahkan antara *networkID* dengan *hostID*. *Subnetting* merupakan cara penulisan notasi angka sebuah *sub network* dari nilai berupa angka desimal ke dalam nilai berupa angka biner menghitung jumlah angka biner bernilai 1 yang ada disebut sebagai *CIDR (Classless Inter Domain Routing).*

Dotted Decimal Subnet Mask	Binary Subnet Mask	Slash Notation
255.0.0.0	11111111.00000000.00000000.00000000	/8
255.128.0.0	11111111.10000000.00000000.00000000	/9
255.192.0.0	11111111.11000000.00000000.00000000	/10
255.224.0.0	11111111.11100000.00000000.00000000	/11
255.240.0.0	11111111.11110000.00000000.00000000	/12
255.248.0.0	11111111.11111000.00000000.00000000	/13
255.252.0.0	11111111.11111100.00000000.00000000	/14
255.254.0.0	11111111.11111110.00000000.00000000	/15
255.255.0.0	11111111.11111111.00000000.00000000	/16
255.255.128.0	11111111.11111111.10000000.00000000	/17
255.255.192.0	11111111.11111111.11000000.00000000	/18
255.255.224.0	11111111.11111111.11100000.00000000	/19
255.255.240.0	11111111.11111111.11110000.00000000	/20
255.255.248.0	11111111.11111111.11111000.00000000	/21
255.255.252.0	11111111.11111111.11111100.00000000	/22
255.255.254.0	11111111.11111111.11111110.00000000	/23
255.255.255.0	11111111.11111111.11111111.00000000	/24
255.255.255.128	11111111.11111111.11111111.10000000	/25
255.255.255.192	11111111.11111111.11111111.11000000	/26
255.255.255.224	11111111.11111111.11111111.11100000	/27
255.255.255.240	11111111.11111111.11111111.11110000	/28
255.255.255.248	11111111.11111111.11111111.11111000	/29
255.255.255.252	11111111.11111111.11111111.11111100	/30

Gambar 11.12. Subnet Mask dan Nilai CIDR
Sumber : https://www.sistemit.com/

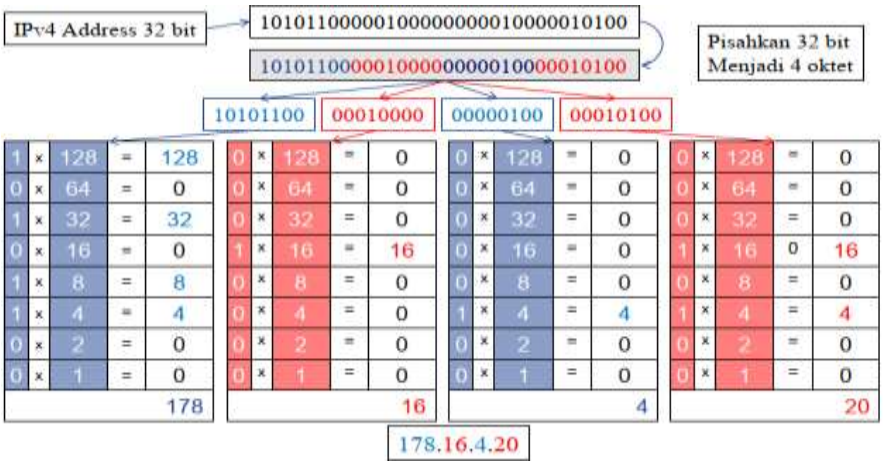
11.4 Format Alamat IPv4

Struktur *IP address* terdiri dari bilangan biner sebesar 32 dalam ukuran bit yang terbagi dua bagian antara lain bagian *networkID* dan *HostID. NetworkID* atau *network address* menunjukkan suatu identitas letak *network* atau jaringan dari *IP Address* dalam jaringan komputer dan merupakan tempat *host* berada. *HostID* digunakan untuk menunjukkan suatu *host* dalam sebuah jaringan dan memiliki nomor ID yang berbeda satu dengan lainya dengan ukuran 8 bit terakhir dari alamat *IP Address* digunakan menyimpan informasi tentang komputer yang terhubung dengan jaringan. *NetworkID* dan *hostID* dapat lihat dalam gambar dengan bentuk sebagai berikut :



Gambar 11.13. Struktur *IP Address* dalam bilangan biner
Sumber : https://citraweb.com/

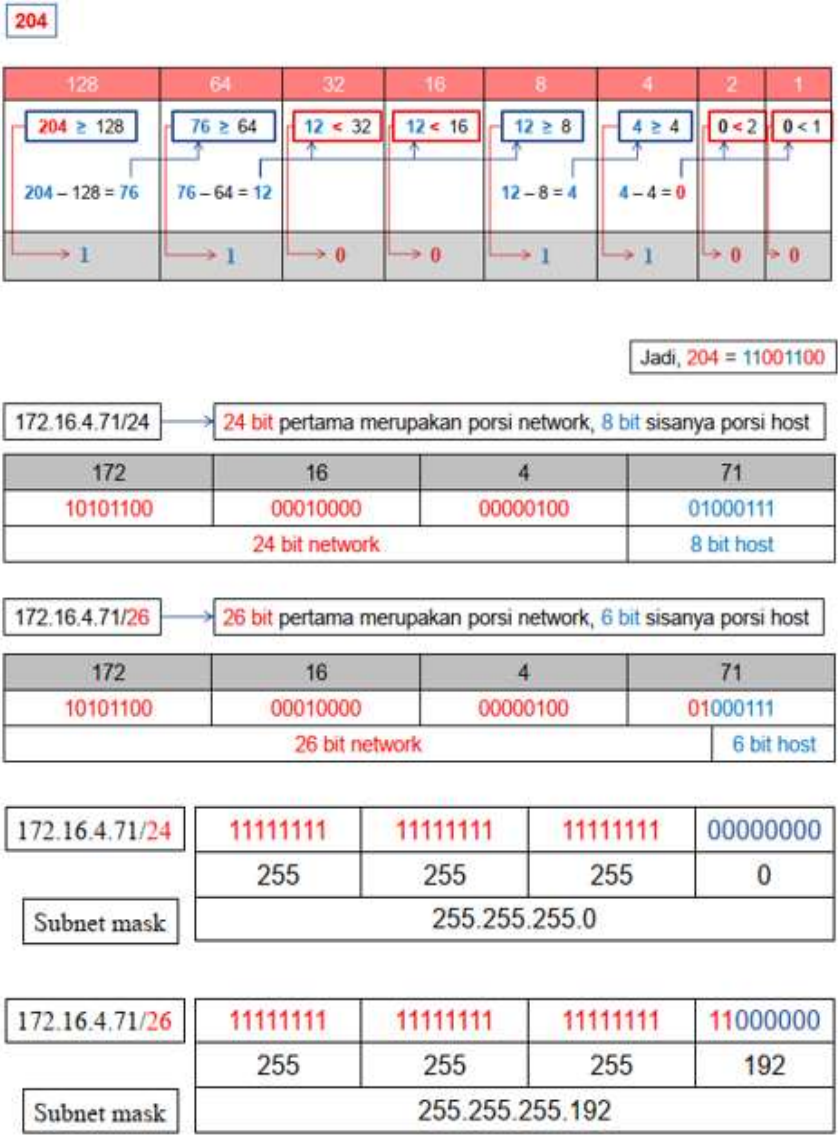
Contoh :
10101100.00010000.00000100.00010100
Struktur *IP address* tersebut berjumlah 32 bit dan terdiri dari 4 buah segmen, setiap segmen berukuran 8 bit disebut dengan oktat, untuk setiap nilai oktat dapat dikonvesi ke angka decimal seperti berikut :



Gambar : 11.14. Perhitungan IP4
Sumber : https://citraweb.com/

Jadi untuk
10101100=178
00010000=16
00000100=4
00010100=20

Mengubah angka decimal menjadi angka biner dengan mengunakan sistem modulus atau sisa bagi yaitu nilai 0 atau 1 seperti dalam tabel berikut:



Gambar 11.15. Format IP4 merubah angka biner ke decimal
Sumber : https://citraweb.com/

11.5 Pengalamatan IPv4

Pengalamatan Ipv4 terdiri dari *Public IP* yang merupakan alamat IP dalam jaringan *global* atau *internet* yang dapat diakses langsung melalui internet dan dikirim ke *router* dalam jaringan oleh *Internet Service Provider* (ISP). *Private IP* hanya akan menghubungkan beberapa perangkat yang terhubung ke sebuah jaringan yang sama atau jaringan lokal (*Local Area Network*) yang berkomunikasi sama lainya tanpa terhubung ke *internet*

Konfigurasi pengalamatan Ipv4 terbagi menjadi 2 yaitu *IP Dynamic* dan *IP Static* berdasarkan bagaimana cara memperolehnya dari *provider internet* atau ISP. *Protokol Internet Dinamis (Dynamic IP)* merupakan alamat sementara yang berubah saat diberikan ke *Host* yang terhubung dengan Internet. *Static IP* adalah IP yang tidak akan berubah yang digunakan oleh sebuah server dalam jaringan lokal *(Local Area Network).*

Spesifikasi IPv4 sebagai berikut :

1. Ukuran alamat IP
   berukuran 32 Bit
2. Metode *IP Address*
   Dalam pengalamatan digunakan nomor numerik, setiap anggka bit dipisah dengan titik.
3. Jumlah kolom *header*
   Jumlah kolom *Header* dalam IPv4 sebanyak 12 kolom *header.*
4. Kemampuan *broadcast*
   Kemampuan IP4 mendukung *broadcast.*
5. Konfigurasi jaringan
   Dalam konfigurasi jaringan dapat dilakukan dengan menetapkan alamat IP secara static atau manual dan dinamis (DHCP).

6. Dukungan *Variable Length Subnet Mask (VLSM)*
   Dapat dikonfigurasikan dengan *Variable Length Subnet Mask (VLSM)*
7. *Media access control address(MAC Address) mapping*
   Penggunaan *Address Resolution Protocol (ARP)* dalam *mapping* jaringan ke *Media access control address(MAC Address).*

Protokol IP4 dengan total 32 bit yang digunakan protokol jaringan TCP/IP dalam pengalamatan sebuah jaringan yang dapat digunakan sebanyak 4.294.967.296 *host* jumlah keseluruhan 255x255x255x255.

DAFTAR PUSTAKA

Forouzan. 2010. *TCP/IP Protocol Suite*. 4th edn. New York: McGraw-Hill.

Forouzan. 2013. *Data Communication and Networking*. 5th edn. New York: McGraw-Hill.

BAB 12
INTERNET CONTROL MESSAGE PROTOCOL (ICMP)

Oleh Adi Heri

12.1 Pengantar Protokol Internet

12.1.1 Munculnya ARPANET dan Protokol Internet

Munculnya ARPANET ditandai dengan perkembangan proyek yang bertujuan untuk menghubungkan komputer-komputer di berbagai lokasi geografis pada tahun 1960-an. Salah satu tonggak awal dalam pengembangan jaringan komputer adalah proyek ARPANET (*Advanced Research Projects Agency Network*) yang dimulai oleh Departemen Pertahanan Amerika Serikat. ARPANET dibangun oleh *Advanced Research Projects Agency* (ARPA) dengan tujuan untuk menciptakan jaringan komputer yang kuat dan tahan bencana. Proyek ini dimulai pada tahun 1969 dan melibatkan kerjasama antara beberapa universitas dan institusi penelitian terkemuka di Amerika Serikat. ARPANET menjadi cikal bakal dari apa yang sekarang kita kenal sebagai Internet.(Referensi : Roberts, L. G., & Walden, D. C. (1972). The ARPANET after twenty years. IEEE Transactions on Communications, 20(1), 3-9.)

ARPANET merupakan jaringan komputer pertama yang menggunakan paket data sebagai unit pengiriman informasi. Jaringan ini memanfaatkan teknologi switching paket dan memungkinkan komputer-komputer yang terhubung untuk berbagi sumber daya dan berkomunikasi satu sama lain secara efisien.

Perkembangan ARPANET menjadi sebuah jaringan yang lebih besar dan kompleks membutuhkan pengembangan berbagai

protokol dan standar. Pada tahun 1972, protokol NCP (*Network Control Program*) digantikan oleh protokol TCP/IP (*Transmission Control Protocol/Internet Protocol*) sebagai protokol yang lebih fleksibel dan dapat digunakan di berbagai jaringan komputer. ARPANET kemudian menjadi bagian dari jaringan yang lebih luas yang dikenal sebagai Internet.

Protokol Internet, juga dikenal sebagai TCP/IP (*Transmission Control Protocol/Internet Protocol*), adalah serangkaian protokol yang digunakan untuk mengatur komunikasi data dalam jaringan komputer. Protokol ini menjadi dasar dari Internet dan memungkinkan berbagai perangkat komputer untuk saling berkomunikasi dan bertukar informasi di seluruh dunia.(Referensi : RFC 791: Internet Protocol https://tools.ietf.org/html/rfc791)

TCP/IP terdiri dari dua protokol utama, yaitu TCP (*Transmission Control Protocol*) dan IP (*Internet Protocol*). TCP bertanggung jawab atas pengaturan koneksi dan pengiriman data yang handal antara perangkat, sementara IP menangani routing dan pengalamatan jaringan. (Referensi: RFC 791: Internet Protocol https://tools.ietf.org/html/rfc791)

Dalam komunikasi menggunakan protokol TCP/IP, data dikemas menjadi paket-paket kecil yang dikirim melalui jaringan. Setiap paket memiliki alamat tujuan dan asal, dan paket-paket ini dikirim secara terpisah dan dapat mengikuti jalur yang berbeda menuju tujuan mereka. Protokol IP bertanggung jawab atas pengiriman paket-paket tersebut ke tujuan yang tepat, dengan menggunakan alamat IP untuk identifikasi tujuan dan routing.(Referensi: Comer, D. E. (2014). Internetworking with TCP/IP: Principles, Protocols, and Architecture (6th Edition). Pearson Education)

Protokol TCP beroperasi di lapisan transport, yang bertanggung jawab atas pengiriman data yang handal dan dalam urutan yang benar antara perangkat-perangkat di jaringan. TCP

menggunakan mekanisme pengiriman yang handal dan pengontrolan aliran untuk memastikan bahwa data yang dikirimkan tiba di tujuan dengan akurasi dan keutuhan yang tinggi.(Refernsi: Kurose, J. F., & Ross, K. W. (2017). Computer Networking: A Top-Down Approach (7th Edition). Pearson Education).

121.2 Perkembangan Protokol IP

Perkembangan Protokol Internet Protocol (IP) telah mengalami beberapa tahapan signifikan sejak pertama kali diperkenalkan.

IP Version 4 (IPv4): IP versi 4 (IPv4) adalah versi awal dari Protokol IP yang pertama kali diperkenalkan pada tahun 1981. IPv4 menggunakan format alamat 32-bit (dalam bentuk notasi desimal berbasis titik) dan mendukung sekitar 4,3 miliar alamat IP unik. Pada awalnya, ini dianggap sebagai jumlah yang cukup, namun dengan pertumbuhan pesat Internet, jumlah alamat IPv4 menjadi terbatas.(Referensi: RFC 791: Internet Protocol (https://tools.ietf.org/html/rfc791))

Kehabisan Alamat IPv4: Pertumbuhan pesat Internet dan penggunaan alamat IP yang semakin meningkat mengakibatkan kekurangan alamat IPv4. Untuk mengatasi masalah ini, berbagai solusi ditemukan, seperti penggunaan alamat IP privat (private IP address) dan Network Address Translation (NAT), yang memungkinkan beberapa perangkat menggunakan satu alamat IP publik.(Referensi: RFC 1631: The IP Network Address Translator (NAT) (https://tools.ietf.org/html/rfc1631))

IP Version 6 (IPv6): IPv6 adalah versi terbaru dari Protokol IP yang diperkenalkan untuk mengatasi kekurangan alamat IPv4. IPv6 menggunakan format alamat 128-bit (dalam notasi heksadesimal) dan mampu mendukung sejumlah alamat yang sangat besar, yaitu sekitar 3,4 x 10^38 alamat IP. IPv6 juga memiliki fitur-fitur baru seperti otentikasi, integritas pesan, dan

dukungan untuk aliran data multimedia. (Referensi: RFC 2460: Internet Protocol, Version 6 (IPv6) Specification (https://tools.ietf.org/html/rfc2460))

Migrasi ke IPv6: Seiring dengan kekurangan alamat IPv4, terjadi pergeseran menuju adopsi IPv6. Organisasi dan penyedia layanan internet (ISP) secara bertahap mengadopsi IPv6 dan melakukan migrasi dari IPv4 ke IPv6. Migrasi ini melibatkan pengembangan infrastruktur jaringan yang mendukung IPv6 dan konfigurasi perangkat dengan alamat IPv6. (Referensi:RFC 5211: An Internet Transition Plan (https://tools.ietf.org/html/rfc5211))

Dual Stack dan Tunnelling: Selama masa transisi dari IPv4 ke IPv6, pendekatan dual stack dan tunnelling digunakan. Dual stack mengacu pada kemampuan perangkat untuk mendukung IPv4 dan IPv6 secara bersamaan, sementara tunnelling melibatkan pembungkusan paket IPv6 di dalam paket IPv4 untuk mentransmisikannya melalui jaringan IPv4. (Referensi: RFC 4213: Basic Transition Mechanisms for IPv6 Hosts and Routers (https://tools.ietf.org/html/rfc4213))

Perkembangan dan Standar Tambahan: Seiring dengan evolusi teknologi dan kebutuhan jaringan yang terus berkembang, ada juga pengembangan dan standarisasi tambahan terkait dengan IPv6, seperti pengaturan otonom alamat IPv6 (*autonomous address configuration*) menggunakan IPv6 *Stateless Address Autoconfiguration* (SLAAC), pengamanan IPv6 dengan *Internet Protocol Security* (IPsec), dan lain-lain. (Referensi: RFC 4301: *Security Architecture for the Internet Protocol* (https://tools.ietf.org/html/rfc4301))

12.2 Protokol Internet Control Message Protocol (ICMP)

12.2.1 Membutuhkan ICMP dalam Protokol IP

Pengiriman paket data dalam jaringan komputer melibatkan sejumlah tantangan yang perlu diatasi untuk memastikan pengiriman yang efisien dan andal. Beberapa tantangan tersebut meliputi latensi, kehilangan paket, pengurutan yang salah, dan kegagalan koneksi. Dalam hal ini, berikut adalah penjelasan lebih rinci mengenai tantangan pengiriman paket dalam jaringan:

1. Latensi: Latensi adalah waktu yang dibutuhkan oleh paket data untuk melakukan perjalanan dari sumber ke tujuan melalui jaringan. Latensi dapat dipengaruhi oleh beberapa faktor, seperti jarak fisik antara sumber dan tujuan, kepadatan lalu lintas jaringan, dan kinerja perangkat jaringan. Latensi yang tinggi dapat mengakibatkan waktu respon yang lambat dan kinerja jaringan yang buruk. (Referensi: Leland, E., & Asoni, D. (2019). The Role of Latency in Network Performance. In IEEE *Global Communications Conference* (GLOBECOM) (pp. 1-6). IEEE.))
2. Kehilangan Paket: Dalam perjalanan melalui jaringan, paket data dapat hilang karena berbagai alasan. Kehilangan paket dapat terjadi karena gangguan dalam saluran transmisi, konflik alamat IP, atau overloading pada perangkat jaringan. Kehilangan paket dapat mengganggu integritas data dan menyebabkan kerugian dalam aplikasi yang mengandalkan pengiriman data yang akurat. (Referensi: Tuan, L. A., & Vung, T. T. (2019). *Analysis of Packet Loss in IP Networks. In International Conference on Advanced Research in Computing, Electronics, and Communication* (ICARCEC) (pp. 169-173). Springer, Singapore.)

