**MAKALAH**

**“KONSEP DASAR/TCP IP dan SUBNETTING”**

**Dosen Pembimbing :**

**Pak Andi Roy, S.kom., MM**

**Oleh :**

**Elvareta Yoseph**

**-16323030-**

**PROGRAM STUDI MANAJEMEN INFORMATIKA**

**POLITEKNIK NEGERI FAKKFAK**

**2024**

# KATA PENGANTAR

Puji syukur atas rahmat yang telah diberikan oleh Tuhan Yang Maha Esa sehingga Penulis dapat menyelesaikan makalah yang berjudul “Konsep Dasar/TCP IP dan Subnetting”. Makalah ini dibuat untuk memenuhi salah satu tugas mata kuliah Jaringan Komputer. Semoga makalah ini dapat bermanfaat bagi penulis maupun pembaca.

Dalam kesempatan ini, penulis mengucapkan terima kasih. Penulis menyadari bahwa makalah ini masih jauh dari sempurna. Oleh karena itu, penulis tidak menutup diri untuk semua kritik dan saran dari pembaca atas segala kekurangannya.

Fakfak, 22 Mei 2024

Penulis

# DAFTAR ISI

[KATA PENGANTAR ii](#_Toc167313742)

[DAFTAR ISI iii](#_Toc167313743)

[BAB I PENDAHULUAN 2](#_Toc167313744)

[A. Latar Belakang 2](#_Toc167313746)

[B. Rumusan Masalah 2](#_Toc167313747)

[C. TUJUAN 2](#_Toc167313748)

[BAB II PEMBAHASAN 3](#_Toc167313749)

[A. OSI Layer 3](#_Toc167313751)

[B. Protocol dan Port 6](#_Toc167313752)

[C. Mac Address 9](#_Toc167313753)

[D. IP Address 11](#_Toc167313754)

[E. Subnetting 14](#_Toc167313755)

[F. Cara Melihat IP dan MAC pada Komputer. 18](#_Toc167313756)

[BAB III PENUTUP 21](#_Toc167313757)

[A. Kesimpulan 21](#_Toc167313759)

[B. Saran 21](#_Toc167313760)

[DAFTAR PUSTAKA 22](#_Toc167313761)

# BAB I

# PENDAHULUAN

## Latar Belakang

TCP/IP protokol adalah jaringan dengan teknologi “packet Switching “ yang berasal dari proyek DARPA ( development of Defense Advanced Research Project Agency ) ditahun 1970-an yang dikenal dengan nama ARPANET.TCP/IP sendiri sebenarnya merupakan suite dari gabungan beberapa protokol. Di dalamnya terdapat protokol TCP, IP, SMTP, POP, dan sebagainya. Sehingga dibutuhkan suatu standart yang dapat menjelaskan bagaimana proses bekerja.

Dalam IP Address juga dikenal sebuah istilah subnetting yang bertujuan untuk membagi jaringan kedalam subnet – subnet sehingga memudahkan dalam pembagian network dan pengontrolan dari sebuah jaringan. Subnetting merupakan teknik memecah network menjadi beberapa subnetwork yang lebih kecil dengan cara mengorbankan bit Host ID pada subnet mask untuk dijadikan Network ID baru.

## Rumusan Masalah

1. Apakah pengertian dari TCP/ IP ?
2. Apakah pengertian dari Protocol dan Port?
3. Apakah pengertian dari Mac Address?
4. Apakah pengertian dari IP Address?
5. Apakah pengertian dari Subnetting?
6. Bagaimana cara melihat IP dan MAC pada computer?

## TUJUAN

1. Agar pembaca mengetahui lebih dalam apa itu TCP/IP, Protocol dan Port, Mac Address, IP Address, Subnetting
2. Agar pembaca dapat mengetahui cara melihat IP dan MAC pada computer

# BAB II

# PEMBAHASAN

## OSI Layer

Lapisan OSI atau OSI Layer adalah sebuah konsep yang menentukan standar komunikasi dalam suatu jaringan komputer. OSI Layer membuat perangkat, misalnya komputer, dapat berkomunikasi satu sama lain sesuai protokol. Dengan OSI Layer, pengguna bisa dengan mudah mengirimkan pesan dari perangkat satu ke perangkat lainnya, misalnya mengirimkan sebuah email.

1. **Sejarah OSI Layer**

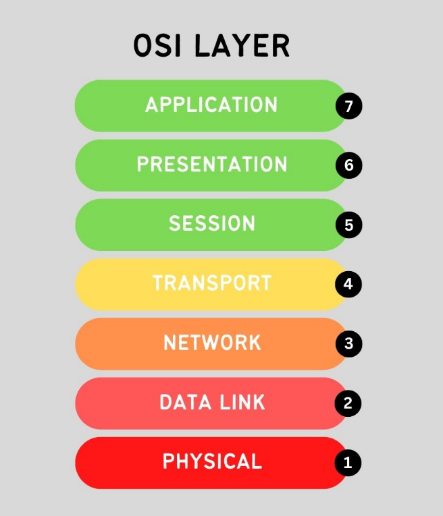
Lapisan OSI atau OSI Layer adalah sebuah konsep yang menentukan standar komunikasi dalam suatu jaringan komputer. OSI Layer membuat perangkat, misalnya komputer, dapat berkomunikasi satu sama lain sesuai protokol. Dengan OSI Layer, pengguna bisa dengan mudah mengirimkan pesan dari perangkat satu ke perangkat lainnya, misalnya mengirimkan sebuah email.