3. Pengurutan yang Salah: Dalam jaringan yang kompleks, paket data dapat mengalami keterlambatan dan tiba di tujuan dalam urutan yang salah. Hal ini dapat terjadi karena variasi dalam rute paket yang diambil atau perbedaan dalam latensi di berbagai bagian jaringan. Pengurutan yang salah dapat menyebabkan kerugian dalam protokol aplikasi yang mengharapkan data yang diurutkan dengan benar. (Referensi: Katti, S., & Anantharamu, S. (2019). *Packet Order Recovery Techniques in IP Networks. In International Conference on Advances in Computing and Data Sciences* (ICACDS) (pp. 498-507). Springer, Singapore.)
4. Kegagalan Koneksi: Jaringan komputer terdiri dari banyak perangkat yang terhubung, dan setiap perangkat memiliki potensi untuk mengalami kegagalan. Kegagalan koneksi dapat terjadi akibat kerusakan perangkat keras, gangguan listrik, kegagalan perangkat lunak, atau kesalahan konfigurasi. Kegagalan koneksi dapat mengakibatkan putusnya komunikasi antara sumber dan tujuan, yang menghambat pengiriman paket data. (Referensi: Sharma, S., Sharma, R., & Bansal, S. (2019). *A Review on Failure Detection and Recovery Mechanism in IP Networks. In International Conference on Communication, Computing and Electronics Systems* (ICCCES) (pp. 1-5). IEEE.)
5. Kesalahan dalam Pengiriman: Dalam pengiriman paket data, kesalahan dapat terjadi di berbagai tingkatan, mulai dari kesalahan bit hingga kesalahan pada lapisan protokol yang lebih tinggi. Kesalahan ini dapat disebabkan oleh interferensi sinyal, gangguan elektromagnetik, atau kondisi lingkungan yang tidak stabil. Kesalahan pengiriman dapat mengakibatkan kehilangan data, kerusakan file, atau informasi yang salah dalam aplikasi yang menggunakan data tersebut. (Referensi: Tripathi, D., & Vankar, V. D.

(2019). *Error Detection and Correction Techniques in IP Networks: A Review. In International Conference on Computing, Communication and Signal Processing* (ICCCSP) (pp. 1-5). IEEE.)

6. Penanganan Jaringan yang Tidak Stabil: Jaringan komputer dapat mengalami fluktuasi dalam kualitas dan keandalan koneksi. Faktor-faktor seperti kepadatan lalu lintas, konfigurasi jaringan yang tidak tepat, atau gangguan eksternal dapat menyebabkan ketidakstabilan jaringan. Hal ini dapat mengakibatkan penurunan kinerja, kehilangan paket, atau kesulitan dalam pengiriman data. (Referensi: Goyal, S., & Kaur, K. (2019). *Handling Network Instabilities in IP Networks: A Comprehensive Review. In International Conference on Artificial Intelligence and Data Engineering* (AIDE) (pp. 1-6). IEEE.)
7. Skalabilitas: Dalam jaringan yang semakin berkembang, skala dan kompleksitas jaringan dapat menjadi tantangan tersendiri. Pengiriman paket yang efisien dan andal harus tetap terjaga meskipun ada peningkatan jumlah pengguna, perangkat, dan lalu lintas data. Memastikan skalabilitas jaringan untuk mengatasi pertumbuhan yang cepat merupakan salah satu tantangan utama dalam pengiriman paket. (Referensi: Agrawal, S., & Gupta, V. (2019). *Scalability Issues and Solutions in IP Networks: A Survey. In International Conference on Computer Science and Engineering* (ICSE) (pp. 1-5). IEEE.)

Dalam menghadapi tantangan-tantangan ini, banyak teknologi dan protokol telah dikembangkan untuk meningkatkan kinerja dan keandalan pengiriman paket dalam jaringan. Referensi-referensi yang disebutkan di atas dapat memberikan informasi lebih lanjut tentang penelitian dan studi terkait tantangan

pengiriman paket dalam jaringan serta solusi yang telah diajukan dalam mengatasinya.

12.2.2 Pengembangan dan Standarisasi ICMP

Pengembangan ICMP dimulai bersama dengan pengembangan protokol Internet pada tahun 1970-an. Saat ini, standar dan spesifikasi ICMP didefinisikan dalam serangkaian dokumen RFC (*Request for Comments*) yang diterbitkan oleh *Internet Engineering Task Force* (IETF). Berikut ini adalah beberapa tahapan pengembangan dan standarisasi ICMP:

1. ICMPv4: ICMP versi 4 (ICMPv4) adalah versi awal dari protokol ICMP yang terintegrasi dengan IPv4. Spesifikasi ICMPv4 didefinisikan dalam RFC 792 dan mencakup pesan-pesan seperti *Echo Request*/*Reply* (digunakan dalam perintah ping), *Destination Unreachable, Time Exceeded, dan Redirect*. (Referensi: RFC 792: *Internet Control Message Protocol* (https://tools.ietf.org/html/rfc792))
2. ICMPv6: Dengan berkembangnya IPv6 sebagai pengganti IPv4, ICMPv6 diperkenalkan untuk digunakan bersama dengan IPv6. ICMPv6 menggantikan ICMPv4 dan menyediakan mekanisme yang diperlukan dalam jaringan IPv6, seperti *Neighbor Discovery Protocol* (NDP) dan Path MTU Discovery. (Referensi: RFC 4443: *Internet Control Message Protocol* (ICMPv6) *for the Internet Protocol Version* 6 (IPv6) (https://tools.ietf.org/html/rfc4443))
3. Standarisasi Lainnya: Selain spesifikasi ICMPv4 dan ICMPv6, ada juga standarisasi tambahan yang berkaitan dengan ICMP, seperti ICMP *Extensions for Multiprotocol Label Switching* (MPLS) (RFC 4950) yang mendukung penggunaan MPLS di dalam pesan ICMP, serta ICMP *Extensions for Multiprotocol Label Switching* (MPLS) *Echo Request/Reply* (RFC 4379) yang mendefinisikan penggunaan ICMP dalam MPLS. (Referensi:

RFC 4379: Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures (https://tools.ietf.org/html/rfc4379))

12.2.3 Struktur dan Format Pesan ICMP

Pesan ICMP (*Internet Control Message Protocol*) memiliki struktur dan format yang ditentukan untuk memfasilitasi pengiriman informasi kontrol dan laporan kesalahan dalam jaringan komputer. Struktur dan format ini mencakup beberapa bidang yang digunakan untuk mengidentifikasi jenis pesan, menghitung checksum, serta membawa data yang relevan. Berikut adalah penjelasan lengkap mengenai struktur dan format pesan ICMP beserta referensi yang relevan:

1. Tipe dan Kode Pesan: Setiap pesan ICMP memiliki tipe dan kode yang digunakan untuk mengidentifikasi jenis pesan yang dikirim. Tipe pesan menggambarkan kategori umum dari pesan tersebut, sedangkan kode pesan memberikan informasi lebih lanjut tentang spesifikasi pesan tersebut. (Referensi: RFC 792: *Internet Control Message Protocol* (ICMP))
2. Checksum: Checksum digunakan untuk memastikan integritas pesan ICMP. Bidang checksum dihitung dari seluruh pesan ICMP, termasuk tipe pesan, kode pesan, dan data yang dibawa pesan. Penerima pesan dapat menggunakan checksum ini untuk memverifikasi keabsahan pesan. (Refensi: Stevens, W. R., Wright, G. R., & Stevens, M. (1994). TCP/IP Illustrated, Volume 1: The Protocols. Addison-Wesley.)
3. Data Tambahan: Beberapa jenis pesan ICMP dapat membawa data tambahan yang relevan. Misalnya, pesan Echo Request/Reply (Ping) mengandung data yang dikirimkan oleh pengirim dan dikembalikan oleh penerima sebagai respons.(Refensi: Comer, D. E. (2000). Internetworking with TCP/IP, Volume 1: *Principles, Protocols, and Architecture. Prentice Hall*)

12.2.4 Jenis Pesan ICMP

ICMP (*Internet Control Message Protocol*) memiliki beberapa jenis pesan yang digunakan untuk berbagai tujuan dalam jaringan komputer. Setiap jenis pesan memiliki fungsi dan karakteristiknya sendiri. Berikut adalah beberapa jenis pesan ICMP yang umum digunakan beserta penjelasan singkat:

1. *Echo Request/Reply* (Ping): Pesan *Echo Request* digunakan untuk mengirimkan permintaan kepada tujuan untuk merespons dengan pesan Echo Reply. Ini sering digunakan untuk menguji ketersediaan dan responsivitas host atau jaringan.
2. *Destination Unreachable: Pesan Destination Unreachable* memberi tahu pengirim bahwa tujuan yang dituju tidak dapat dicapai. Ini dapat terjadi karena alamat tujuan tidak valid, rute tidak ada, atau firewall yang memblokir akses ke tujuan.
3. *Time Exceeded:* Pesan *Time Exceeded* memberi tahu pengirim bahwa batas waktu tertentu telah terlampaui saat paket melakukan perjalanan melalui jaringan. Ini biasanya terjadi ketika paket terjebak dalam loop tak terbatas atau ketika TTL (*Time-to-Live*) mencapai nilai nol.
4. Redirect: Pesan Redirect digunakan oleh router untuk memberi tahu host pengirim bahwa ada rute yang lebih baik untuk mencapai tujuan yang diinginkan. Ini membantu meningkatkan efisiensi pengiriman paket dalam jaringan.
5. *Source Quench*: Pesan *Source Quench* digunakan untuk memberi tahu host pengirim agar mengurangi laju pengiriman paket. Ini terjadi ketika jaringan atau tujuan yang dituju tidak dapat menangani laju paket yang tinggi.

12.3 Pesan Kesalahan ICMP

12.3.1 Destination Unreachable

Destination Unreachable adalah pesan ICMP yang dikirim oleh router atau host untuk menunjukkan bahwa suatu tujuan tidak dapat dijangkau. Ketika paket tidak dapat mencapai tujuan yang dimaksud, router atau host yang mengalami masalah tersebut menghasilkan pesan *Destination Unreachable* ICMP untuk memberi tahu pengirim tentang masalah yang terjadi. (Refernsi : RFC 792: *Internet Control Message Protocol* (https://tools.ietf.org/html/rfc792))

Pesan Destination Unreachable ICMP berisi informasi tentang alasan tujuan yang tidak dapat dijangkau. Pesan ini mencakup kode ICMP, yang mengindikasikan jenis spesifik tujuan yang tidak dapat dijangkau, dan tipe ICMP, yang mengidentifikasi jenis pesan secara keseluruhan sebagai pesan Destination Unreachable.

Beberapa kode ICMP umum untuk pesan Destination Unreachable meliputi:

1. *Network Unreachable*: Kode ini menunjukkan bahwa jaringan yang menghosting alamat IP tujuan tidak dapat dijangkau. Ini bisa disebabkan oleh rute jaringan yang salah dikonfigurasi atau kegagalan jaringan.
2. *Host Unreachable*: Kode ini menunjukkan bahwa host spesifik (alamat IP tujuan) tidak dapat dijangkau. Hal ini bisa terjadi karena host mati, tidak terhubung ke jaringan, atau router tidak memiliki rute yang valid ke host tersebut.
3. *Protocol Unreachable*: Kode ini menunjukkan bahwa protokol transportasi yang ditentukan untuk paket (misalnya, TCP, UDP) tidak didukung oleh host tujuan.
4. *Port Unreachable*: Kode ini digunakan ketika port tujuan pada host tidak tersedia atau ditutup. Biasanya terjadi ketika layanan atau aplikasi yang diminta tidak berjalan di host tujuan.

Fragmentation Needed and Don't Fragment was Set: Kode ini digunakan ketika ukuran paket melebihi unit transmisi maksimum (MTU) dari suatu link di sepanjang jalur. Ini menunjukkan bahwa paket perlu dipecah, tetapi flag "*Don't Fragment*" (DF) telah diatur, mencegah pelepasan paket. (Referrensi : RFC 1191: Path MTU *Discovery* (https://tools.ietf.org/html/rfc1191))

12.3.2 Time Exceeded

Pesan Destination Unreachable ICMP ini membantu administrator jaringan dan alat pemecahan masalah mengidentifikasi dan mendiagnosis masalah konektivitas. Dengan menganalisis pesan ICMP, mereka dapat menentukan penyebab tujuan yang tidak dapat dijangkau dan mengambil tindakan yang tepat untuk menyelesaikan masalah tersebut.

Pesan Time Exceeded adalah salah satu pesan kesalahan yang dikirim melalui protokol ICMP (Internet Control Message Protocol) dalam jaringan komputer. Pesan ini digunakan untuk memberi tahu pengirim bahwa paket yang dikirimnya telah melewati batas waktu tertentu atau melewati hop maksimum yang diizinkan dalam perutean jaringan.

Pesan Time Exceeded digunakan dalam dua situasi utama:

1. *Time-to-Live (*TTL) Expired: Ketika sebuah paket dikirim melalui jaringan, setiap router yang dilewati akan mengurangi nilai TTL dalam header IP. Jika nilai TTL mencapai nol sebelum paket mencapai tujuan, router tersebut akan mengirimkan pesan Time Exceeded ke pengirim asli untuk memberitahukan bahwa paket tersebut telah mengalami TTL habis.
2. *Fragment Reassembly Timeout*: Ketika sebuah paket IP dipecah menjadi fragmen-fragmen lebih kecil untuk pengiriman, masing-masing fragmen akan dikirim secara terpisah. Jika salah satu fragmen tidak sampai ke tujuan dalam waktu yang ditentukan, atau jika paket asli tidak dapat dirakit kembali dalam waktu yang ditentukan, router di sisi tujuan akan

mengirimkan pesan Time Exceeded ke pengirim asli untuk memberi tahu bahwa fragmen-fragmen tersebut tidak berhasil dirakit kembali.

3. Pesan *Time Exceeded* mengandung beberapa informasi penting, seperti alamat IP router terakhir yang melaporkan pesan *Time Exceeded*, serta beberapa byte pertama dari paket yang menyebabkan pesan ini. Informasi ini membantu dalam proses pemecahan masalah dan identifikasi penyebab terjadinya pesan *Time Exceeded*. (Refrensi Comer, D. E. (2014). *Internetworking with* TCP/IP: *Principles, Protocols, and Architecture* (6th Edition). *Pearson Education*.)

12.3.3 Parameter Problem

Parameter Problem adalah salah satu pesan kesalahan yang dikirim melalui protokol ICMP (Internet Control Message Protocol) dalam jaringan komputer. Pesan ini digunakan untuk memberi tahu pengirim bahwa ada masalah dengan parameter tertentu dalam header IP yang terkait dengan paket yang dikirim.

Pesan Parameter Problem dapat dikirim dalam dua situasi utama:

1. Pointer Error: Pesan Parameter Problem dengan tipe ini mengindikasikan bahwa terdapat kesalahan pada pointer dalam header IP. Pointer ini mengacu pada lokasi di dalam header IP dimana masalah parameter terjadi. Pesan ini membantu mengidentifikasi kesalahan spesifik dalam header IP.
2. Bad IP Header Length: Pesan Parameter Problem dengan tipe ini menunjukkan bahwa ada kesalahan pada panjang header IP. Hal ini bisa terjadi jika panjang header yang tercantum dalam paket tidak sesuai dengan panjang yang seharusnya. Pesan ini membantu dalam mendeteksi kesalahan dalam konstruksi paket.

Pesan Parameter Problem mengandung beberapa informasi penting, seperti alamat IP router terakhir yang melaporkan pesan Parameter Problem, serta beberapa byte pertama dari paket yang menyebabkan pesan ini. Informasi ini membantu dalam pemecahan masalah dan identifikasi penyebab terjadinya pesan Parameter Problem.

12.3.4 Redirect

Pesan Redirect adalah salah satu pesan yang dikirim melalui protokol ICMP (*Internet Control Message Protocol*) dalam jaringan komputer. Pesan ini digunakan oleh router untuk memberi tahu pengirim bahwa ada rute yang lebih efisien untuk mencapai tujuan yang diinginkan.(Refernsi : RFC 792: Internet Control Message Protocol (https://tools.ietf.org/html/rfc792))
Pesan Redirect digunakan dalam dua situasi utama:

1. *Redirect for Host*: Pesan *Redirect* untuk host digunakan ketika router mengetahui bahwa pengirim sedang mengirim paket ke tujuan yang dapat dicapai secara lebih efisien melalui router lain. Router tersebut akan mengirimkan pesan Redirect ke pengirim asli untuk memberitahukan bahwa ada rute yang lebih baik untuk mencapai tujuan tersebut.
2. *Redirect for Network*: Pesan Redirect untuk jaringan digunakan ketika router mengetahui bahwa pengirim sedang mengirim paket ke tujuan yang dapat dicapai secara lebih efisien melalui jaringan lokal atau subnet yang sama. Router akan mengirimkan pesan Redirect ke pengirim asli untuk memberitahukan bahwa pengiriman paket dapat dilakukan secara langsung ke tujuan melalui jaringan lokal, tanpa melalui router.

Pesan *Redirect* mengandung informasi tentang alamat IP tujuan yang harus diarahkan ulang, alamat IP router yang harus

digunakan sebagai pengganti, dan alamat IP host atau jaringan pengirim asli.

12.3.5 Source Quench

Pesan *Source Quench* adalah salah satu pesan yang dikirim melalui protokol ICMP (*Internet Control Message Protocol*) dalam jaringan komputer. Pesan ini digunakan untuk memberi tahu pengirim bahwa aliran data yang dikirimkan terlalu cepat sehingga menyebabkan kelebihan beban pada penerima atau router. (Referensi: RFC 792: *Internet Control Message Protocol* (https://tools.ietf.org/html/rfc792))

Pesan *Source Quench* digunakan dalam situasi ketika penerima atau router tidak mampu mengolah aliran data yang diterimanya dengan kecepatan yang sama dengan kecepatan pengiriman. Hal ini dapat mengakibatkan penumpukan paket di buffer penerima atau router, yang pada gilirannya dapat menyebabkan penurunan kinerja jaringan.

Ketika router atau penerima mengalami kondisi kelebihan beban, mereka dapat mengirimkan pesan Source Quench ke pengirim asli untuk memberi tahu bahwa pengiriman data perlu diperlambat agar jaringan dapat mengatasi beban yang ada. Pesan ini bertujuan untuk mengontrol laju pengiriman paket dari sumber agar sesuai dengan kemampuan penerima atau router.

Pesan *Source Quench* mengandung informasi penting, termasuk alamat IP tujuan yang memicu pesan ini dan alamat IP pengirim asli yang perlu memperlambat pengiriman data.

12.4 Pesan Informasi ICMP

12.4.1 Echo Request/Reply (Ping)

(*Internet Control Message Protocol*) *Echo Request*/*Reply*, yang juga dikenal sebagai "Ping," adalah pesan ICMP yang digunakan untuk menguji konektivitas jaringan antara dua host. Pesan ini dikirim oleh host pengirim (*Echo Request*) dan dijawab

oleh host penerima (*Echo Reply*). Berikut ini adalah informasi lebih rinci tentang pesan ICMP *Echo Request/Reply* (Ping):

1. Echo Request:
    a. Tipe ICMP: 8
    b. Kode ICMP: 0
    c. Deskripsi: Echo Request dikirim oleh host pengirim ke host penerima. Pesan ini berisi permintaan untuk mendapatkan respons (*reply*) dari host penerima. Echo Request biasanya digunakan untuk menguji apakah host penerima dapat dijangkau dalam jaringan.
2. Echo Reply:
    a. Tipe ICMP: 0
    b. Kode ICMP: 0
    c. Deskripsi: Echo Reply dikirim oleh host penerima sebagai respons terhadap Echo Request yang diterima. Pesan ini berisi balasan yang mengindikasikan bahwa host penerima dapat dijangkau dan berfungsi dengan baik. Echo Reply menyertakan isi dari Echo Request asli agar host pengirim dapat memverifikasi keterhubungan.

Ketika host pengirim mengirim Echo Request ke host penerima, ia mencatat waktu pengiriman. Ketika host penerima menerima Echo Request, ia menghasilkan Echo Reply dan mengirimkannya kembali ke host pengirim. Host pengirim kemudian mencatat waktu penerimaan Echo Reply tersebut. Dengan membandingkan waktu pengiriman dan penerimaan, host pengirim dapat menghitung *round-trip time* (RTT), yang merupakan waktu yang dibutuhkan untuk paket pergi dari host pengirim ke host penerima dan kembali.(Refrensi: RFC 1122: *Requirements for Internet Hosts—Communication Layers* (https://tools.ietf.org/html/rfc1122))

Pesan ICMP Echo Request/Reply (Ping) sangat berguna untuk:

1. Menguji ketersediaan dan keterhubungan host dalam jaringan.
2. Memeriksa kecepatan respons jaringan (RTT).
3. Mengidentifikasi masalah konektivitas dan latency (tunda) dalam jaringan.
4. Memeriksa keandalan jaringan dengan mengukur packet loss (kehilangan paket).

12.4.2 Address Mask Request/Reply

Address Mask Request/Reply adalah pesan ICMP (*Internet Control Message Protocol*) yang digunakan untuk mengambil informasi tentang subnet mask dari host atau router dalam jaringan. Pesan ini memungkinkan host untuk mempelajari masker subnet yang digunakan oleh host tujuan atau router untuk mengelompokkan alamat IP.

Berikut ini adalah informasi mengenai *Address Mask Request*/*Reply*:

1. Address Mask Request:
   a. Tipe ICMP: 17
   b. Kode ICMP: 0
   c. Deskripsi: *Address Mask Request* dikirim oleh host pengirim ke host tujuan atau router dalam jaringan. Pesan ini berisi permintaan untuk mendapatkan informasi tentang masker subnet yang digunakan oleh host tujuan atau router.(Refernsi: RFC 950: Internet Standard Subnetting Procedure (https://tools.ietf.org/html/rfc950))
2. Address Mask Reply:
   a. Tipe ICMP: 18
   b. Kode ICMP: 0
   c. Deskripsi: Address Mask Reply dikirim oleh host tujuan atau router sebagai respons terhadap Address Mask Request yang diterima. Pesan ini berisi informasi

tentang masker subnet yang digunakan oleh host tujuan atau router.(Refensi: RFC 1812: Requirements for IP Version 4 Routers (https://tools.ietf.org/html/rfc1812))

Pesan Address Mask Request/Reply berguna dalam beberapa skenario, seperti:

1. Konfigurasi otomatis alamat IP: Ketika host terhubung ke jaringan baru, host dapat mengirim Address Mask Request untuk mendapatkan informasi tentang masker subnet yang digunakan oleh router dalam jaringan tersebut. Dengan informasi tersebut, host dapat mengkonfigurasi alamat IP dengan benar untuk komunikasi di dalam subnet.
2. Perutean: Router dalam jaringan dapat menggunakan Address Mask Request/Reply untuk mengumpulkan informasi tentang masker subnet dari host di jaringan yang terhubung. Informasi ini dapat digunakan oleh router untuk melakukan perutean paket dengan benar.
3. Konfigurasi jaringan: Administrator jaringan dapat menggunakan *Address Mask Request*/*Reply* untuk memeriksa konfigurasi masker subnet yang digunakan oleh host dalam jaringan. Informasi ini dapat membantu dalam memverifikasi pengaturan subnet dan mengidentifikasi masalah konfigurasi yang mungkin terjadi.

12.4.3 *Router Solicitation*/*Advertisement*

Router Solicitation/*Advertisement* (RS/RA) adalah pesan-pesan yang digunakan dalam protokol IPv6 (*Internet Protocol version* 6) untuk melakukan konfigurasi otomatis jaringan dan menemukan router dalam jaringan. RS/RA memungkinkan host IPv6 untuk memperoleh alamat IPv6, informasi perutean, dan

parameter jaringan lainnya secara otomatis. Berikut ini adalah informasi tentang Router Solicitation/Advertisement:

1. Router Solicitation (RS):
   a. Tipe ICMPv6: 133
   b. Deskripsi: Host yang baru terhubung ke jaringan IPv6 dapat mengirim RS untuk mencari router dalam jaringan. RS dikirim dalam bentuk multicast ke alamat tujuan khusus yang disebut All-Routers multicast address. RS memberi tahu router bahwa host membutuhkan informasi perutean dan konfigurasi jaringan. (Refernsi: RFC 4861: Neighbor Discovery for IP version 6 (IPv6) (https://tools.ietf.org/html/rfc4861))
2. Router Advertisement (RA):
   a. Tipe ICMPv6: 134
   b. Deskripsi: Router dalam jaringan IPv6 mengirim RA secara periodik atau sebagai respons terhadap RS yang diterima. RA mengandung informasi konfigurasi jaringan seperti:
      1) Alamat IPv6 router
      2) Opsi perutean seperti default route
      3) Informasi prinsipal (*Prefix Information*) yang mencakup alamat jaringan dan prefix lengkap untuk konfigurasi otomatis alamat IPv6 pada host.
      4) Opsi lain seperti opsi MTU (Maximum Transmission Unit) dan opsi autentikasi.

Penggunaan RS/RA dalam jaringan IPv6 memiliki beberapa manfaat, antara lain:

1. Konfigurasi otomatis alamat: Host yang terhubung ke jaringan IPv6 secara otomatis mendapatkan alamat IPv6 dan informasi konfigurasi jaringan melalui RA yang dikirim oleh router. Hal ini memudahkan dan mempercepat konfigurasi alamat pada host.

2. Informasi perutean: RS/RA digunakan untuk memperoleh informasi perutean. Host dapat mempelajari rute default dan prefix lengkap dari RA yang dikirim oleh router. Ini memungkinkan host untuk melakukan perutean dengan benar dalam jaringan IPv6.
3. Pembaruan konfigurasi jaringan: Jika ada perubahan dalam konfigurasi jaringan, seperti penambahan atau penghapusan router, RA akan dikirim secara periodik oleh router. Host dapat mendeteksi perubahan ini dan memperbarui konfigurasi jaringan mereka sesuai.
4. Efisiensi jaringan: Dengan menggunakan RS/RA, konfigurasi jaringan dan informasi perutean dapat dikirim ke host secara otomatis. Hal ini mengurangi tugas manual dan memastikan efisiensi dalam jaringan IPv6.

12.4.4 Timestamp Request/Reply

Timestamp Request/*Reply* adalah pesan ICMP (*Internet Control Message Protocol*) yang digunakan untuk mengukur waktu atau sinkronisasi waktu antara host atau router dalam jaringan. Pesan ini memungkinkan host untuk meminta atau memberikan informasi timestamp (penanda waktu) kepada host lainnya. Berikut ini adalah informasi mengenai *Timestamp Request*/*Reply*:

1. Timestamp Request:
   a. Tipe ICMP: 13
   b. Kode ICMP: 0
   c. Deskripsi: Timestamp Request dikirim oleh host pengirim ke host tujuan atau router dalam jaringan. Pesan ini berisi permintaan untuk memperoleh informasi timestamp dari host tujuan atau router.

2. Timestamp Reply:
   a. Tipe ICMP: 14
   b. Kode ICMP: 0

c. Deskripsi: Timestamp Reply dikirim oleh host tujuan atau router sebagai respons terhadap Timestamp Request yang diterima. Pesan ini berisi informasi timestamp yang diberikan oleh host tujuan atau router.

Pesan Timestamp Request/Reply digunakan untuk beberapa tujuan, termasuk:

1. Sinkronisasi waktu: Host dapat menggunakan Timestamp Request untuk meminta informasi timestamp dari host tujuan atau router guna melakukan sinkronisasi waktu. Dengan menggunakan informasi timestamp tersebut, host dapat menyesuaikan waktu internalnya dengan waktu host tujuan.
2. Pengukuran RTT (*Round-Trip Time*): Host dapat menggunakan Timestamp Request untuk mengukur RTT atau waktu tempuh pulang-pergi. Host pengirim mencatat waktu saat mengirimkan Timestamp Request dan waktu saat menerima Timestamp Reply. Dengan membandingkan kedua timestamp tersebut, host dapat menghitung RTT dan mengukur *latency* (tunda) jaringan.
3. Diagnostik jaringan: Timestamp Request/Reply juga dapat digunakan untuk tujuan diagnostik jaringan. Dengan melihat perbedaan timestamp antara host pengirim dan host tujuan, administrator jaringan dapat mengidentifikasi masalah dalam sinkronisasi waktu antar-host atau masalah dalam jaringan yang mempengaruhi waktu.

Pesan *Timestamp Request*/*Reply* membantu dalam memastikan sinkronisasi waktu antara host atau router dalam jaringan, serta membantu dalam pemecahan masalah dan pengukuran kinerja jaringan.

12.5 ICMP dalam Pengelolaan Jaringan

12.5.1 Deteksi dan Pelaporan Kesalahan

Deteksi dan pelaporan kesalahan ICMP (*Internet Control Message Protocol*) merujuk pada proses identifikasi dan pelaporan masalah yang terkait dengan pesan ICMP yang diterima dalam jaringan. Ketika pesan ICMP mencerminkan kondisi atau kesalahan yang tidak diharapkan, host atau router dapat mendeteksi dan melaporkan masalah tersebut. Berikut adalah langkah-langkah umum dalam deteksi dan pelaporan kesalahan ICMP:

1. Menerima pesan ICMP: Host atau router menerima pesan ICMP yang dikirim oleh perangkat lain dalam jaringan. Pesan ICMP dapat berupa pesan kesalahan, permintaan, atau respons.
2. Menganalisis jenis dan kode: Host atau router menganalisis jenis dan kode ICMP dari pesan yang diterima. Jenis dan kode ini memberikan informasi tentang tujuan dan sifat pesan ICMP.
3. Memeriksa kondisi pesan ICMP: Host atau router memeriksa kondisi pesan ICMP untuk menentukan apakah ada kesalahan atau masalah yang perlu dilaporkan. Contohnya, jika jenis dan kode menunjukkan "Destination Unreachable" atau "Time Exceeded", itu bisa mengindikasikan masalah dalam mencapai tujuan atau batasan waktu yang terlampaui.
2. Mengumpulkan informasi: Jika ada kesalahan atau masalah yang terdeteksi, host atau router dapat mengumpulkan informasi tambahan yang relevan. Misalnya, host dapat mencatat alamat sumber dan tujuan, waktu terjadinya pesan ICMP, serta informasi terkait jaringan seperti alamat IP, port, atau protokol yang terlibat.
3. Pelaporan kesalahan: Setelah mengumpulkan informasi, host atau router dapat melaporkan kesalahan atau masalah tersebut. Pelaporan ini dapat dilakukan dengan berbagai

cara, termasuk pencatatan ke log sistem, pengiriman notifikasi atau alarm kepada administrator jaringan, atau penggunaan alat pemantauan jaringan yang secara otomatis mengidentifikasi dan melaporkan masalah.

4. Tindakan pemecahan masalah: Setelah melaporkan kesalahan, langkah-langkah pemecahan masalah dapat diambil untuk mengatasi masalah tersebut. Ini mungkin melibatkan inspeksi lebih lanjut terhadap jaringan, penyesuaian konfigurasi, perbaikan perangkat keras atau perangkat lunak, atau tindakan lain yang sesuai untuk mengatasi masalah yang terdeteksi.

Penting untuk memiliki sistem pemantauan jaringan yang baik dan prosedur pemecahan masalah yang efektif untuk mendeteksi dan melaporkan kesalahan ICMP dengan tepat. Hal ini membantu dalam menjaga kinerja dan keandalan jaringan, serta memungkinkan respons cepat terhadap masalah yang terdeteksi.

12.5.2 Penggunaan Utility Ping dan Traceroute

Penggunaan *utility Ping* dan *Traceroute* sangat berguna dalam memeriksa konektivitas dan melacak jalur paket dalam jaringan. Berikut ini adalah penjelasan tentang penggunaan kedua utilitas tersebut, beserta referensinya:

1. Ping:
    a. Ping adalah utilitas yang digunakan untuk menguji konektivitas ke host atau alamat IP tertentu dalam jaringan. (Referensi: RFC 792: Internet Control Message Protocol (https://tools.ietf.org/html/rfc792))
    b. Dengan mengirim pesan ICMP Echo Request ke host tujuan, Ping menunggu dan mencatat waktu yang dibutuhkan untuk menerima balasan ICMP Echo Reply.

c. Penggunaan Ping dapat membantu menguji apakah host tujuan dapat dicapai dan mengukur latensi (ping) antara host pengirim dan tujuan.