1. **Fungsi OSI Layer**

Setiap lapisan dalam model OSI memiliki fungsi spesifik dan berinteraksi dengan lapisan di atas dan di bawahnya. Data yang dikirimkan oleh suatu aplikasi akan melalui setiap lapisan, dimulai dari lapisan aplikasi hingga lapisan fisik, sebelum dikirimkan melalui media jaringan. Di sisi penerima, data tersebut akan melalui lapisan-lapisan tersebut secara terbalik, dari lapisan fisik hingga lapisan aplikasi.

Contoh aliran data dalam model OSI:

1. Lapisan Aplikasi : Aplikasi pengguna mengirimkan data.
2. Lapisan Presentasi : Data dikonversi, dienkripsi, atau dikompresi.
3. Lapisan Sesi : Sesi komunikasi dibentuk.
4. Lapisan Transport : Data dibagi menjadi segmen dan kontrol kesalahan ditambahkan.
5. Lapisan Jaringan : Paket data diberi alamat IP dan dirutekan.
6. Lapisan Data Link : Frame data diberi alamat MAC dan dipersiapkan untuk transmisi.
7. Lapisan Fisik : Bit data ditransmisikan melalui media fisik.
8. **7 Lapisan OSI Layer**

****

1. Physical Layer (Lapisan Fisik)

* Fungsi : Menangani transmisi bit mentah melalui media fisik jaringan. Lapisan ini bertanggung jawab untuk aspek fisik dari transmisi data seperti kabel, konektor, voltase, dan frekuensi sinyal.
* Contoh : Ethernet, USB, DSL.

1. Data Link Layer (Lapisan Data Link)

* Fungsi : Menyediakan metode pengiriman data yang bebas kesalahan antara dua perangkat yang terhubung langsung. Lapisan ini menangani alamat fisik (alamat MAC) dan pengontrolan akses media.
* Contoh : Ethernet, PPP (Point-to-Point Protocol), Switch.

1. Network Layer (Lapisan Jaringan)

* Fungsi : Menangani pengalamatan logis dan penentuan rute (routing) data dalam jaringan. Lapisan ini bertanggung jawab untuk mengirimkan paket dari sumber ke tujuan melalui berbagai jaringan.
* Contoh : IP (Internet Protocol), ICMP (Internet Control Message Protocol), Router.

1. Transport Layer (Lapisan Transport)

* Fungsi : Menyediakan transfer data end-to-end yang reliabel dan pengontrolan kesalahan. Lapisan ini memastikan bahwa data yang dikirimkan tiba dengan benar dan dalam urutan yang benar.
* Contoh : TCP (Transmission Control Protocol), UDP (User Datagram Protocol).

1. Session Layer (Lapisan Sesi)

* Fungsi : Mengatur dan mengontrol koneksi antara aplikasi. Lapisan ini bertanggung jawab untuk pembentukan, pengelolaan, dan terminasi sesi komunikasi.
* Contoh : NetBIOS, RPC (Remote Procedure Call).

1. Presentation Layer (Lapisan Presentasi)

* Fungsi : Mengatur konversi data, enkripsi, dan kompresi. Lapisan ini bertanggung jawab untuk memastikan bahwa data yang dikirim oleh aplikasi diubah ke format yang dapat dimengerti oleh lapisan aplikasi penerima.
* Contoh : SSL/TLS (Secure Sockets Layer/Transport Layer Security), JPEG, ASCII.

1. Application Layer (Lapisan Aplikasi)

* Fungsi : Menyediakan layanan jaringan untuk aplikasi pengguna. Lapisan ini bertanggung jawab untuk interaksi dengan aplikasi perangkat lunak yang membutuhkan akses ke jaringan.
* Contoh : HTTP (HyperText Transfer Protocol), FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol).

1. **Contoh aliran data dalam model OSI**

Setiap lapisan dalam model OSI memiliki fungsi spesifik dan berinteraksi dengan lapisan di atas dan di bawahnya. Data yang dikirimkan oleh suatu aplikasi akan melalui setiap lapisan, dimulai dari lapisan aplikasi hingga lapisan fisik, sebelum dikirimkan melalui media jaringan. Di sisi penerima, data tersebut akan melalui lapisan-lapisan tersebut secara terbalik, dari lapisan fisik hingga lapisan aplikasi.

Contoh aliran data dalam model OSI:

1. Lapisan Aplikasi : Aplikasi pengguna mengirimkan data.
2. Lapisan Presentasi: Data dikonversi, dienkripsi, atau dikompresi.
3. Lapisan Sesi : Sesi komunikasi dibentuk.
4. Lapisan Transport: Data dibagi menjadi segmen dan kontrol kesalahan ditambahkan.
5. Lapisan Jaringan : Paket data diberi alamat IP dan dirutekan.
6. Lapisan Data Link : Frame data diberi alamat MAC dan dipersiapkan untuk transmisi.
7. Lapisan Fisik : Bit data ditransmisikan melalui media fisik.
8. **Manfaat Model OSI**
9. Standarisasi: Menyediakan kerangka kerja standar untuk mengembangkan dan memahami berbagai protokol jaringan.
10. Interoperabilitas: Memungkinkan perangkat dan sistem yang berbeda untuk bekerja sama dengan lancar.
11. Modularitas: Memungkinkan pengembangan dan pemeliharaan jaringan yang lebih mudah dengan memisahkan fungsi jaringan menjadi lapisan-lapisan terpisah.
12. Pemecahan Masalah: Memudahkan identifikasi dan pemecahan masalah jaringan dengan memisahkan berbagai fungsi ke dalam lapisan yang berbeda.