2. Traceroute:
   a. Traceroute adalah utilitas yang digunakan untuk melacak jalur yang dilalui oleh paket dari host pengirim ke tujuan.(Referensi: RFC 1393: Traceroute Using an IP Option (https://tools.ietf.org/html/rfc1393))
   b. Dengan mengirim serangkaian pesan ICMP dengan TTL (*Time-to-Live*) yang meningkat secara bertahap, Traceroute mencatat hop-hops (titik-titik antara router) yang dilewati oleh paket dan waktu yang dibutuhkan oleh masing-masing hop.
   c. Traceroute membantu mengidentifikasi jalur dan hop-hops yang dilewati paket, serta mengukur latensi di setiap hop.

12.5.3 Melacak Rute Paket dan Identifikasi Masalah

Melacak rute paket dan mengidentifikasi masalah dalam jaringan dapat membantu dalam pemecahan masalah dan pemeliharaan jaringan yang efektif. Berikut ini adalah beberapa metode yang dapat digunakan untuk melacak rute paket dan mengidentifikasi masalah

Traceroute adalah utilitas yang digunakan untuk melacak jalur yang dilalui oleh paket dari sumber ke tujuan. Ini membantu mengidentifikasi titik-titik yang dilewati paket dan menunjukkan waktu yang dibutuhkan oleh setiap hop. Traceroute menggunakan serangkaian pesan ICMP dengan TTL (*Time-to-Live*) yang bertambah secara bertahap untuk mendapatkan respons dari hop-hops di jalur.(Referensi: RFC 1393: Traceroute Using an IP Option (https://tools.ietf.org/html/rfc1393))

PathPing adalah utilitas yang menggabungkan fitur-fitur dari Ping dan Traceroute. Ini memberikan informasi tentang

kehilangan paket, latensi, dan jalur yang dilalui paket menuju tujuan. PathPing menggunakan serangkaian pesan ICMP dan menghitung statistik dari setiap hop yang dilewati.(Referensi: Microsoft Docs - PathPing (https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/pathping))

MTR (*My Traceroute*): MTR adalah utilitas yang menggabungkan fitur-fitur dari Ping dan Traceroute. Ini memberikan informasi tentang lalu lintas, latensi, dan kehilangan paket pada setiap hop di jalur. MTR secara terus-menerus memantau jalur dan memberikan output yang diperbarui secara real-time. (Referensi: MTR - Homepage (https://www.bitwizard.nl/mtr/))

Analisis Log Perutean (*Routing*): Menganalisis log perutean pada perangkat jaringan, seperti router, dapat memberikan wawasan tentang perutean yang sedang berlangsung dan masalah yang mungkin terjadi. Log perutean berisi informasi tentang rute yang dipilih, perubahan perutean, dan pesan-pesan kesalahan terkait perutean.(Referensi: Cisco - Troubleshooting Routing (https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13714-40.html))

12.6 Keamanan dan Ancaman Terkait ICMP

12.6.1 Ancaman DDoS menggunakan ICMP

Ancaman DDoS (*Distributed Denial of Service*) menggunakan ICMP (*Internet Control Message Protocol*) dapat menjadi masalah serius dalam jaringan. Berikut ini adalah beberapa bentuk ancaman DDoS yang menggunakan ICMP:

1. ICMP Flood: Serangan DDoS jenis ini melibatkan pengiriman sejumlah besar pesan ICMP ke target dalam waktu singkat. Pesan ICMP yang dikirim bisa berupa ICMP Echo Request (Ping) atau pesan ICMP lainnya. Dengan membanjiri target dengan lalu lintas ICMP, sumber daya

jaringan target dapat terbebani, mengakibatkan penurunan kinerja atau kegagalan akses bagi pengguna yang sah. (Referensi: RFC 4950: ICMP Extensions for Multiprotocol Label Switching (https://tools.ietf.org/html/rfc4950))

2. Smurf Attack: Serangan DDoS Smurf memanfaatkan karakteristik protokol ICMP dan IP. Serangan ini melibatkan pengiriman pesan ICMP Echo Request dengan alamat sumber yang dipalsukan (*spoofed*) ke jaringan yang menggunakan broadcast IP. Setiap host dalam jaringan kemudian membalas pesan ICMP tersebut ke alamat sumber palsu, yang menyebabkan target banjir dengan lalu lintas ICMP yang besar dan membuatnya menjadi tidak responsif. (Referensi: CERT Advisory CA-1998-01: Smurf IP *Denial-of-Service Attacks* (https://www.cert.org/historical/advisories/CA-1998-01.cfm))
3. Ping of Death: Serangan Ping of Death melibatkan pengiriman pesan ICMP Echo Request yang dimanipulasi dengan ukuran yang sangat besar melebihi batasan yang diizinkan. Pesan ICMP yang terlalu besar ini dapat menyebabkan kerentanan dalam implementasi protokol di host target, menyebabkan kegagalan atau kerusakan pada sistem tersebut. (Referensi: CERT Advisory CA-1996-21: Teardrop IP Denial-of-Service Attack (https://www.cert.org/historical/advisories/CA-1996-21.cfm))
4. ICMP Redirect Attack: Serangan ini melibatkan pengiriman pesan ICMP *Redirect* yang dipalsukan ke host dalam jaringan. Pesan ICMP Redirect yang palsu akan memberitahu host untuk mengirim paket ke alamat gateway yang tidak benar, sehingga mengarahkan lalu lintas ke alamat yang tidak valid atau tidak ada. Hal ini dapat mengganggu konektivitas dan mengganggu aliran lalu lintas normal dalam jaringan. (Referensi: CERT Advisory CA-1998-12: ICMP Redirect Attack

(https://www.cert.org/historical/advisories/CA-1998-12.cfm))

12.6.2 Proteksi terhadap Serangan ICMP

Proteksi terhadap serangan ICMP (*Internet Control Message Protocol*) yang berpotensi merugikan dapat dilakukan dengan menerapkan langkah-langkah keamanan yang tepat. Berikut ini adalah beberapa langkah proteksi yang dapat Anda terapkan:

1. Filter Lalu lintas ICMP: Gunakan firewall atau perangkat keamanan jaringan untuk membatasi atau memblokir lalu lintas ICMP yang tidak diperlukan atau berlebihan. Ini dapat melindungi jaringan Anda dari serangan ICMP yang berpotensi merusak. (Referensi: RFC 4890: Recommendations for Filtering ICMPv6 Messages in Firewalls (https://tools.ietf.org/html/rfc4890))
2. Rate Limiting: Terapkan pembatasan tingkat (rate limiting) pada lalu lintas ICMP yang masuk. Dengan membatasi jumlah pesan ICMP yang diterima dalam waktu tertentu, Anda dapat membatasi dampak serangan yang berlebihan atau banjir pesan ICMP. (Referensi: RFC 8085: UDP Usage Guidelines (https://tools.ietf.org/html/rfc8085))
3. Penerapan Access Control List (ACL): Gunakan Access Control List (ACL) pada perangkat jaringan, seperti router atau switch, untuk memfilter atau membatasi lalu lintas ICMP yang diperbolehkan ke atau dari jaringan Anda. Ini memungkinkan Anda untuk mengontrol dengan lebih detail aliran lalu lintas ICMP dan melindungi jaringan dari serangan yang mungkin terjadi. (Referensi: RFC 8273: Unique IPv6 Prefix per Host (https://tools.ietf.org/html/rfc8273))
4. Deteksi dan Mitigasi Serangan DDoS: Implementasikan solusi deteksi serangan DDoS yang dapat memantau dan mendeteksi aktivitas mencurigakan, termasuk serangan yang melibatkan lalu lintas ICMP. Dengan mendeteksi serangan dengan cepat,

Anda dapat mengambil tindakan responsif untuk melindungi jaringan. (Referensi: RFC 4732: Internet Denial-of-Service Considerations (https://tools.ietf.org/html/rfc4732))

5. Segmenasi Jaringan: Melakukan segmentasi jaringan dengan menggunakan VLAN atau jaringan yang terisolasi secara fisik dapat membantu membatasi dampak serangan ICMP. Dengan membagi jaringan menjadi segmen yang terpisah, serangan yang terjadi pada satu segmen tidak akan secara langsung mempengaruhi segmen lainnya. (Referensi: RFC 4038: *Application Aspects of* IPv6 Transition (https://tools.ietf.org/html/rfc4038))

12.7 Implementasi ICMP dalam Jaringan IPv6

12.7.1 ICMPv6 dan Perubahan dari ICMPv4

ICMPv6 (*Internet Control Message Protocol version* 6) adalah versi protokol ICMP yang dikembangkan khusus untuk digunakan dalam jaringan berbasis IPv6 (*Internet Protocol version* 6). Berikut ini adalah beberapa perubahan penting dari ICMPv4 ke ICMPv6, beserta referensinya:

1. Alamat IP: ICMPv4 menggunakan alamat IPv4 dalam header IP, sedangkan ICMPv6 menggunakan alamat IPv6 dalam header IP versi 6. Hal ini memungkinkan penggunaan ICMPv6 dalam jaringan yang menggunakan protokol IPv6. (Referensi: RFC 2460: Internet Protocol, Version 6 (IPv6) *Specification* (https://tools.ietf.org/html/rfc2460))
2. Header ICMP: Struktur header ICMPv6 berbeda dari ICMPv4. ICMPv6 memiliki format header yang lebih sederhana dan tetap, dengan panjang yang konsisten untuk setiap jenis pesan ICMP. (Referensi: RFC 4443: *Internet Control Message Protocol* (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification (https://tools.ietf.org/html/rfc4443))
3. Penggantian ICMP Redirect: Dalam ICMPv4, pesan ICMP Redirect digunakan untuk memberitahu host pengirim agar

mengirim paket ke alamat gateway yang berbeda. Namun, dalam ICMPv6, pesan ICMP Redirect telah dihapus, dan pengalihan rute ditangani oleh protokol perutean khusus seperti NDP (*Neighbor Discovery Protocol*). (Referensi: RFC 4861: Neighbor Discovery for IP version 6 (IPv6) (https://tools.ietf.org/html/rfc4861))

4. *Neighbor Discovery Protocol* (NDP): ICMPv6 terkait erat dengan NDP, yang digunakan untuk mencapai tujuan yang sama dengan ICMPv4 dalam hal menemukan tetangga dalam jaringan, mengelola tabel cache ARP (Address Resolution Protocol), dan melakukan konfigurasi otomatis alamat IPv6.
5. *Stateless Address Autoconfiguration* (SLAAC): ICMPv6 mendukung SLAAC, yang memungkinkan host untuk mengonfigurasi otomatis alamat IPv6 mereka berdasarkan informasi yang diterima melalui pesan ICMPv6 Router Advertisement (RA). (Referensi: RFC 4862: IPv6 Stateless Address Autoconfiguration (https://tools.ietf.org/html/rfc4862))

12.7.2 Penggunaan ICMPv6 dalam Pengalamatan dan Konfigurasi

Penggunaan ICMPv6 (*Internet Control Message Protocol version* 6) dalam pengalamatan dan konfigurasi dalam jaringan IPv6 memiliki beberapa aspek penting. Berikut ini adalah penggunaan utama ICMPv6 dalam pengalamatan dan konfigurasi.

1. Autoconfiguration (Auto konfigurasi): ICMPv6 berperan dalam konfigurasi otomatis alamat IPv6 pada host dalam jaringan. Pesan ICMPv6 Router Advertisement (RA) dan ICMPv6 Neighbor Solicitation (NS) digunakan dalam proses Stateless Address Autoconfiguration (SLAAC). RFC 4861: Neighbor Discovery for IP version 6 (IPv6) (https://tools.ietf.org/html/rfc4861) menjelaskan penggunaan ICMPv6 dalam auto konfigurasi.

2. *Neighbor Discovery Protocol* (NDP): NDP adalah protokol yang penting dalam jaringan IPv6 dan berhubungan erat dengan ICMPv6. NDP menggunakan pesan-pesan ICMPv6 seperti *Neighbor Solicitation* (NS), *Neighbor Advertisement* (NA), dan Redirect untuk menemukan, memetakan, dan mengelola tetangga dalam jaringan. RFC 4861 menjelaskan lebih lanjut tentang NDP dan penggunaan ICMPv6 dalam protokol ini.
3. *Multicast Listener Discovery* (MLD): MLD menggunakan pesan ICMPv6 dalam pengelolaan keanggotaan grup multicast pada host IPv6. Pesan-pesan MLD digunakan untuk bergabung dengan grup multicast, meninggalkan grup multicast, atau melaporkan keanggotaan grup multicast. RFC 3810: *Multicast Listener Discovery Version* 2 (MLDv2) for IPv6 (https://tools.ietf.org/html/rfc3810) menjelaskan penggunaan MLD dan pesan-pesan ICMPv6 terkait.
4. *Path MTU Discovery*: ICMPv6 digunakan dalam proses Path MTU Discovery untuk menemukan ukuran maksimum paket yang dapat dikirim melalui jalur jaringan IPv6 tanpa harus dipecah menjadi fragmen. Pesan ICMPv6 *Packet Too Big* (PTB) digunakan untuk memberi tahu host pengirim bahwa paket yang dikirim terlalu besar dan perlu dikurangi ukurannya. RFC 1981: Path MTU Discovery for IP version 6 (https://tools.ietf.org/html/rfc1981) menjelaskan penggunaan ICMPv6 dalam Path MTU Discovery.
5. *Redirect Messages*: Pesan ICMPv6 Redirect digunakan oleh router untuk memberi tahu host pengirim bahwa ada rute yang lebih efisien melalui tetangga yang berbeda untuk mencapai tujuan tertentu. Penggunaan pesan ICMPv6 Redirect dijelaskan dalam RFC 4861.

Penggunaan ICMPv6 dalam pengalamatan dan konfigurasi mencerminkan fitur dan fungsionalitas IPv6 yang unik. Referensi yang disebutkan di atas adalah sumber yang diterima dan diakui dalam spesifikasi dan standar *Internet Engineering Task Force* (IETF) yang terkait dengan pengembangan protokol Internet.

12.8 Pemecahan Masalah dan Troubleshooting dengan ICMP

12.8.1 Penggunaan Pesan ICMP dalam Pemecahan Masalah

Penggunaan Pesan ICMP dalam Pemecahan Masalah:

1. Pemeriksaan Konektivitas: ICMP Echo Request (Ping) dan ICMP Echo Reply digunakan untuk menguji konektivitas dan latensi antara dua host dalam jaringan. Informasi tentang penggunaan ICMP Ping dalam pemecahan masalah dapat ditemukan di RFC 792: Internet Control Message Protocol (https://tools.ietf.org/html/rfc792).
2. Mendeteksi Masalah Jaringan: Pesan ICMP seperti Destination Unreachable, Time Exceeded, Redirect, dan Parameter Problem dapat memberikan informasi penting tentang masalah yang terjadi dalam jaringan. RFC 1122: Requirements for Internet Hosts—Communication Layers (https://tools.ietf.org/html/rfc1122) dan RFC 1812: Requirements for IP Version 4 Routers (https://tools.ietf.org/html/rfc1812) memberikan detail tentang penggunaan dan interpretasi pesan-pesan ICMP dalam pemecahan masalah.
3. Mengetahui MTU (*Maximum Transmission Unit*): Pesan ICMPv4 dan ICMPv6 Packet Too Big (PTB) digunakan untuk mengetahui MTU pada jalur jaringan. Informasi tentang penggunaan pesan PTB dapat ditemukan di RFC 1191: Path MTU Discovery (https://tools.ietf.org/html/rfc1191) dan RFC 1981: Path MTU Discovery for IP version 6 (https://tools.ietf.org/html/rfc1981).

4. Mengetahui Informasi Jaringan: Pesan ICMPv6 *Router Advertisement* (RA) memberikan informasi tentang konfigurasi otomatis alamat IPv6 pada host. RFC 4861: *Neighbor Discovery for IP version* 6 (IPv6) (https://tools.ietf.org/html/rfc4861) menjelaskan penggunaan pesan RA dalam pemecahan masalah dan konfigurasi jaringan.
5. Mengecek Responsivitas Host: Penggunaan pesan ICMP Redirect untuk menguji responsivitas host terkait pengalihan rute dapat ditemukan di RFC 792 dan RFC 1122.
6. Deteksi dan Pemantauan Serangan: Penggunaan pesan ICMP dalam deteksi dan pemantauan serangan dapat dikaji dalam RFC 4950: ICMP *Extensions for Multiprotocol Label Switching* (https://tools.ietf.org/html/rfc4950) dan RFC 8085: UDP Usage Guidelines (https://tools.ietf.org/html/rfc8085).

12.8.2 Teknik Troubleshooting menggunakan ICMP

ICMP (*Internet Control Message Protocol*) dapat digunakan dalam teknik troubleshooting untuk memeriksa konektivitas, melacak rute paket, dan mendeteksi masalah dalam jaringan. Berikut ini adalah beberapa teknik troubleshooting yang menggunakan ICMP.

1. Ping: Utilitas ping menggunakan pesan ICMP Echo Request dan ICMP Echo Reply untuk menguji konektivitas dan mengukur latensi (ping) antara host pengirim dan tujuan. Ping dapat digunakan untuk memeriksa apakah host tujuan dapat dicapai dan memeriksa responsivitasnya.(Referensi: RFC 792: Internet Control Message Protocol (https://tools.ietf.org/html/rfc792))
2. Traceroute: Traceroute menggunakan pesan ICMP Time Exceeded dan ICMP Echo Request dengan TTL (Time-to-Live) yang meningkat secara bertahap untuk melacak jalur paket dari host pengirim ke tujuan. Ini membantu dalam melihat hop-hops yang dilewati oleh paket dan mengukur latensi di

setiap hop.(Referensi: RFC 1393: Traceroute Using an IP Option (https://tools.ietf.org/html/rfc1393))

3. Path MTU Discovery: Pesan ICMP Packet Too Big digunakan untuk menemukan MTU (Maximum Transmission Unit) yang lebih kecil pada jalur jaringan. Ini membantu menghindari fragmentasi paket yang berlebihan dan kehilangan paket di jaringan. (Referensi: RFC 1191: Path MTU Discovery (https://tools.ietf.org/html/rfc1191))
4. ICMP Redirect: Pesan ICMP Redirect digunakan oleh router untuk memberi tahu host pengirim bahwa ada rute yang lebih efisien melalui tetangga yang berbeda untuk mencapai tujuan tertentu. Dengan menganalisis pesan ICMP Redirect, Anda dapat melacak perutean yang salah atau mengoptimalkan perutean dalam jaringan. (Referensi: RFC 792, RFC 1122: Requirements for Internet Hosts—Communication Layers (https://tools.ietf.org/html/rfc1122))

12.9 Pemantauan dan Pengukuran Kinerja Jaringan dengan ICMP

12.9.1 Penggunaan ICMP dalam Pemantauan Kinerja Jaringan

ICMP (*Internet Control Message Protocol*) dapat digunakan dalam pemantauan kinerja jaringan untuk mengukur dan memantau parameter-parameter penting seperti latensi, kehilangan paket, dan kualitas layanan. Berikut ini adalah beberapa penggunaan ICMP dalam pemantauan kinerja jaringan.

1. ICMP *Echo Request*/*Reply* (Ping): Pesan ICMP *Echo Request* dan ICMP Echo Reply (umumnya dikenal sebagai "Ping") digunakan untuk mengukur latensi dan kehilangan paket dalam jaringan. Dengan mengirim pesan ICMP Echo Request ke host tujuan dan menerima ICMP Echo Reply, Anda dapat memperoleh informasi tentang waktu tempuh paket dan mengukur responsivitas host tersebut.(Referensi: RFC 792:

Internet Control Message Protocol (https://tools.ietf.org/html/rfc792))

2. ICMP *Time Exceeded*: Pesan *ICMP Time Exceeded* digunakan dalam pemantauan jaringan untuk mengidentifikasi hop-hops yang mengalami masalah atau menghasilkan penundaan yang berlebihan. Dengan melacak pesan ICMP Time Exceeded, Anda dapat menentukan hop-hops mana yang memiliki latensi atau konfigurasi yang tidak normal.
3. ICMP *Destination Unreachable*: Pesan ICMP Destination Unreachable digunakan untuk memantau ketersediaan tujuan atau layanan dalam jaringan. Jika tujuan tidak dapat dijangkau atau layanan tidak tersedia, host pengirim akan menerima pesan ICMP Destination Unreachable yang memberikan indikasi tentang masalah tersebut.
4. ICMP *Router Advertisement*: Pesan ICMPv6 *Router Advertisement* (RA) digunakan dalam pemantauan kinerja jaringan IPv6. RA berisi informasi tentang pengaturan jaringan seperti prefix, gateway default, dan opsi konfigurasi lainnya. Dengan memantau pesan RA, Anda dapat memperoleh wawasan tentang konfigurasi jaringan IPv6. (Referensi: RFC 4861: *Neighbor Discovery for IP version* 6 (IPv6) (https://tools.ietf.org/html/rfc4861))

12.9.2 Metrik Kinerja yang Diukur melalui ICMP

Melalui ICMP (*Internet Control Message Protocol*), beberapa metrik kinerja jaringan dapat diukur untuk memantau dan menganalisis kualitas layanan dan kinerja jaringan. Berikut ini adalah beberapa metrik kinerja yang diukur melalui ICMP.

1. Latensi (Ping Time):
    - Latensi mengukur waktu yang dibutuhkan untuk pesan pergi dari host pengirim ke tujuan dan kembali lagi.
    - Diukur menggunakan pesan ICMP Echo Request dan ICMP Echo Reply (Ping).

- Menunjukkan responsivitas dan kecepatan komunikasi dalam jaringan.

2. Kehilangan Paket:
   - Mengukur jumlah paket yang hilang atau tidak berhasil dikirim dari host pengirim ke tujuan.
   - Diukur menggunakan pesan ICMP Echo Request dan melihat apakah ada ICMP Echo Reply yang diterima.
   - Menunjukkan reliabilitas dan kualitas koneksi jaringan.

3. Jitter:
   - Jitter mengukur variasi waktu antara kedatangan paket-paket dalam jaringan.
   - Diukur dengan membandingkan waktu tiba paket-paket berurutan menggunakan pesan ICMP Echo Request.
   - Menunjukkan stabilitas dan konsistensi latensi jaringan.
     Referensi: RFC 5481: Packet Delay Variation Applicability Statement (https://tools.ietf.org/html/rfc5481)

4. Round-Trip Time (RTT):
   - RTT mengukur waktu yang dibutuhkan oleh paket untuk pergi dari host pengirim ke tujuan dan kembali lagi.
   - Diukur dengan membandingkan waktu tiba pesan ICMP Echo Request dan waktu tiba ICMP Echo Reply.
   - Menunjukkan waktu total yang diperlukan untuk mengirim dan menerima paket dalam jaringan.

   Referensi: RFC 792
5. Path MTU (Maximum Transmission Unit):
   - Mengukur ukuran maksimum paket yang dapat dikirim melalui jalur jaringan tanpa harus dipecah menjadi fragmen.
   - Diukur menggunakan pesan ICMPv4 atau ICMPv6 Packet Too Big (PTB).

- Menunjukkan kemampuan jaringan untuk mengirim paket berukuran besar tanpa kehilangan atau fragmentasi. Referensi: RFC 1191: Path MTU Discovery (https://tools.ietf.org/html/rfc1191), RFC 1981: Path MTU Discovery for IP version 6 (https://tools.ietf.org/html/rfc1981)

12.10 Masa Depan ICMP

12.10.1 Perkembangan dan Evolusi ICMP

ICMP (*Internet Control Message Protocol*) telah mengalami perkembangan dan evolusi sejak awal diperkenalkan. Berikut ini adalah beberapa tahap perkembangan dan evolusi ICMP.

1. ICMPv4: Versi awal ICMP dikembangkan untuk digunakan dengan protokol IPv4 (Internet Protocol version 4). Spesifikasi ICMPv4 dijelaskan dalam RFC 792: Internet Control Message Protocol (https://tools.ietf.org/html/rfc792). ICMPv4 digunakan untuk mengirim pesan kontrol dan kesalahan dalam jaringan IPv4, seperti pesan Echo Request/Reply (Ping) dan pesan-pesan kesalahan seperti Destination Unreachable dan Time Exceeded.
2. ICMPv6: Dalam pengenalan protokol IPv6 (Internet Protocol version 6), ICMPv6 dikembangkan untuk digunakan dalam jaringan IPv6. ICMPv6 memiliki perbedaan signifikan dalam format dan fungsionalitas dibandingkan dengan ICMPv4. Spesifikasi ICMPv6 dijelaskan dalam RFC 4443: Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification (https://tools.ietf.org/html/rfc4443). ICMPv6 digunakan untuk tujuan yang serupa dengan ICMPv4, tetapi diadaptasi untuk lingkungan IPv6, seperti auto-konfigurasi alamat, penyamaran tetangga, dan pesan-pesan perutean.

3. ICMP Extensions: Selain ICMPv4 dan ICMPv6, ada beberapa RFC yang mengusulkan ekstensi dan pengembangan lain untuk ICMP. Misalnya, RFC 4884: Extended ICMP to Support Multi-Part Messages (https://tools.ietf.org/html/rfc4884) memperkenalkan format pesan ICMP yang memungkinkan pesan yang lebih besar dibagi menjadi beberapa bagian. RFC 4890: Recommendations for Filtering ICMPv6 Messages in Firewalls (https://tools.ietf.org/html/rfc4890) memberikan panduan tentang bagaimana menyaring pesan ICMPv6 di firewall.

12.10.2 Tantangan dan Peluang di Masa Depan

Tantangan dan peluang di masa depan terkait dengan ICMP (*Internet Control Message Protocol*) dan jaringan secara umum terus berkembang seiring dengan kemajuan teknologi. Berikut ini adalah beberapa tantangan dan peluang yang mungkin dihadapi di masa depan:

1. Pertumbuhan *Internet of Things* (IoT): Dengan peningkatan jumlah perangkat yang terhubung dalam ekosistem IoT, akan ada tantangan dalam mengelola lalu lintas jaringan yang semakin padat dan memastikan ketersediaan dan keamanan komunikasi antar perangkat. ICMP dapat terlibat dalam pemantauan dan pelaporan kinerja jaringan IoT. (Referensi: RFC 7452: Architectural Considerations in Smart Object Networking (https://tools.ietf.org/html/rfc7452))
2. Keamanan Jaringan: Dalam menghadapi ancaman keamanan yang terus berkembang seperti serangan DDoS, spoofing, dan pengintaian, perlu diperkuat perlindungan terhadap protokol ICMP agar tidak disalahgunakan sebagai alat serangan. Langkah-langkah seperti filtering ICMP dan implementasi kebijakan keamanan yang tepat akan menjadi penting. (Referensi: RFC 4890: Recommendations for Filtering ICMPv6 Messages in Firewalls (https://tools.ietf.org/html/rfc4890))

3. Peningkatan Kapasitas Jaringan: Dengan meningkatnya permintaan akan kecepatan dan kapasitas jaringan, ICMP perlu terus berkembang dan beradaptasi untuk mengukur dan memantau kinerja jaringan yang semakin cepat dan canggih. Pengembangan metrik kinerja yang lebih akurat dan responsif serta perubahan dalam format pesan ICMP dapat menjadi peluang di masa depan. (Referensi: RFC 8304: *Transport Features of Internet Control Message Protocol* (ICMPv6) (https://tools.ietf.org/html/rfc8304))
4. Migrasi ke IPv6: Seiring dengan peningkatan adopsi protokol IPv6, penggunaan ICMPv6 sebagai bagian integral dari IPv6 akan menjadi lebih penting. Tantangan dan peluang muncul dalam memastikan interoperabilitas yang baik antara perangkat dan jaringan IPv4 dan IPv6, serta memahami dan mengelola pesan-pesan ICMPv6 yang relevan. (Referensi: RFC 4861: Neighbor Discovery for IP version 6 (IPv6) (https://tools.ietf.org/html/rfc4861))

DAFTAR PUSTAKA

RFC 791: Internet Protocol (https://tools.ietf.org/html/rfc791)

RFC 793: Transmission Control Protocol (https://tools.ietf.org/html/rfc793)

Comer, D. E. 2014. Internetworking with TCP/IP: Principles, Protocols, and Architecture (6th Edition). Pearson Education.

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

Roberts, L. G., & Walden, D. C. 1972. The ARPANET after twenty years. IEEE Transactions on Communications, 20(1), 3-9.

RFC 791: Internet Protocol (https://tools.ietf.org/html/rfc791)

RFC 1631: The IP Network Address Translator (NAT) (https://tools.ietf.org/html/rfc1631)

RFC 2460: Internet Protocol, Version 6 (IPv6) Specification (https://tools.ietf.org/html/rfc2460))

RFC 5211: An Internet Transition Plan (https://tools.ietf.org/html/rfc5211))

RFC 4213: Basic Transition Mechanisms for IPv6 Hosts and Routers (https://tools.ietf.org/html/rfc4213))

RFC 4301: Security Architecture for the Internet Protocol (https://tools.ietf.org/html/rfc4301)

Leland, E., & Asoni, D. 2019. The Role of Latency in Network Performance. In IEEE Global Communications Conference (GLOBECOM) (pp. 1-6). IEEE.)

Tuan, L. A., & Vung, T. T. 2019. Analysis of Packet Loss in IP Networks. In International Conference on Advanced Research in Computing, Electronics, and Communication (ICARCEC) (pp. 169-173). Springer, Singapore.)

Katti, S., & Anantharamu, S. 2019. Packet Order Recovery Techniques in IP Networks. In International Conference on Advances in Computing and Data Sciences (ICACDS) (pp. 498-507). Springer, Singapore.)
Sharma, S., Sharma, R., & Bansal, S. 2019. A Review on Failure Detection and Recovery Mechanism in IP Networks. In International Conference on Communication, Computing and Electronics Systems (ICCCES) (pp. 1-5). IEEE.)
Tripathi, D., & Vankar, V. D. 2019. Error Detection and Correction Techniques in IP Networks: A Review. In International Conference on Computing, Communication and Signal Processing (ICCCSP) (pp. 1-5). IEEE.)
Goyal, S., & Kaur, K. 2019. Handling Network Instabilities in IP Networks: A Comprehensive Review. In International Conference on Artificial Intelligence and Data Engineering (AIDE) (pp. 1-6). IEEE.)
Agrawal, S., & Gupta, V. 2019. Scalability Issues and Solutions in IP Networks: A Survey. In International Conference on Computer Science and Engineering (ICSE) (pp. 1-5). IEEE.)
RFC 792: Internet Control Message Protocol (https://tools.ietf.org/html/rfc792))
RFC 4443: Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) (https://tools.ietf.org/html/rfc4443))
RFC 4379: Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures (https://tools.ietf.org/html/rfc4379))
RFC 792: Internet Control Message Protocol (ICMP)
Stevens, W. R., Wright, G. R., & Stevens, M. 1994. TCP/IP Illustrated, Volume 1: The Protocols. Addison-Wesley
Comer, D. E. 2000. Internetworking with TCP/IP, Volume 1: Principles, Protocols, and Architecture. Prentice Hall)

RFC 1191: Path MTU Discovery (https://tools.ietf.org/html/rfc1191))
RFC 792: Internet Control Message Protocol (https://tools.ietf.org/html/rfc792)
RFC 1122: Requirements for Internet Hosts—Communication Layers (https://tools.ietf.org/html/rfc1122)
RFC 950: Internet Standard Subnetting Procedure (https://tools.ietf.org/html/rfc950)
RFC 1812: Requirements for IP Version 4 Routers (https://tools.ietf.org/html/rfc1812)
RFC 4861: Neighbor Discovery for IP version 6 (IPv6) (https://tools.ietf.org/html/rfc4861)
RFC 792: Internet Control Message Protocol (https://tools.ietf.org/html/rfc792)
RFC 1393: Traceroute Using an IP Option (https://tools.ietf.org/html/rfc1393)
RFC 1393: Traceroute Using an IP Option (https://tools.ietf.org/html/rfc1393)
Microsoft Docs - PathPing (https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/pathping)
MTR - Homepage (https://www.bitwizard.nl/mtr/)
Referensi:Cisco-TroubleshootingRouting (https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13714-40.html)
RFC 4950: ICMP Extensions for Multiprotocol Label Switching (https://tools.ietf.org/html/rfc4950)
CERT Advisory CA-1998-01: Smurf IP Denial-of-Service Attacks (https://www.cert.org/historical/advisories/CA-1998-01.cfm)
CERT Advisory CA-1996-21: Teardrop IP Denial-of-Service Attack (https://www.cert.org/historical/advisories/CA-1996-21.cfm)

CERT Advisory CA-1998-12: ICMP Redirect Attack (https://www.cert.org/historical/advisories/CA-1998-12.cfm)
RFC 4890: Recommendations for Filtering ICMPv6 Messages in Firewalls (https://tools.ietf.org/html/rfc4890)
RFC 8085: UDP Usage Guidelines (https://tools.ietf.org/html/rfc8085)
RFC 8273: Unique IPv6 Prefix per Host (https://tools.ietf.org/html/rfc8273)
RFC 4732: Internet Denial-of-Service Considerations (https://tools.ietf.org/html/rfc4732)
RFC 4038: Application Aspects of IPv6 Transition (https://tools.ietf.org/html/rfc4038)
RFC 2460: Internet Protocol, Version 6 (IPv6) Specification (https://tools.ietf.org/html/rfc2460)
RFC 4443: Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification (https://tools.ietf.org/html/rfc4443)
RFC 4861: Neighbor Discovery for IP version 6 (IPv6) (https://tools.ietf.org/html/rfc4861)
RFC 4862: IPv6 Stateless Address Autoconfiguration (https://tools.ietf.org/html/rfc4862)
RFC 792: Internet Control Message Protocol (https://tools.ietf.org/html/rfc792)
RFC 1393: Traceroute Using an IP Option (https://tools.ietf.org/html/rfc1393)
RFC 1191: Path MTU Discovery (https://tools.ietf.org/html/rfc1191)
RFC 792, RFC 1122: Requirements for Internet Hosts—Communication Layers (https://tools.ietf.org/html/rfc1122)
RFC 792: Internet Control Message Protocol (https://tools.ietf.org/html/rfc792)

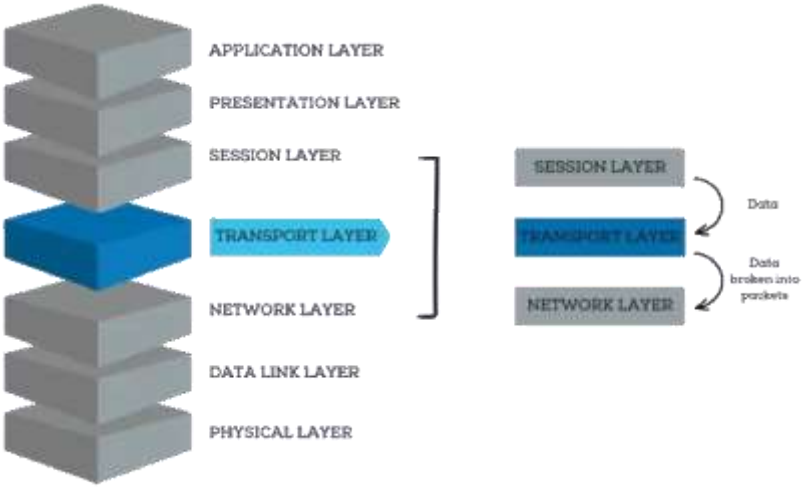
RFC 4861: Neighbor Discovery for IP version 6 (IPv6) (https://tools.ietf.org/html/rfc4861)
RFC 1191: Path MTU Discovery (https://tools.ietf.org/html/rfc1191),
RFC 1981: Path MTU Discovery for IP version 6 (https://tools.ietf.org/html/rfc1981)
RFC 7452: Architectural Considerations in Smart Object Networking (https://tools.ietf.org/html/rfc7452)
RFC 4890: Recommendations for Filtering ICMPv6 Messages in Firewalls (https://tools.ietf.org/html/rfc4890)
RFC 8304: Transport Features of Internet Control Message Protocol (ICMPv6) (https://tools.ietf.org/html/rfc8304)
RFC 4861: Neighbor Discovery for IP version 6 (IPv6) (https://tools.ietf.org/html/rfc4861)
Refrensi Comer, D. E. 2014. Internetworking with TCP/IP: Principles, Protocols, and Architecture (6th Edition). Pearson Education.)
RFC 792: Internet Control Message Protocol (https://tools.ietf.org/html/rfc792))

BAB 13
LAPISAN TRANSPORT

Oleh Shah Khadafi

13.1 Pengenalan Lapisan Transport

Protokol Model OSI (*Open System Interconnection*) memiliki tujuh lapisan, yang masing-masing diberi satu set fungsi. Lapisan ke 4 (empat), yaitu lapisan transport, adalah lapisan yang berfungsi dalam mengkomunikasikan pesan secara end-to-end pada komputer *host* di dalam jaringan. Pada pembahasan ini, penjelasan lapisan transport adalah memberikan pemahaman mengenai lapisan transport dan bagaimana fungsinya, serta dua protokol pentingnya, TCP (*Transmission Control Protocol*) dan UDP (*User Datagram Protocol*).