## Protocol dan Port

Protokol dan port merupakan dua elemen penting yang memungkinkan perangkat yang berbeda untuk berkomunikasi satu sama lain secara efisien dan aman. Protokol menentukan aturan dan format komunikasi data, sementara port digunakan untuk mengidentifikasi layanan atau aplikasi tertentu pada perangkat jaringan.

1. **Jenis- Jenis Port**
2. Logical Port (Port Non-Fisik)

* Well-known port : berkisar dari 0 – 1023. Ini merupakan port yang dikenali atau port sistem. Port ini selalu merepresentasikan layanan jaringan yang sama dan ditetapkan oleh IANA.
* Registered port : berkisar dari 1024 – 49151. Port ini diketahui dan terdaftar di IANA tetapi tidak dialokasikan secara permanen, sehingga dapat menggunakan port number yang sama.
* Dynamically assigned port : berkisar dari 49152 – 65535. Port ini ditetapkan oleh sistem operasi atau aplikasi yang digunakan untuk melayani request dari pengguna sesuai dengan kebutuhan.

1. Physical Portr (Port Fisik)

* Serial Port : Serial port berfungsi untuk mentransmisikan data jarak jauh secara lambat. Sesuai namanya, serial port bekerja secara seri. Jadi, port ini tidak dapat melakukan pemindahan data sekaligus. Penggunaan port serial sudah banyak ditinggalkan dan telah digantikan dengan port USB dan Firewire. Contoh penggunaannya pada keyboard, mouse, monitor, dan modem dial-up.



* Paralel Port : Port paralel digunakan untuk mentransmisikan data pada jarak pendek secara cepat. Pemindahan data dapat dilakukan secara bersamaan sehingga informasi yang terkirim lebih banyak dibandingkan serial port. Jenis ini biasa dipakai pada penghubung perangkat printer, disk external, atau tape magnetik.



* SCSI (Small Computer System Interface) : Port SCSI berguna untuk mentransmisikan data secara cepat, bahkan bisa dipakai untuk menghubungkan tujuh alat sekaligus atau disebut dengan daisy chain.



* USB Port : USB port mampu mentransmisikan data hingga 127 periferal dalam rangkaian daisy chain. Banyak perangkat keras yang bisa dihubungkan melalui port USB, misalnya media penyimpanan USB flashdisk, printer, scanner, optical disk drive eksternal, dan sebagainya.



1. **Protokol Jaringan**
2. HTTP (HyperText Transfer Protocol)

* Port : 80
* Fungsi : Protokol utama untuk mengakses dan mengirimkan halaman web di internet. HTTP bekerja pada lapisan aplikasi model OSI.

1. HTTPS (HTTP Secure)

* Port : 443
* Fungsi : Versi aman dari HTTP yang menggunakan enkripsi SSL/TLS untuk melindungi data selama transmisi.

1. FTP (File Transfer Protocol)

* Port : 21
* Fungsi : Digunakan untuk transfer file antara klien dan server. FTP menyediakan fungsi untuk mengunggah dan mengunduh file.

1. SMTP (Simple Mail Transfer Protocol)

* Port : 25
* Fungsi : Protokol untuk mengirim email dari klien email ke server email dan antara server email.

1. IMAP (Internet Message Access Protocol)

* Port : 143
* Fungsi : Protokol untuk mengakses email di server. IMAP memungkinkan sinkronisasi email antara klien dan server, sehingga email dapat diakses dari berbagai perangkat.

1. POP3 (Post Office Protocol version 3)

* Port : 110
* Fungsi: Protokol untuk mengunduh email dari server ke klien email. POP3 mengunduh email dan biasanya menghapusnya dari server, sehingga email tidak dapat diakses dari perangkat lain setelah diunduh.

1. DNS (Domain Name System)

* Port : 53
* Fungsi : Protokol yang menerjemahkan nama domain yang mudah dibaca manusia (seperti www.example.com) menjadi alamat IP yang digunakan oleh komputer untuk berkomunikasi.

1. DHCP (Dynamic Host Configuration Protocol)

* Port : 67/68
* Fungsi : Protokol yang secara otomatis mengalokasikan alamat IP dan informasi konfigurasi jaringan lainnya kepada perangkat di jaringan.

1. Telnet

* Port : 23
* Fungsi : Protokol untuk akses jarak jauh ke komputer atau perangkat jaringan melalui koneksi teks. Telnet tidak menyediakan enkripsi, sehingga rentan terhadap serangan keamanan.

1. SSH (Secure Shell)

* Port : 22
* Fungsi : Protokol untuk akses jarak jauh yang aman ke komputer atau perangkat jaringan melalui koneksi teks. SSH menyediakan enkripsi untuk melindungi data yang ditransmisikan.

1. SNMP (Simple Network Management Protocol)

* Port : 161/162
* Fungsi : Protokol untuk mengelola dan memantau perangkat jaringan. SNMP digunakan untuk mengumpulkan informasi tentang status dan kinerja perangkat jaringan.

1. NTP (Network Time Protocol)

* Port : 123
* Fungsi : Protokol untuk sinkronisasi waktu antara komputer dan perangkat jaringan lainnya.