Gambar 13.1. Letak Lapisan Transport Pada Protokol Jaringan (Sumber : https://www.whatismyip.com/transport-layer/)

Lapisan transport bertanggung jawab untuk membangun sesi komunikasi antara dua aplikasi yang hendak mengirimkan data di antara dua buah komputer *host*. Seperti yang ditunjukkan pada gambar 13.1, lapisan transport selaku penghubung antara lapisan aplikasi dan lapisan di bawahnya yang bertanggung jawab untuk melakukan transmisi jaringan.

Tanggung jawab utama protokol lapisan transport adalah (Dye, McDonald and Rufi, 2008):

1. Melakukan pelacakan komunikasi yang terjadi antara aplikasi pada komputer host sumber dan tujuan.
2. Melakukan segmentasi data sebagai bentuk pengelolaan data dan penyusunan kembali data melalui aliran data.
3. Melakukan identifikasi aplikasi yang sesuai dengan setiap aliran komunikasi diantara komputer host pengirim dan penerima.
4. Melakukan mulitplexing dari berbagai segmentasi data yang dikirimkan dari berbagai macam aplikasi dengan masing-masing layanan tertentu.

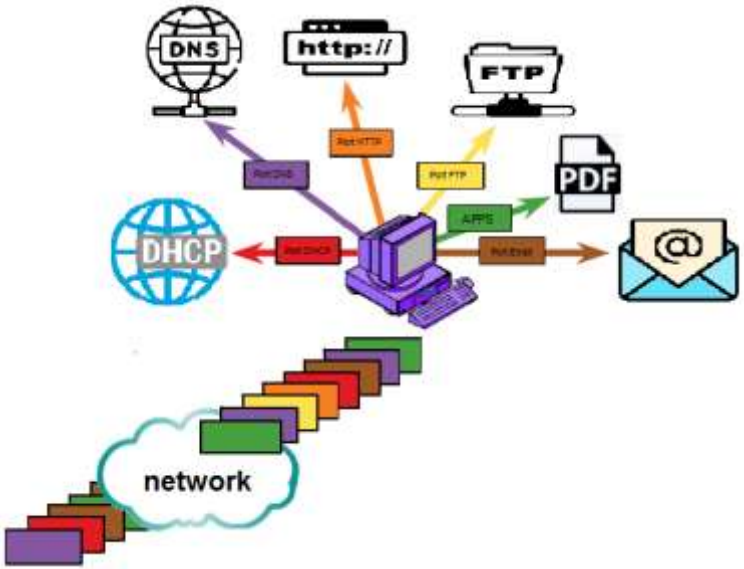
Pelacakan komunikasi pada lapisan *transport,* terjadi pada aplikasi yang digunakan diantara komputer pengirim dan penerima (Khadafi *et al.*, 2019). Dalam melakukan komunikasinya memungkinkan terjadinya banyak aplikasi komunikasi yang digunakan yang bersamaan berjalan dalam jaringan komputer (Khadafi, Nurmuslimah and Anggakusuma, 2019). Masing-masing aplikasi berkomunikasi dengan satu atau lebih aplikasi yang sesuai pada satu atau lebih komputer secara jarak jauh. Merupakan tanggung jawab lapisan transport untuk memelihara dan melacak banyak komunikasi yang terjadi.

Segmentasi data dilakukan karena terbatasnya jumlah data yang dikirimkan ke media jaringan komputer dalam satu paket pegiriman. Lapisan transport memiliki layanan yang dapat mengelompokkan data aplikasi ke dalam segment data dalam

bentuk blok-blok dengan ukuran yang sesuai. Pada proses segmentasi data ini juga mencakup enkapsulasi yang diperlukan pada setiap bagian segment data. Dimana, masing-masing segment data terdapat *header*, yang ditambahkan ke setiap blok data yang digunakan untuk melakukan identifikasi ketika perakitan ulang (*reassembly*). Selain itu, header juga digunakan untuk melacak aliran data ketika proses pengiriman.

Identifikasi layanan yang digunakan oleh aplikasi yang berjalan di dalam jaringan komputer oleh komputer pengirima dan penerima melalui aliran segment data yang dikirimkan. Lapisan transport mengenali layanan melalui identifikasi nomor *port* dengan memberikan pengenal pada setiap aplikasi. Masing-masing layanan yang digunakan oleh perangkat lunak aplikasi yang menggunakan akses jaringan diberi nomor *port* unik di komputer host. Lapisan transport menggunakan port untuk mengidentifikasi aplikasi atau layanan (Andrew S. Tanenbaum and Wetherall, 2011).

Segmentasi data merubah paket data menjadi potongan yang lebih kecil, yang memungkinkan banyak aplikasi menggunakan berbagai komunikasi yang berbeda yang dilakukan oleh banyak user yang berbeda juga. Dari segmentasi data, dilakukanlah *multiplexing* (sisipan) blok data pada saat pengiriman melewati media jaringan yang digunakan. *Multiplexing* di dalam protokol lapisan *transport* juga menyediakan sarana untuk mengirim dan menerima data secara bersama-sama ketika menjalankan beberapa aplikasi yang dijalankan secara bersamaan di dalam komputer. Keseluruhan tanggung jawab yang dilakukan oleh lapisan Transport digambar yang nampak pada gambar 14.2.



Gambar 13.2. Lapisan Transport Melakukan Identifikasi Aplikasi, Pelacakan Komunikasi, Segmentasi dan Multiplexing Data.

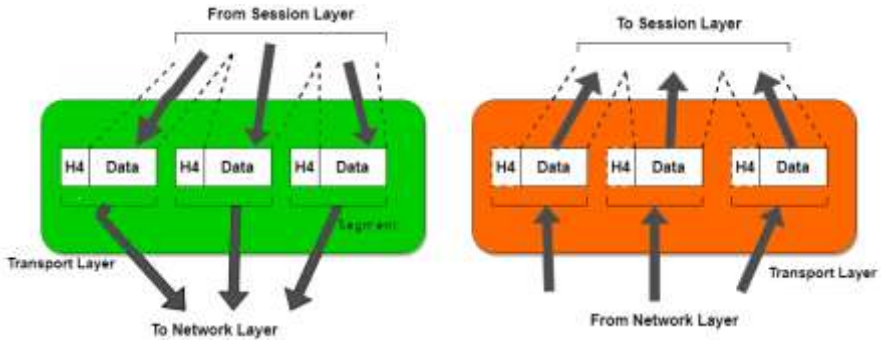
13.2 Cara Kerja Lapisan Transport

Lapisan transport mengambil layanan dari lapisan di atasnya yaitu lapisan Application (lapisan Presentation dan di bawahnya lapisan Session biasanya menjadi satu unit bagian pada sebuah aplikasi atau aplikasi sistem. Secara prinsip kerja lapisan *Presentation* dan *Session* sudah termasuk dalam lapisan Application) dan menyediakan untuk layanan di bawahnya yaitu ke lapisan Network yang di dalamnya (Kurose *et al.*, 2017), yang terjadi proses *encapsulation* (penambahan header informasi pada data) terhadap data yang hendak dikirimkan, seperti yang nampak pada gambar 13.3.

Pada komputer host pengirim, lapisan transport menerima data (pesan) dari lapisan di atasnya yaitu lapisan Application, dan kemudian melakukan Segmentasi, membagi pesan aslinya menjadi ke dalam beberapa blok segment data, dan kemudian

menambahkan nomor *port* sumber dan *port* tujuan ke dalam *header* segmen data (Khadafi, Meilani and Arifin, 2017), dan mengirim masing-masing blok data ke lapisan di bawahnya yaitu lapisan *Network*.

Pada komputer host penerima, lapisan transport menerima data dari lapisan di bawahya yaitu lapisan Network, membaca *header* segmen data berupa blok data, mengidentifikasi nomor port tujuan, dan kemudian segment data tersebut disusun kembali sehingga sesuai dengan pesan asli yang dikirimkan oleh komputer pengirim. Setelah blok-blok data tersebut telah tersusun seperti data asilnya, lapisan Transport meneruskannya ke lapisan di atasnya yaitu lapisan Application dengan mengidentifikas nomor port yang sesuai.



Gambar 12.3. Header Lapisan Transport

13.2.1 Komunikasi Antar Komputer Host Pengirim dan Penerima

Komunikasi diantara host pengirim dan penerima diperlukan ketika terjadinya pengiriman data di dalam jaringan. Lapisan transport juga bertanggung jawab untuk membuat Koneksi *end-to-end* diantara komputer host yang utamanya menggunakan layanan TCP dan UDP. TCP adalah protokol yang aman dan *connection-orientated* yang menggunakan mekanisme

handshaking untuk membuat koneksi yang kuat diantara dua host pengirim dan penerima (Stallings, 2014). TCP memastikan pengiriman pesan yang andal dan digunakan dalam berbagai aplikasi. UDP, adalah protokol *stateless* yang kurang handal yang belum tentu pengiriman dengan cara yang terbaik. UDP ini cocok untuk aplikasi yang tidak memperhatikan flow atau *error control* dan pengiriman data dalam jumlah besar, seperti video.

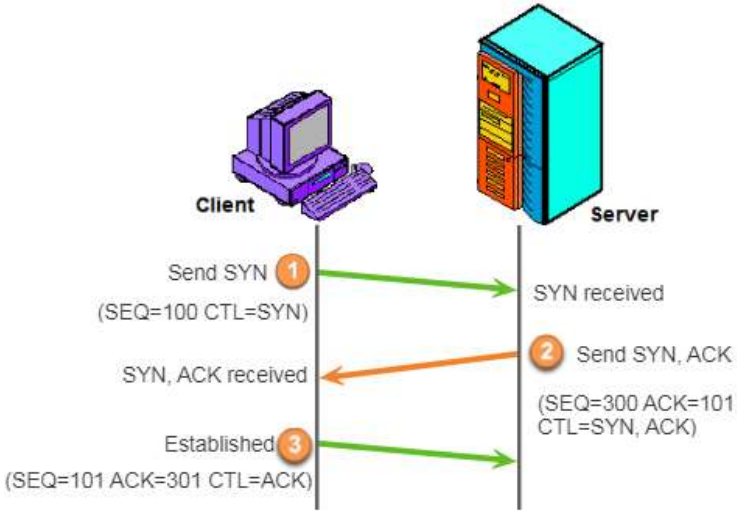
13.2 Protokol data pada Lapisan Transport

Pada protokol OSI maupun TCP/IP proses data segmented data *re-assembled* dapat dicapai dengan menggunakan dua protokol lapisan transport yang sangat berbeda: *Transmission Control Protocol* (TCP) dan *User Datagram Protocol* (UDP). TCP dianggap sebagai protokol lapisan *Transport* yang fiturnya lengkap dan juga andal, yang memastikan bahwa semua *segment packet* data tiba di komputer tujuan terkirim dengan baik. Sebaliknya, UDP adalah protokol lapisan *Transport* yang sangat sederhana yang memiliki keandalan sangat rendah (Purbo, 2018).

13.3 Fitur-fitur Layanan pada TCP

13.3.1 Pembentukan dan Pemutusan Koneksi

Sebelum terjadinya pengiriman data secara *end-to-end*, dilakukan terlebih dahulu pembentukan koneksi TCP diantara host yang dikenal dengan *three-way handshaking*, karena TCP adalah protokol *connection-oriented*. Pengertian dari protokol *connection-oriented* adalah protokol yang membuat koneksi permanen antara host *client* dengan *host server* sebelum transfer data dimulai (Khadafi, Meilani and Hidayat, 2017). Selama proses *three-way handshaking*, client dan server saling berkomunikasi mengenai jumlah lalu lintas (*payload*, *byte*, jumlah segmen data) yang diteruskan melalui jaringan, yang harus diselesaikan sebelum transfer data dapat dimulai.



Gambar 13.4. Proses *three-way handshaking* pada TCP

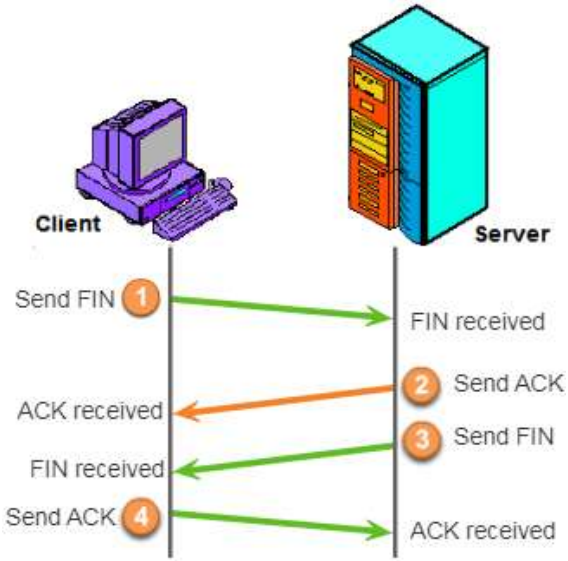
Gambar 13.4 menunjukkan proses *three-way handshaking*, proses pertama *host client* memulai meminta sesi komunikasi dengan mengirimkan segmen dengan *set flag* kontrol *the synchronize sequence number* (SYN). Nomor pengenal awal, dikenal dengan *the initial sequence number* (SEQ) yaitu 100 yang terletak di *header*, digunakan untuk mulai melacak aliran data dari *client* ke *server* pada sesi pertama ini.

Proses yang ke dua yaitu, host *server acknowledges* (mengakui) permintaan segment SYN komunikasi dari client yaitu dimulai ketika *server* menggunakan flag SYN dengan cara yang sama seperti yang dilakukan *client*. Ketika proses pengakuan terjadi, nilai nomor *acknowledges* ditambahkan 1 menjadi 101, sebagai pengakuan bahwa *server* menerima SYN dari client. Nomor pengenal *the initial sequence number* (SEQ) yaitu 300 yang terletak di *header*, yang digunakan untuk melacak aliran data dalam sesi ini dari *server* kembali ke *client*. Sesi penerimaan komunikasi ini dengan mengirimkan kontrol segmen dengan *set flag* berisi SYN

dan ACK yang menunjukkan bahwa nomor *acknowledges* signifikan.

Proses yang ke tiga proses yang terakhir dari *three-way handshaking* yaitu, *host client* merespons segmen ACK dengan menerima *flag* SYN dan ACK yang dikirim oleh *server*. Ketika proses respon ini terjadi dengan mengirimkan control segmen dengan *set flag* berisi ACK yang menunjukkan semua sesi telah dibuat. Kemudian, pembentukan komunikasi antara *client* dan *server* telah terbentuk, dan data pengguna pada sesi ini siap dikirimkan.

Ketika segment data telah terkirim lengkap semuanya, maka untuk menutup koneksi pengguna diperlukan mekanisme pertukaran informasi seperti pada proses *three-way handshaking*. Pada gambar 13.4 menunjukkan proses pemutusan koneksi, proses pertama yaitu *host client* telah lengkap mengirim data dalam aliran jaringan, selanjutnya mengirimkan segmen dengan *set flag* berisi Finish (FIN). Proses yang ke dua yaitu, *host server* merespons permintaan pemutusan koneksi dengan mengirimkan *set flag* berisi *ACK* untuk mengakui penerimaan FIN dari *client*. Proses yang ke tiga yaitu, *server* juga mengirimkan balik *set flag* berisi FIN, untuk mengakhiri sesi *server* ke *client* untuk mengakhiri sesi komunikasi antara *client* dengan *server*. Proses yang ke empat yaitu, *client* merespons dengan *set flag* berisi ACK untuk mengakui permintaan pemutusan set flag FIN dari *server*.



Gambar 13.5. Proses Pemutusan Koneksi pada TCP

13.3.2 Segmentasi Data pada TCP

Di dalam protokol TCP pesan-pesan dipecah menjadi potongan-potongan kecil dan diberikan header tambahan yang dikenal sebagai packets segment TCP. Pada pembahasan ini juga dibahas kehadalan TCP.

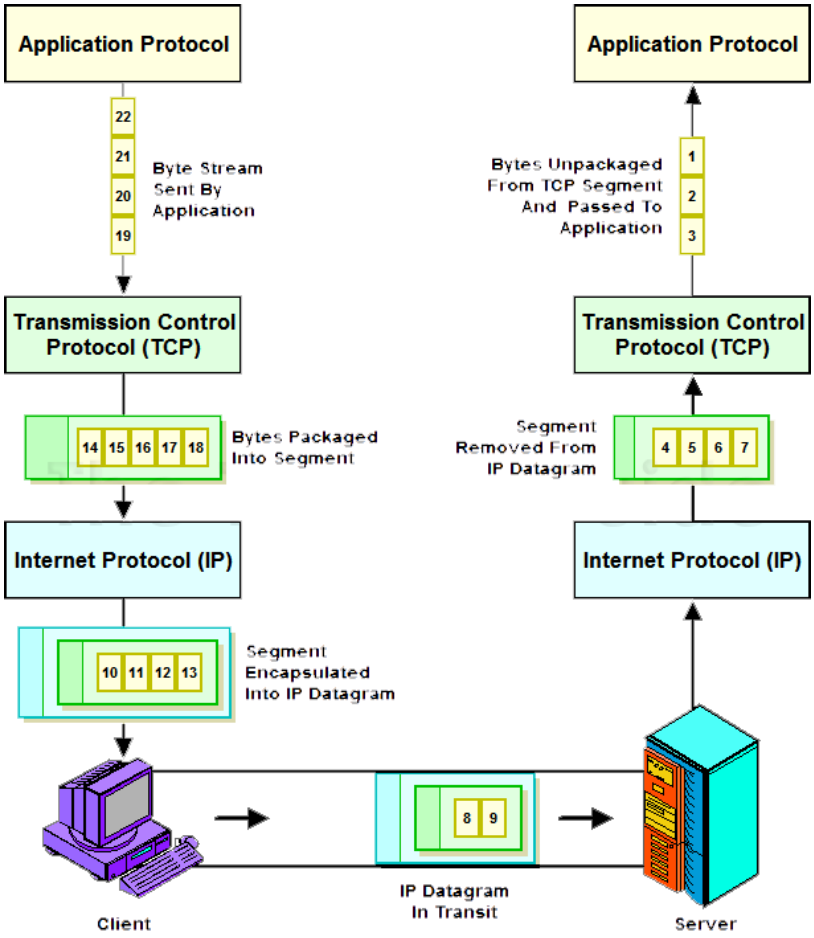
Masing-masing segment diberi nomor secara berurutan yang disebut dengan *segment sequence number* kemudian diteruskan untuk dilakukan proses penambahan header IP. *Segment sequence number* memungkinkan cara mengembalikan dan menyusun ulang segmen data yang diterima oleh *host server*, seperti pada gambar 13.6.

TCP juga melacak jumlah dari masing-masing packets segment data yang telah dikirim ke komputer host *server* dan TCP mengelolah jika terdapat *packet loss*. Jika komputer *host client* tidak menerima *acknowledgment* (persetujuan) dalam periode waktu tertentu, *client* menganggap bahwa paket *segment packet loss* yang

dapat diidentifikasi dari nomor *header*, dan kemudian *host client* mentransmisikannya kembali segment yang hilang.

Flow control pada TCP diperlukan untuk menjaga pengiriman aliran segment data dari *client* menuju *server* dengan menyesuaikan laju aliran data antara *client* dan *server* pada pengiriman sesi tertentu. Mekanisme ini dilakukan dengan cara membatasi jumlah segmen data yang dikirimkan pada satu waktu, dan dengan memerlukan pengiriman *Acknowledges* (ACK) terlebih dahulu dari sisi *server*, sebelum *client* mengirimkan segment data lebih banyak lagi.

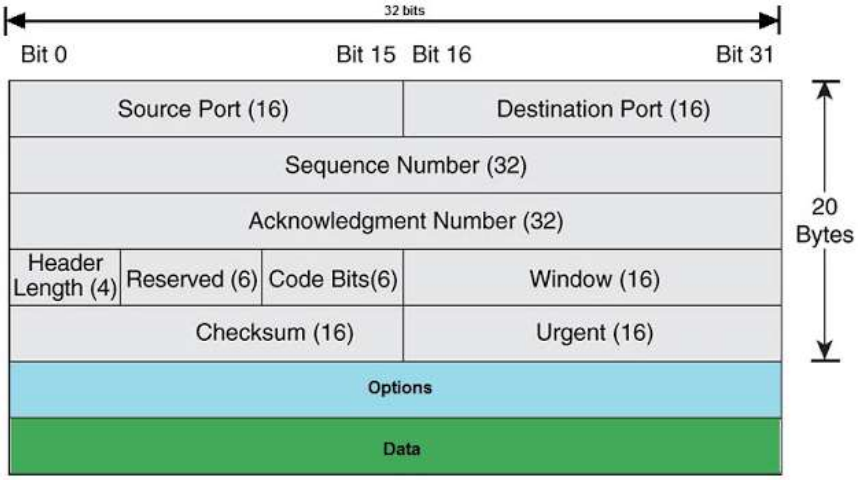
Untuk membantu kontrol aliran, di dalam *header* TCP terdapat salah satu field berukuran 16-bit yang berfungsi untuk menentukan berapa jumlah *byte* yang dapat diterima dan diproses oleh *client* dengan *server* disebut dengan *window size*. Ukuran byte *window size* awal harus disepakati selama permulaan sesi melalui proses *three-way handshaking* sebelumnya. Setelah disepakati, perangkat yang dimiliki *host client* dan *server* membatasi jumlah segmen data yang dikirim berdasarkan *byte* dari *window size*.



Gambar 13.6. *Traffic Segment* Data pada TCP

13.3.3 Header Segment TCP

Kehandalan yang dimiliki oleh protokol TCP menyebabkab *overhead* segment data. Segment TCP memiliki *overhead* sebanyak 20 byte terletak pada header dari data *encapsulation*. *Overhead* segment TCP nampak pada gambar 13.7.

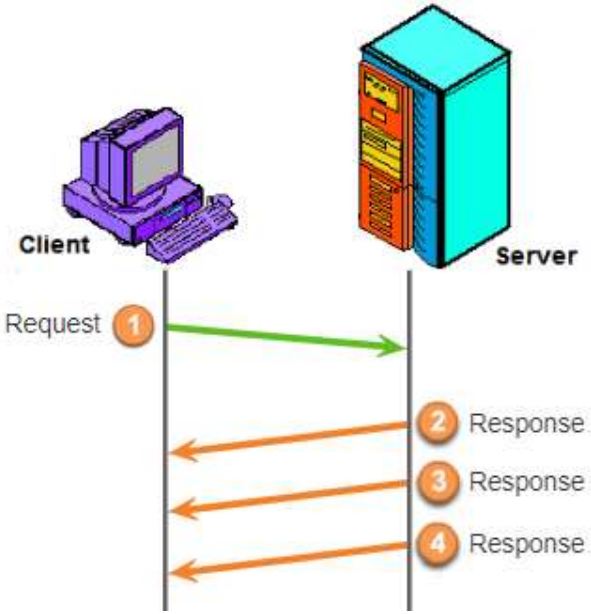


Gambar 13.7. Header *Segment* TCP
(Sumber : https://www.networkurge.com/2017/10/tcp-header-details.html)

13.4 Fitur-fitur Layanan pada UDP

13.4.1 Koneksi Pada UDP

Protokol UDP juga melakukan pengiriman data secara *end-to-end*, namun tidak seperti TCP melakukan pembentukan koneksi dengan *three-way handshaking*. UDP adalah protokol *connectionless,* yang berarti protokol yang tidak membuat koneksi permanen antara *host client* dengan *host server*. Pada gambar 14.8, selama proses pengiriman data antara *client* dan *server* yang diteruskan melalui jaringan, dan ketika sebuah aplikasi memiliki data untuk dikirim, hanyalah mekanisme *request* dan *response* saja yang terjadi sampai dengan potongan terakhir datagram UDP.



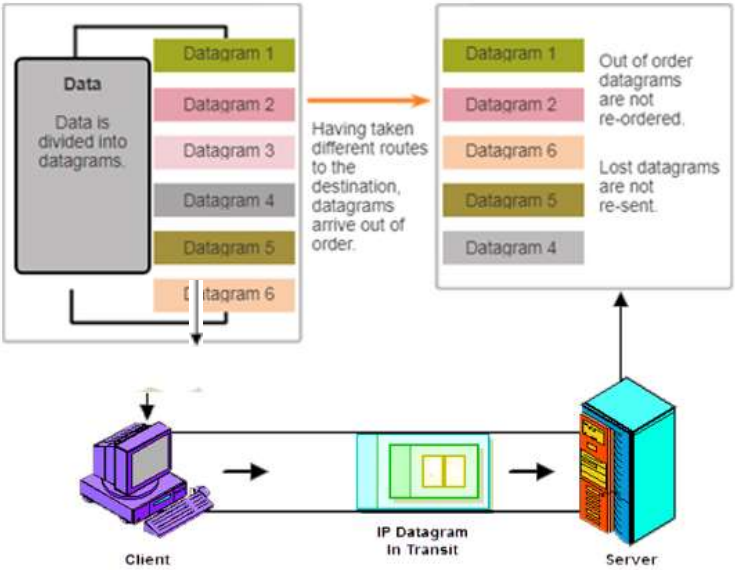
Gambar 13.8. Proses Koneksi pada UDP

13.4.2 Datagram Pada UDP

Di dalam protokol UDP, sama dengan TCP yang melakukan *breaks up* (pemecahan) terhadap pesan menjadi potongan-potongan kecil yang disebut dengan datagram. UDP memiliki *overhead* yang sangat rendah, yang sangat berbeda dengan TCP yang memiliki *overhead* yang detail dan tinggi. Pada UDP tidak ada *sequence number* yang berurutan pada datagram, Di host penerima, UDP menerima packets datagram dan tidak melakukan penyusunan ulang datagram asli yang sesuai dengan urutan, seperti yang ditunjukkan pada gambar 14.9.

UDP tidak melakukan pelacakan pengiriman datagram yang dikirim dari *host* client ke *server*, dengan demikian tidak melakukan pelacakan nomor urut datagram ketika dikirimkan, hanya menyusun ulang data sesuai urutan diterima dan meneruskannya ke aplikasi (Muthahari *et al.*, 2022).

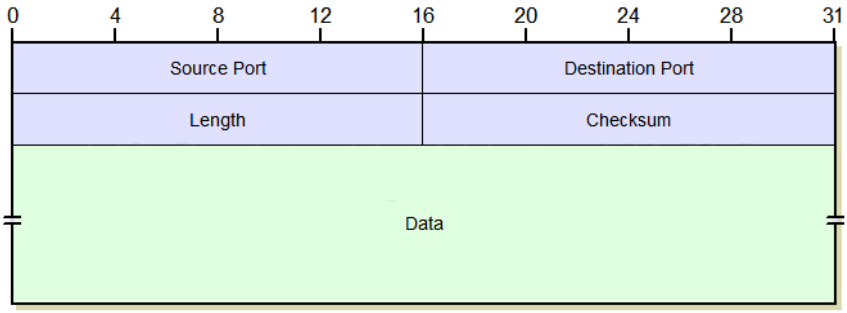
Pada UDP tidak ada *connection-oriented*, *retransmit* terhadap *datagram loss* atau rusak, dan mekanisme ketentuan jumlah bit untuk mengontrol jumlah blok datagram yang dikirim, dikarenakan pada *header* UDP tidak ada field *window size* dan *control byte*.



Gambar 13.9. Traffic Datagram UDP

13.4.3 Header Datagram UDP

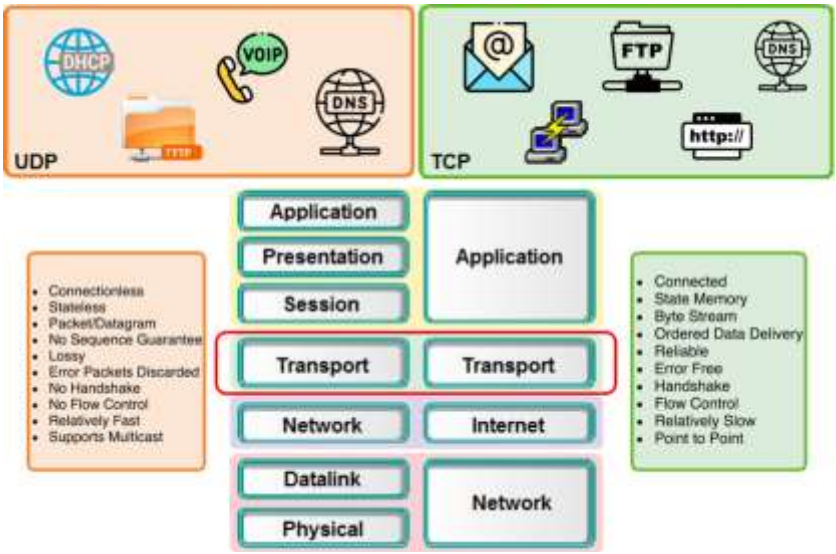
Sifat *connectionless* yang dimiliki oleh protokol UDP menyebabkan *overhead* sangat rendah. Datagram TCP memiliki *overhead* sebanyak 20 byte terletak pada header dari data *encapsulation*. *Overhead* segment TCP nampak pada gambar 14.4.



Gambar 13.6. Header *Segment* TCP
(Sumber :
http://www.tcpipguide.com/free/t_UDPMessageFormat.htm)

13.5 Aplikasi Yang Menggunakan TCP dan UDP

Protokol TCP dan UDP keduanya protokol valid yang berjalan pada lapisan *Transport*. Beberapa sistem aplikasi ada yang menggunakan TCP atau UDP untuk menjalankan aplikasi di dalam sistem yang berbasiskan jaringan. *Application developer* dapat memilih jenis protokol *Transport* mana yang sesuai berdasarkan kebutuhan aplikasi yang digunakan yang dapat berjalan pada *client* dan juga *server,* bahkan untuk keamanan komputer *server* (Khadafi, Pratiwi and Alfianto, 2021)



Gambar 13.6. Aplikasi yang Menggunakan Protokol TCP dan UDP

DAFTAR PUSTAKA

Andrew S. Tanenbaum and Wetherall, D.J. 2011. 'Computer Networks - A Tanenbaum - 5th edition'. Available at: http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:No+Title#0%5Cnhttp://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:No+title#0.

Dye, M.A., McDonald, R. and Rufi, A.W. 2008. Network fundamentals : CCNA exploration companion guide. Cisco Press.

Khadafi, S. et al. 2019. 'Rancang Bangun Website UKM Reviora Tanggulangin Sidoarjo Menggunakan Metode Waterfall Sebagai Media Pemasaran Online', Seminar Nasional Sains dan Teknologi Terapan VII 2019, pp. 705–710.

Khadafi, S., Meilani, B.D. and Arifin, S. 2017. 'Sistem Keamanan Open Cloud Computing Menggunakan Ids (Intrusion Detection System) Dan Ips (Intrusion Prevention System)', Jurnal IPTEK, 21(2), p. 67. Available at: https://doi.org/10.31284/j.iptek.2017.v21i2.207.

Khadafi, S., Meilani, B.D. and Hidayat, S.A. 2017. 'Pengukuran Kompatibilitas Performa Komputer Server Menggunakan JMeter pada Raspberry Pi dan PC Sebagai Layanan Web Server', Seminar Nasional Sains dan Teknologi Terapan V 2017, pp. 157–162. Available at: https://ejurnal.itats.ac.id/sntekpan/article/view/294%0Ahttps://ejurnal.itats.ac.id/sntekpan/article/viewFile/294/183.

Khadafi, S., Nurmuslimah, S. and Anggakusuma, F.K. 2019. 'Implementasi Firewall Dan Port Knocking Sebagai Keamanan Data Transfer Pada Ftp Server Berbasiskan Linux Ubuntu Server', Jurnal Ilmiah NERO, 4(3), pp. 181–188. Available at: https://nero.trunojoyo.ac.id/index.php/nero/article/view/137/127.

Khadafi, S., Pratiwi, Y.D. and Alfianto, E. 2021. 'Keamanan Ftp Server Berbasiskan Ids Dan Ips Menggunakan Sistem Operasi Linux Ubuntu', Network Engineering Research Operation, 6(1), p. 11. Available at: https://doi.org/10.21107/nero.v6i1.190.

Kurose, J.F. et al. 2017. Computer Networking A Top-Down Approach Seventh Edition. 7th edn. Pearson. Available at: www.pearsoned.com/permissions/.