## Mac Address

1. **Pengertian**

MAC address (Media Access Control address) adalah pengenal unik yang diberikan ke setiap antarmuka jaringan untuk komunikasi pada segmen jaringan fisik. Alamat ini digunakan dalam berbagai teknologi jaringan, termasuk Ethernet dan Wi-Fi, untuk mengidentifikasi perangkat dalam jaringan lokal. MAC address adalah komponen penting dalam pengoperasian jaringan komputer karena memungkinkan pengiriman data yang akurat antara perangkat.

1. **Fungsi MAC Address dalam Jaringan**

Fungsi MAC Address sendiri adalah untuk mengidentifikasi perangkat yang terhubung pada satu jaringan, contohnya Wi-Fi. Untuk itu, umumnya jaringan wireless dilengkapi dengan MAC Filtering demi keamanan. Hanya perangkat dengan MAC Address yang telah ditentukan sajalah, yang dapat mengakses jaringan wireless tersebut. MAC address memainkan beberapa peran penting dalam jaringan komputer, terutama dalam lapisan Data Link (Lapisan 2) model OSI :

1. Identifikasi Perangkat

Setiap perangkat jaringan memiliki MAC address yang unik, memungkinkan identifikasi perangkat secara individual dalam jaringan.

1. Kontrol Akses Media

MAC address digunakan dalam proses kontrol akses media, membantu dalam pengaturan siapa yang dapat mengirim data pada saat tertentu untuk menghindari tabrakan data dalam jaringan.

1. Pengiriman Data Lokal

MAC address digunakan untuk pengiriman data dalam segmen jaringan lokal (LAN). Ketika perangkat ingin berkomunikasi dalam LAN, data yang dikirimkan mengandung alamat MAC tujuan.

1. Resolusi Alamat (ARP)

Protokol ARP (Address Resolution Protocol) digunakan untuk memetakan alamat IP ke MAC address. Ketika perangkat mengetahui alamat IP tujuan tetapi tidak tahu MAC address-nya, ARP akan membantu dalam menemukan alamat MAC yang sesuai.

1. **Struktur dan Format MAC Address**
2. Struktur MAC Address

* Organizationally Unique Identifier (OUI)
* Terdiri dari 24 bit pertama (3 byte).
* Mengidentifikasi produsen atau organisasi yang mengeluarkan alamat MAC.
* Ditentukan oleh IEEE.
* Network Interface Controller (NIC) Specific
* Terdiri dari 24 bit terakhir (3 byte).
* Ditentukan oleh produsen untuk memberikan identifikasi unik kepada setiap perangkat yang mereka buat.

1. Format MAC Address

MAC address terdiri dari 48 bit (6 byte) yang biasanya dinyatakan dalam format heksadesimal. Alamat ini ditulis dalam salah satu dari dua format utama:

* Format Canonical (separasi titik dua): 00:1A:2B:3C:4D:5E
* Format Microsoft (separasi tanda hubung): 00-1A-2B-3C-4D-5E

## IP Address

IP address (Internet Protocol address) adalah pengenal numerik yang digunakan untuk mengidentifikasi perangkat dalam jaringan komputer. Alamat IP memungkinkan perangkat untuk berkomunikasi satu sama lain melalui jaringan yang berbeda, termasuk internet.

1. **Fungsi IP Address**
2. Menghubungkan perangkat ke jaringan internet

fungsi IP address yang utama yaitu menghubungkan setiap perangkat (device) ke jaringan internet sehingga memudahkan proses komunikasi di dalam jaringan komputer. Dengan memiliki IP address, setiap perangkat yang menggunakan internet dapat terhubung satu sama lain. Sehingga antar perangkat bisa saling berkomunikasi.

1. Menunjukkan identitas perangkat

IP Address juga disebut sebagai identitas perangkat dalam jaringan internet. Sebuah perangkat dapat teridentifikasi dari alamat IP-nya. Pemilik situs atau pada jaringan WiFi publik dapat mengetahui alamat-alamat IP yang mengaksesnya.

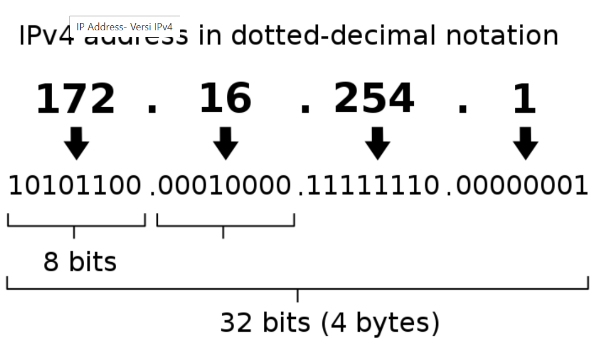
1. Mengidentifikasi host atau interface

Setiap kali perangkat melakukan permintaan akses website, server website akan langsung melakukan screening untuk mengidentifikasi IP address yang akan masuk.Jika IP address tersebut dirasa aman, maka server akan memberikan akses untuk dapat mengakses website tersebut. Sebaliknya, jika host tersebut mengandung ancaman, maka server secara otomatis akan menolak permintaan tersebut.

1. Sebagai alamat pengiriman data ke perangkat

IP Address berfungsi sebagai alamat pengiriman data ke perangkat. Ketika kamu mengakses sebuah website sebenarnya terjadi proses pengunduhan yang dilakukan oleh perangkat terhadap data yang dikirim dari website tersebut. Proses itu dapat terjadi karena adanya IP Address sebagai alamat pengiriman data.

1. **Bagian-Bagian IP Address**
2. Network ID. Network ID adalah identitas sebuah jalur dalam jaringan. Dalam hal ini, Network ID berfungsi untuk menunjukkan di jaringan mana sebuah device berada.
3. Host ID. ID Host adalah identitas dari host (interface router, workstation, dan device) yang terhubung ke jaringan. Perannya untuk mengidentifikasi host dalam suatu jaringan. Seluruh host yang ada akan tersambung dalam jaringan yang sama, yakni jaringan yang memiliki Network ID yang sama.
4. **Versi IP Address**
5. IPv4 (Internet Protocol version 4)



IPv4 adalah versi alamat IP yang paling umum digunakan, terdiri dari 32 bit yang biasanya dinyatakan dalam format desimal yang dipisahkan oleh titik (dot-decimal notation). Contoh: 192.168.1.1.

* Struktur: IPv4 dibagi menjadi empat oktet, masing-masing terdiri dari 8 bit.
* Contoh: 192.168.1.1 -> 11000000.10101000.00000001.00000001 (biner)
* Rentang: IPv4 dapat menyediakan sekitar 4,3 miliar alamat unik (2^32 alamat).
* Kelas Alamat :
* Kelas A: 0.0.0.0 hingga 127.255.255.255
* Kelas B: 128.0.0.0 hingga 191.255.255.255
* Kelas C: 192.0.0.0 hingga 223.255.255.255
* Kelas D: 224.0.0.0 hingga 239.255.255.255 (digunakan untuk multicast)
* Kelas E: 240.0.0.0 hingga 255.255.255.255 (cadangan untuk penggunaan masa depan)

1. IPv6 (Internet Protocol version 6)

IPv6 adalah versi alamat IP yang lebih baru, dikembangkan untuk mengatasi keterbatasan IPv4. IPv6 menggunakan 128 bit untuk alamat, yang biasanya dinyatakan dalam format heksadesimal yang dipisahkan oleh titik dua (colon-separated notation). Contoh: 2001:0db8:85a3:0000:0000:8a2e:0370:7334.

* Struktur: IPv6 dibagi menjadi delapan grup, masing-masing terdiri dari 16 bit.
* Contoh: 2001:0db8:85a3:0000:0000:8a2e:0370:7334
* Rentang: IPv6 dapat menyediakan sekitar 3.4×10^38 alamat unik (2^128 alamat).
* Keunggulan IPv6 :
* Ruang Alamat Lebih Besar : Mengatasi keterbatasan alamat IPv4.
* Konfigurasi Otomatis : Mendukung autokonfigurasi stateless melalui Neighbor Discovery Protocol (NDP).
* Keamanan yang Lebih Baik : Dukungan wajib untuk IPsec (Internet Protocol Security).
* Rute Lebih Efisien : Simplicity dalam header yang mengurangi beban proses pada router.

1. **Jenis IP Address**
2. IP Publik

Jenis IP Publik menghubungkanmu dengan jaringan internet secara global. Cakupannya sangat luas dan digunakan oleh segala perangkat yang dipergunakan untuk umum. Pengguna IP Publik dapat mengakses internet karena jenis alamat IP inilah yang menghubungkan perangkat ke jaringan internet. Pengguna internet mendapatkan IP Publik melalui provider internet atau ISP (Internet Service Provider) yang digunakan.

1. IP Privat

IP Privat digunakan hanya untuk jaringan lokal. IP Privat biasanya digunakan untuk sistem jaringan lokal (LAN) seperti misalnya yang digunakan di perkantoran, hotel, dan lain-lain. Di setiap jaringan lokal, tiap perangkat yang tetap mempunyai alamat IP Privat tersendiri. Alamat IP Privat ini memungkinkan setiap perangkat dapat berkomunikasi satu dengan yang lainnya dalam lingkup lokal.

1. IP Dinamis

IP Dinamis dapat berubah sewaktu-waktu. Hal tersebut terjadi karena jumlah alamat IP yang kian menipis, maka penggunaannya pun bergantian. Jenis IP Dinamis biasanya digunakan untuk umum. Penyedia layanan internet (ISP) yang bertanggung jawab untuk mengatur alokasi pemberian alamat IP ke pelanggannya. Maka dari itu, alamat IP penggunanya dapat berubah sewaktu-waktu. Melakukan restart perangkat atau router internet juga dapat menyebabkan berubahnya alamat IP.

1. IP Statis

IP Statis tidak akan berubah-ubah. Penggunanya melakukan pemesanan khusus terhadap alamat IP kepada ISP dengan membayar sejumlah biaya. IP Statis biasanya digunakan oleh penyedia server, web hosting, ataupun lembaga penting yang sangat bergantung pada layanannya. ISP akan memberikan alamat IP Statis kepada pelanggan yang melakukan reservasi dan memastikan alamat IP tidak akan berubah.

1. Shared IP merupakan jenis alamat IP yang digunakan oleh beberapa domain/situs dalam satu server yang sama. Alamat IP jenis ini biasanya dipakai pada layanan shared hosting.
2. Dedicated IP

Jika Shared IP digunakan bersama-sama oleh beberapa domain dalam satu server, berbeda halnya dengan Dedicated IP. Jenis alamat IP Dedicated hanya digunakan oleh satu domain. Alamat IP jenis ini hanya dimiliki oleh satu domain/situs saja. Dengan menggunakan Dedicated IP, reputasi domain pengguna tidak terpengaruhi oleh domain lainnya. Dedicated IP umumnya digunakan oleh pengguna cloud VPS hosting dan pengguna dedicated hosting.