Muthahari, F.A. et al. 2022. 'SNESTIK Seminar Nasional Teknik Elektro, Sistem Informasi, dan Teknik Informatika Implementasi VPS Pada Cloud Infrastructure Untuk Layanan Mail Server Personal PT.Garuda Voucher Indonesia', 3, p. 239. Available at: https://ejurnal.itats.ac.id/snestikdanhttps://snestik.itats.ac.id.

Purbo, O.W. 2018. 'Internet – Tcp / Ip ':, p. 264.

Stallings, W. 2014. 'Network Organization and Topologies. BT - Computing Handbook, Third Edition: Computer Science and Software Engineering', in, pp. 45: 1–20.

BIODATA PENULIS

Agung Susilo Yuda Irawan, S.Kom., M.Kom.
Dosen Program Studi Informatika
Fakultas Ilmu Komputer Universitas Singaperbangsa Karawang

Penulis lahir di Kuningan tanggal 15 Juni 1993. Penulis adalah dosen tetap pada Program Studi Informatika Fakultas Ilmu Komputer Universitas Singaperbangsa Karawang . Menyelesaikan pendidikan S1 pada Jurusan Teknik Informatika dan melanjutkan S2 pada Jurusan Magister Ilmu Komputer.

BIODATA PENULIS

Zen Munawar.
Dosen Program Studi Manajemen Informatika
Politeknik LP3I Bandung

Penulis memiliki jabatan akademik lektor, dan alumni dari TI UNPAS, Pasca Sarjana AdPen UNINUS, Sistem Informasi dari STMIK IM dan Pasca Sarjana Sistem Informasi STMIK LIKMI Bandung serta mengikuti Program Doktoral Teknologi Informasi dan Komunikasi di UTeM Melaka Malaysia. Penulis aktif menjadi editor board dan reviewer jurnal nasional dan internasional terakreditasi Sinta serta aktif dalam menulis artikel di jurnal nasional maupun internasional serta menulis buku. Selain itu pula penulis aktif sebagai pengurus bidang kerjasama industri pada organisasi APTIKOM Prov. Jabar, sebagai sekretaris DPW Jawa Barat pada Ikatan Ahli Informatika Indonesia (IAII) sebagai Dewan Pengawas pada organisasi Perkumpulan Auditor Teknologi Informasi dan Komunikasi Indonesia (PASTIKINDO). Penulis memiliki kompetensi Information Technology Expert Auditor, ICT Project Manager, System Analyst dan Assesor Of Competency dari BNSP.

BIODATA PENULIS

Anindya Khrisna Wardhani, S.Kom., M.Kom.,
Dosen pada Program Studi Rekam Medis dan Informasi Kesehatan pada Politeknik Rukun Abdi Luhur, Kudus, Jawa Tengah

Anindya Khrisna Wardhani, S.Kom., M.Kom., lahir di Kudus, Jawa Tengah pada tanggal 15 Agustus 1994. Saat ini penulis merupakan dosen pada Program Studi Rekam Medis dan Informasi Kesehatan pada Politeknik Rukun Abdi Luhur, Kudus, Jawa Tengah. Penulis menyelesaikan Program Sarjana Teknik Informatika di Fakultas Ilmu Komputer Universitas Dian Nuswantoro (Udinus) Semarang tahun 2016. Semangat untuk terus belajar itu membuat penulis terpilih sebagai penerima Beasiswa Unggulan Masyarakat Berprestasi Kementerian Pendidikan dan kebudayaan RI pada Program Magister Sistem Informasi di Universitas Diponegoro (Undip) Semarang dan selesai pada tahun 2018.

BIODATA PENULIS

Arip Solehudin, S.Kom., M.Kom.
Dosen Program Studi Informatika
Fakultas Ilmu Komputer Universitas Singaperbangsa Karawang

Penulis lahir di Ciamis tanggal 16 April 1989. Penulis adalah dosen tetap pada Program Studi Informatika Fakultas Ilmu Komputer, Universitas Singaperbangsa Karawang. Menyelesaikan pendidikan S1 pada Jurusan Teknik Informatika dan melanjutkan S2 pada Jurusan Ilmu Komputer. Saya tertarik untuk menulis buku ini karena ingin berbagi pengetahuan dan pengalaman saya tentang perangkat keras physical layer dengan pembaca. Saya percaya bahwa pemahaman yang baik tentang perangkat keras physical layer merupakan landasan yang penting dalam mengelola jaringan komputer yang andal dan efisien. Saya berharap tulisan saya dapat memberikan manfaat dan wawasan bagi pembaca dalam memahami, mengimplementasikan, dan mengelola perangkat keras physical layer.

Publikasi Lainnya: Selain menulis buku ini, saya juga telah berkontribusi dalam beberapa artikel dan publikasi di bidang jaringan komputer. Artikel-artikel tersebut fokus pada topik-topik

terkait ilmu komputer dan bisa diakses melalu url https://scholar.google.co.id/citations?user=7-2kneIAAAAJ&hl .

BIODATA PENULIS

Azhari Ali Ridha
Dosen Tetap Fakultas ilmu komputer Universitas Asahan

Penulis lahir di Karawang, 15 September 1980. Sekolah Dasar Negeri Darma bhakti 1 Tamat Tahun 1992 di Medan. Melanjutkan Sekolah Menengah Pertama SMPN 2 karawang barat Tamat Tahun 1995 di Medan. Selanjutnya Sekolah Menengah Atas Nasional 3 karawang barat Tamat Tahun 1998. Selanjutnya Masuk Fakultas ilmu komputer Universitas Gunadarma Tahun 1998 dan Lulus Tahun 2003 di Jakarta. Melanjutkan Pasca Sarjana Universitas Gunadarma Magister manajemen sistem iinformasi di jakarta Tahun 2014 dan Lulus Tahun 2019.

Sejak Menjadi Mahasiswa, Penulis Banyak Mendapatkan Pengalaman Terutama Dari Organisasi Mahasiswa periode 2000-2004.

Setelah Tamat Dari Fakultas ilmu komputer Universitas Gunadarma Tahun 2003 berpengalaman bekerja di Perusahaan pembiayaan Suzuki finance Indonesia dan sebagai broadband operation center di PT Telkom indonesia dan Beralih Menjadi Dosen Tetap Fakultas ilmu komputer Universitas Singaperbangsa karawang Sejak Tahun 2008 Sampai Sekarang. Penulis Memperoleh Sertifikasi Dosen Sejak Tahun 2022 Sampai Sekarang. Selama Menjadi Dosen Tetap Fakultas ilmu komputer Universitas Asahan. Penulis Pernah Menduduki Jabatan Mulai Kepala

laboratorium Fakultas ilmu komputer 2021-2022, Ketua Prodi Manajemen 2022-sekarang, Sebagai Dosen Penulis Juga Aktif Pada Asosiasi perguruan tinggi komputer (APTIKOM) Sejak Tahun 2012 Sampai Saat Ini.

BIODATA PENULIS

Suwito Pomalingo, S.Kom., M.Kom.
Dosen Program Studi Informatika
Fakultas Teknik dan Informatika
Universitas Multimedia Nusantara

Penulis adalah dosen tetap pada Program Studi Informatika Fakultas Teknik dan Informatika Universitas Multimedia Nusantara. Menyelesaikan pendidikan S1 pada Jurusan Teknik Informatika dan melanjutkan S2 pada Program Magister Informatika Universitas Islam Indonesia.

Saat ini sementara menyelesaikan studi Doktoral dengan topik penelitian di bidang Security Science dengan pendekatan Deep Learning. Penulis menekuni bidang keilmuan meliputi Cyber Security, Malware Analytics, Data Science, Machine Learning, dan Deep Learning, selain itu, penulis juga memiliki beberapa serifikasi internasional di bidang Cyber Security, Digital Forensics, Data Science dan Machine Learning.

BIODATA PENULIS

Arief Yanto Rukmana, S.T., M.M.
Mahasiswa Doktoral Universitas Pendidikan Indonesia
Dosen Perguruan Tinggi Indonesia Mandiri Bandung
Dosen Universitas Nurtanio Bandung

Penulis sebelumnya telah memegang posisi penting di sejumlah bisnis yang beroperasi pada skala nasional dan dunia. penulis saat ini berprofesi sebagai praktisi bisnis (Pemilik Perusahaan di Bidang Fashion, Kuliner dan Bisnis Digital juga sebagai seorang akademisi. Penulis mengajar di Universitas Nurtanio Bandung, dan dosen tetap di perguruan tinggi indonesia mandiri (STMIK IM & STIE STAN IM). alumni dari Program Studi Informatika (S1) Sekolah Tinggi Manajemen Informatika dan Komputer Indonesia Mandiri (STMIK IM), Program Magister Manajemen (S2) di Pasca Sarjana Universitas Widyatama dan sedang melanjutkan studi Pendidikan (S3) Program Doktoral Pendidikan Teknologi dan Vokasional di Universitas Pendidikan Indonesia. Penulis aktif sebagai pembicara dan narasumber kewirausahaan digital juga berdedikasi sebagai praktisi bisnis / owner / pemilik beberapa perusahaan yang bergerak pada industri food, fashion and fun. serta aktif dalam organisasi nasional maupun internasional. Penulis juga seorang profesional dalam bidang public

speaking & sebagai asesor kompetensi digital dan instruktur berpengalaman untuk sertifikasi kompetensi SKKNI BNSP Digital Marketing, Social Media Marketing dan Metodologi Pelatihan Level III, Graphic Design serta Sertifikasi Kompetensi beberapa lainnya yang diselenggarakan dinas tenaga kerja kota bandung, PT Rice INTI dan Balai Besar Pengembangan Latihan Kerja (BBPLK) Bandung. Selain itu pula penulis produktif sebagai pendamping UMKM dan pengelola Inkubator Bisnis Perguruan Tinggi Indonesia Mandiri dengan membina dan melatih / coaching, mentoring serta melakukan pendampingan bisnis UMKM / Start UP untuk mahasiswa yang berminat menjadi seorang Entrepreneur / Technopreneurship tangguh yang mampu berdayasaing pada kancah internasional.

BIODATA PENULIS

Angga Aditya Permana
Dosen Informatika
Universitas Multimedia Nusantara

Angga Aditya Permana (lahir pada Desember 1989 di Jakarta) seorang dosen full time di bidang Computer Science pada Universitas Multimedia Nusantara sejak tahun 2021, fokus penelitian pada kriptografi, steganografi serta keamanan computer, namun pada tahun 2021 sedang mendalami topik bioinformatika dan network science. Angga juga memiliki hobi yaitu touring dan juga bermain bulutangkis, saat ini sedang menjadi mahasiswa program doctoral pada IPB University. Memulai karir pertama kali sebagai Network Enginner tahun 2011 dan memulai profesinya sebagai dosen pada 2013 di kampus swasta yang ada di Jakarta, pernah juga mengajar di kampus negri yang berada di Jakarta dan Tangerang, juga pernah di undang menjadi dosen tamu untuk mengenalkan Bioinformatika di kampus negeri di Jakarta. Terimakasih..

BIODATA PENULIS

Dr. Abdurohim, SE, MM.
Dosen Lektor pada Universitas Jenderal Achmad Yani, Cimahi, Jawa Barat

Kelahiran Cirebon (Jawa Barat) 12 April 1964, berkecimpung sebagai praktisi Perbankan selama 31 tahun pada PT. Bank Papua, dengan jabatan terakhir *Vice President* pada Divisi Perencanaan Strategis (Renstra).

Keahlian yang dimiliki adalah Audit Perbankan, Perencanaan Strategis, Pemasaran, *Manajemen Human Capital,* Penyusunan BPP & SOP dan Struktur Organisasi Perusahaan Perbankan.

Pendidikan Doktor (S3) Ilmu Manajemen dari Universitas Cendrawasih (2017), Pendidikan Magister Manajemen (S2)-Manajemen Keuangan, dari Universitas Hasanudin (2003), dan Pendidikan Sarjana (S1) Manajemen Keuangan & Perbankan dari STIE YPKP Bandung (1989). Saat ini sebagai pengajar/dosen Lektor pada Universitas Jenderal Achmad Yani, Cimahi, Jawa Barat.

Telah menyelesaikan penulisan buku (Kolaborasi) sebanyak: 86 buah *Book Chapter*, dan 3 buku Penulis tunggal.

E-Commerce (Strategi dan Inovasi Bisnis berbasis Digital), Analisa Laporan Keuangan, Anggaran Operasional Perusahaan

Manufaktur, Bank dan lembaga Keuangan Lainnya, Etika Bisnis Suatu Pengantar, HRM in Industry 5.0, Isu-Isu Kontemporer Akuntansi Manajemen, Kesehatan Lingkungan suatu pengantar, Knowledge Management, Marketing Tourism Service, Menakar Ekonomi masa pademi & New normal, New Normal Era Edisi II, Operations Management, Tantangan Pendidikan Indonesia di Masa depan, Teori dan Praktik Manajemen Bank Syariah Indonesia, The Art of Branding, Pasar Modal Syariah, Manajemen Pemasaran (Implementasi Strategi Pemasaran di Era Society 5.0). Perencanaan & Simulasi Bisnis, Manajemen Strategi, *Business Sustainability, eCommerce*, Mencari wajah pembangunan di Indonesia, *Business Intelligence, Digital Economy e Government,* Analisa Laporan Keuangan, Metode Penelitian Kualitatif, Pengantar Manajemen, Manajemen Konflik, Sistem Transaksi Keuangan, Kebijakan Perpajakan di Indonesia,. Keuangan Daerah (Perencanaan & Anggaran Daerah), Konsep dasar Akuntansi, *Financial Technology*, HRM: Perencanaan & Rekrutmen SDM

Telah mengikuti pendidikan/Lulus: Sekolah Pimpinan Bank (Sespibank), Sekolah Pemimpin Cabang, Manajemen Risiko level 4, Keuangan Berkelanjutan (SDGs).

Bersertifikat : Dosen Profesional (Serdos)

Telah mengikuti pendidikan/Lulus: Sekolah Pimpinan Bank (Sespibank), Sekolah Pemimpin Cabang, Manajemen Risiko level 4, Keuangan Berkelanjutan (SDGs).

Bersertifikat :Dosen Profesional (Serdos)

Anggota : *Project Management Office* Indonesia (POPI)

Email : Abdurrohim@mn.Unjani.ac.id

BIODATA PENULIS

Dr. Raimon Efendi,S.A.B,M.Kom
Dosen Program Studi Teknologi Pendidikan
Fakultas Keguruan dan Ilmu Pendidikan
Universitas Dharmas Indonesia

Dr. Raimon Efendi. S.A.B., M.Kom., lahir tanggal 10 September 1983, sejak tahun 2012 menjadi dosen di Universitas Dharmas Indonesia. Pendidikan S1 Jurusan Ilmu Administrasi Bisnis, Fakultas Ilmu Sosial dan Ilmu Politik Universitas Terbuka, S2 Jurusan Sistem Informasi, Fakultas Ilmu Komputer di Universitas Putra Indonesia 'YPTK' Padang dan S3 Jurusan program studi Pendidikan Teknologi dan Kejuruan Fakultas Teknik Universitas Negeri Padang. Memiliki kepakaran dalam bidang Entrepreneurship, Teknologi Informatika, dan Teknologi Pendidikan Kejuruan. Telah melakukan penemuan-penemuan bidang Entrepreneurship, Pendidikan Teknologogi dan kejuruan terutama pada model-model pembelajaran berbasis IT dan pelatihan Kewirausahaan. Saat ini penulis aktif mengelola Usaha di Bidang Teknologi Informatika dan aktif meneliti dan menulis sebagai wujud sumbangsih keilmuan bagi perkembangan pendidikan Bangsa Indonesia di era digital. Moto: Upgrade Your Skill, Upgrade your Life

BIODATA PENULIS

Bambang Suprayogi, S.E., M.Si.
Dosen Program Studi Manajemen Informatika
Politeknik Lembaga Pendidikan Dan Pengembangan Profesi Indonesia Bandung

Penulis adalah dosen tetap pada Program Studi Manajemen Informatika Politeknik Lembaga Pendidikan Dan Pengembangan Profesi Indonesia Bandung. Alumni SMAN 20 Bandung dan menyelesaikan pendidikan S1 pada Jurusan Manajemen di Jakarta dan melanjutkan S2 pada Jurusan Ilmu Administrasi di Jakarta. Penulis menekuni bidang Manajemen dan Computer Science dengan keahlian bidang Database Developer, Full Stack Developer, Network Operation System and Internet Cisco Certified Network Associate, Net Programming, Java and Android Programming.

BIODATA PENULIS

Shah Khadafi, S.Kom., M.Kom.
Dosen Program Studi Sistem Informasi
Fakultas Teknik Elektro dan Teknologi Informasi

Penulis lahir di Surabaya tanggal 28 september 1983. Penulis adalah dosen tetap pada Program Studi Sistem Informasi Fakultas Teknik Elektro dan Teknologi Informasi. Menyelesaikan pendidikan S1 pada Jurusan Sistem Komputer dan melanjutkan S2 pada Jurusan Teknologi Informasi. Penulis menekuni bidang keilmuan Artificial Intelligence, jaringan komputer, dan keamanan sistem informasi dan teknologi informasi. Berkarir sebagai dosen profesional, penulis pun aktif sebagai peneliti sesuai dengan bidang kepakarannya. Beberapa penelitian yang telah dilakukan baik itu didanai oleh internal perguruan tinggi ataupun didanai oleh Kemenristek DIKTI. Hasil dari penelitian, penulis melakukan beberapa publikasi baik pada buku, jurnal, prosiding maupun book chapter. Harapan dari beberapa penelitai ndan publikasi dapat memberikan kontribusi yang bermanfaat bagi para pembacanya.