## Subnetting

Subnetting adalah proses membagi sebuah jaringan IP besar menjadi jaringan-jaringan IP yang lebih kecil yang disebut subnet. Subnetting membantu dalam manajemen jaringan, meningkatkan efisiensi penggunaan alamat IP, dan meningkatkan keamanan dan kinerja jaringan.

1. **Fungsi Subnetting**
2. Penghematan Alamat IP

Dengan menggunakan subnetting, kita dapat membagi jaringan besar menjadi subnet yang lebih kecil. Ini memungkinkan kita untuk menggunakan alamat IP secara lebih efisien dan menghindari pemborosan alamat IP yang terbatas. Tanpa subnetting, jika kita memiliki jaringan kecil dengan sedikit perangkat, kita harus mengalokasikan seluruh rentang alamat IP, yang bisa berarti banyak alamat IP terbuang percuma. Subnetting memungkinkan kita untuk mengalokasikan hanya jumlah alamat IP yang dibutuhkan untuk setiap subnet, mengurangi pemborosan.

1. Pengaturan Lalu Lintas Jaringan

Dengan menggunakan subnetting, lalu lintas jaringan dapat dibatasi pada tingkat subnet. Ketika perangkat di satu subnet ingin berkomunikasi dengan perangkat di subnet lain, lalu lintas harus melewati router. Ini memungkinkan administrator untuk mengatur kebijakan lalu lintas dan mengoptimalkan kinerja jaringan dengan mengarahkan lalu lintas hanya ke subnet yang relevan.

1. Keamanan Jaringan

Subnetting membantu meningkatkan keamanan jaringan dengan membatasi akses antara subnet yang berbeda. Komunikasi antara subnet harus melewati router, yang berfungsi sebagai penghalang untuk melindungi subnet dari ancaman luar atau perangkat yang tidak berwenang di subnet lain. Dengan cara ini, serangan dari dalam jaringan juga dapat diatasi dengan lebih baik.

1. Manajemen Jaringan yang Lebih Efisien

Subnetting memungkinkan administrator untuk mengorganisasi jaringan berdasarkan kebutuhan dan lokasi. Misalnya, dalam lingkungan kantor, departemen tertentu dapat ditempatkan dalam subnet yang terpisah untuk memfasilitasi manajemen dan pemeliharaan yang lebih mudah. Hal ini juga membantu dalam mendeteksi masalah dan membatasi dampaknya pada seluruh jaringan.

1. Skalabilitas Jaringan

Dengan membagi jaringan menjadi subnet, kita dapat dengan mudah menambahkan atau mengurangi perangkat dalam subnet tersebut tanpa mengubah struktur jaringan utama. Ini membuat jaringan lebih skalabel dan memudahkan perluasan jaringan tanpa harus merombak seluruh alamat IP yang ada.

1. **Tujuan Subnetting**
2. Optimalisasi Penggunaan Alamat IP

Salah satu tujuan utama subnetting adalah untuk mengoptimalkan penggunaan alamat IP yang terbatas. Dengan membagi jaringan besar menjadi subnet yang lebih kecil, administrator dapat mengalokasikan hanya jumlah alamat IP yang dibutuhkan untuk setiap subnet. Hal ini mengurangi pemborosan alamat IP dan memungkinkan lebih banyak perangkat terhubung ke jaringan tanpa kehabisan alamat IP.

1. Pengelolaan Jaringan yang Lebih Efisien

Subnetting memungkinkan administrator untuk mengatur dan mengelompokkan perangkat dalam jaringan berdasarkan kebutuhan dan lokasi. Hal ini membuat manajemen jaringan menjadi lebih mudah dan lebih efisien. Perangkat dalam satu subnet dapat dikelompokkan berdasarkan fungsi, departemen, atau lokasi fisik, sehingga memfasilitasi pemantauan, pemeliharaan, dan konfigurasi yang lebih terorganisir.

1. Pembatasan Lalu Lintas Jaringan

Dengan menggunakan subnetting, lalu lintas jaringan dapat dibatasi pada tingkat subnet. Komunikasi antar subnet harus melewati router, yang memungkinkan administrator untuk mengatur kebijakan lalu lintas dengan lebih tepat. Hal ini membantu mengurangi lalu lintas yang tidak perlu dan meningkatkan kinerja jaringan secara keseluruhan.

1. Keamanan Jaringan yang Lebih Baik

Subnetting membantu meningkatkan keamanan jaringan dengan membatasi akses antara subnet yang berbeda. Dengan menggunakan router sebagai perangkat penghubung antar subnet, serangan dari luar jaringan dapat dihalangi lebih efektif. Subnetting juga memungkinkan penggunaan firewall untuk mengatur kebijakan keamanan pada tingkat subnet yang lebih terkontrol.

1. Peningkatan Skalabilitas

Dengan membagi jaringan menjadi subnet, skala jaringan dapat ditingkatkan dengan lebih mudah dan lebih fleksibel. Penambahan perangkat dalam satu subnet tidak akan mempengaruhi subnet lainnya, sehingga memudahkan perluasan jaringan tanpa merombak seluruh struktur jaringan.

1. Efisiensi dalam Penyebaran Layanan

Dengan mengelompokkan perangkat yang memerlukan layanan khusus dalam satu subnet, administrator dapat menyediakan layanan secara lebih efisien dan terfokus pada subnet yang tepat.

1. **Proses Subnetting**

Proses Subnetting adalah langkah-langkah yang diikuti untuk membagi jaringan IP besar menjadi subnet-subnet yang lebih kecil. Berikut adalah langkah-langkah dalam proses subnetting:

1. Tentukan Jumlah Subnet yang Dibutuhkan

Pertama, tentukan berapa banyak subnet yang diperlukan untuk jaringan Anda. Jumlah subnet yang dibutuhkan akan ditentukan berdasarkan jumlah kelompok perangkat yang ingin dipisahkan dalam jaringan.

1. Tentukan Jumlah Host per Subnet

Setelah menentukan jumlah subnet, selanjutnya tentukan berapa banyak host yang diperlukan dalam setiap subnet. Hal ini akan membantu menentukan ukuran subnet yang tepat dan berapa banyak bit yang perlu dialokasikan untuk bagian host pada alamat IP.

1. Tentukan Jumlah Bit Borrowed

Setelah mengetahui jumlah host per subnet, hitung berapa banyak bit yang perlu dipinjam dari bagian host dalam alamat IP untuk mencukupi jumlah host yang diperlukan. Bit yang dipinjam akan diubah menjadi bagian subnet, sehingga menghasilkan lebih banyak subnet dengan jumlah host yang sesuai.

1. Tentukan Ukuran Subnet

Setelah menentukan jumlah bit yang dipinjam, tentukan ukuran subnet untuk setiap subnet yang dihasilkan. Ukuran subnet ditentukan oleh jumlah bit yang dipinjam dan menentukan rentang alamat IP yang valid untuk setiap subnet.

1. Tetapkan Alamat IP untuk Setiap Subnet

Dalam langkah ini, tentukan alamat IP untuk setiap subnet berdasarkan ukuran subnet yang ditentukan sebelumnya. Biasanya, alamat IP pertama dalam subnet digunakan sebagai alamat jaringan (network address), dan alamat IP terakhir digunakan sebagai alamat broadcast dalam subnet.

1. Tetapkan Alamat IP untuk Perangkat

Setelah menetapkan alamat IP untuk setiap subnet, selanjutnya tetapkan alamat IP untuk setiap perangkat dalam masing-masing subnet. Pastikan bahwa setiap perangkat memiliki alamat IP unik dalam subnetnya.

1. Konfigurasi Router dan Perangkat Jaringan

Terakhir, konfigurasi router dan perangkat jaringan sesuai dengan pengaturan subnetting yang telah ditentukan. Pastikan bahwa router dapat mengarahkan lalu lintas antar subnet dengan benar dan atur firewall atau kebijakan keamanan sesuai dengan kebutuhan.

1. **Klasifikasi Subnetting**

Subnetting dapat diklasifikasikan berdasarkan ukuran subnet dan jumlah host yang diperbolehkan dalam setiap subnet. Berikut adalah klasifikasi subnetting berdasarkan ukuran subnet:

1. Subnetting dengan Penggunaan Bit Borrowed yang Sama

* Classful Subnetting: Pada metode ini, subnetting dilakukan dengan menggunakan jumlah bit yang sama untuk setiap subnet dalam kelas jaringan tertentu. Sebagai contoh, dalam subnetting kelas C, biasanya digunakan 3 bit tambahan untuk subnetting, sehingga menghasilkan 8 subnet dengan 5 bit host.
* Variable Length Subnet Mask (VLSM): VLSM adalah teknik subnetting yang memungkinkan alokasi ukuran subnet yang berbeda untuk subnet-subnet yang berbeda dalam satu jaringan. Dengan menggunakan VLSM, administrator dapat mengalokasikan jumlah host yang sesuai untuk setiap subnet, mengoptimalkan penggunaan alamat IP secara efisien.

1. Subnetting dengan Ukuran Subnet yang Tetap

Fixed Length Subnet Mask (FLSM): FLSM adalah metode subnetting di mana setiap subnet memiliki ukuran subnet yang tetap dan sama. Misalnya, dalam subnetting kelas C, menggunakan 3 bit untuk subnetting akan selalu menghasilkan 8 subnet dengan 5 bit untuk host, tidak peduli seberapa banyak host yang dibutuhkan dalam setiap subnet. FLSM biasanya digunakan dalam lingkungan jaringan yang memerlukan pengaturan yang sederhana dan konsisten untuk setiap subnet.

1. Subnetting dengan Pemborosan IP Minimum

Classless Subnetting: Dalam metode ini, subnetting dilakukan tanpa memperhatikan pembagian kelas jaringan tradisional (kelas A, B, atau C). Subnetting berdasarkan kebutuhan sebenarnya dari setiap subnet untuk menghindari pemborosan alamat IP. Classless Subnetting umumnya mengacu pada penggunaan VLSM untuk mengalokasikan ukuran subnet yang tepat untuk setiap subnet dalam jaringan.

1. Subnetting dengan Pemborosan IP Maksimum

* Classful Subnetting: Classful Subnetting adalah metode subnetting yang didasarkan pada pembagian kelas jaringan tradisional (kelas A, B, atau C). Ini dapat menyebabkan pemborosan alamat IP karena setiap subnet harus menggunakan jumlah bit yang sama, terlepas dari jumlah host yang sebenarnya dibutuhkan.

## Cara Melihat IP dan MAC pada Komputer.

Untuk melihat IP dan MAC address pada komputer yang terhubung ke jaringan, Anda dapat menggunakan berbagai metode tergantung pada sistem operasi yang digunakan. Berikut ini adalah cara-cara untuk melihat IP dan MAC address pada sistem operasi Windows, macOS, dan Linux.

1. **Windows**
2. Menggunakan Command Prompt (CMD)

* Buka Command Prompt:
* Tekan tombol Windows + R, ketik cmd, dan tekan Enter.
* Lihat Alamat IP:
* Ketik ipconfig dan tekan Enter.
* Alamat IP akan ditampilkan di bawah "Ethernet adapter" atau "Wireless LAN adapter" sesuai dengan koneksi yang digunakan. Cari "IPv4 Address".
* Lihat Alamat MAC:
* Ketik ipconfig /all dan tekan Enter.
* Alamat MAC akan ditampilkan sebagai "Physical Address" di bawah adapter jaringan yang relevan.

1. Menggunakan Control Panel

* Buka Control Panel:
* Tekan tombol Windows + R, ketik control, dan tekan Enter.
* Navigasi ke Network and Sharing Center:
* Pilih "Network and Internet" > "Network and Sharing Center".
* Lihat Detail Koneksi:
* Klik pada nama koneksi yang sedang aktif (biasanya terlihat sebagai link).
* Klik tombol "Details".
* Di sini, Anda akan melihat alamat IP (IPv4 Address) dan alamat MAC (Physical Address).

1. **MacOS**
2. Menggunakan Terminal

* Buka Terminal:
* Pergi ke Applications > Utilities > Terminal, atau tekan Command + Space dan ketik Terminal, lalu tekan Enter.
* Lihat Alamat IP:
* Ketik ifconfig dan tekan Enter.
* Alamat IP akan ditampilkan di bawah antarmuka jaringan yang digunakan (biasanya en0 untuk Ethernet atau en1 untuk Wi-Fi).
* Lihat Alamat MAC:
* Ketik ifconfig dan tekan Enter.
* Alamat MAC akan ditampilkan di bawah antarmuka jaringan yang digunakan (sebagai ether).

1. Menggunakan System Preferences

* Buka System Preferences:
* Klik ikon Apple di pojok kiri atas layar dan pilih "System Preferences".
* Navigasi ke Network:
* Klik "Network".
* Pilih Koneksi Jaringan:
* Pilih koneksi jaringan yang sedang aktif (Wi-Fi atau Ethernet) dari daftar di sisi kiri.
* Lihat Alamat IP dan MAC:
* Untuk Wi-Fi, klik "Advanced" dan pergi ke tab "TCP/IP" untuk melihat alamat IP, dan ke tab "Hardware" untuk melihat alamat MAC.
* Untuk Ethernet, informasi ini biasanya langsung terlihat di tab "TCP/IP" dan "Hardware".

1. **Linux**
2. Menggunakan Terminal

* Buka Terminal:
* Bisa ditemukan di Applications > Accessories > Terminal, atau dengan menekan Ctrl + Alt + T.
* Lihat Alamat IP:
* Ketik ip addr show atau ifconfig dan tekan Enter.
* Alamat IP akan ditampilkan di bawah antarmuka jaringan yang digunakan (misalnya, eth0 untuk Ethernet atau wlan0 untuk Wi-Fi).
* Lihat Alamat MAC:
* Ketik ip addr show atau ifconfig dan tekan Enter.
* Alamat MAC akan ditampilkan di bawah antarmuka jaringan yang digunakan sebagai "link/ether".

1. **Menggunakan Alat Pihak Ketiga**

Selain metode bawaan dari sistem operasi, ada juga berbagai alat pihak ketiga yang dapat digunakan untuk melihat alamat IP dan MAC. Beberapa di antaranya adalah:

1. Advanced IP Scanner (Windows)
2. Angry IP Scanner (Windows, macOS, Linux)
3. Wireshark (Windows, macOS, Linux)

# BAB III

# PENUTUP

## Kesimpulan

TCP/IP (Transmission Control Protocol/Internet Protocol) adalah sekelompok protocol yang mengatur komunikasi data komputer di Internet. Komputer-komputer yang terhubung ke internet berkomunikasi dengan protocol ini. Karena menggunakan bahasa yang sama, yaitu protocol TCP/IP, perbedaan jenis komputer dan system operasi tidak menjadi masalah.. Karena berupa kumpulan protokol (protocol suite) maka Protokol ini tidaklah mampu berdiri sendiri.

Subnetting adalah teknik memecah suatu jaringan besar menjadi jaringan yang lebih kecil dengan cara mengorbankan bit Host ID pada subnet mask untuk dijadikan Network ID baru.

## Saran

Demikian sedikit ulasan mengenai “Konsep Dasar/TCP IP dan Subnetting”, mudah – mudahan materi yang saya sajikan ini dapat sedikit menambah wawasan bagi para pembaca umumnya dan bagi penyusun khususnya. Saya sadar bahwa yang saya sajikan ini masih sangat sederhana baik dalam cakupan materi makalah, metode penyusunan makalah dan lain – lain, kesalahan dan kekurangan tersebut dapat di jumpai pada makalah ini, oleh karenanya kritik dan saran sangat Saya butuhkan demi memperoleh kesempurnaan dalam menyusun materi berikutnya.

# DAFTAR PUSTAKA

<https://www.academia.edu/31678393/Makalah_TCP_IP_Fikri_Zakaria_Rahman>

<https://search.yahoo.com/search;_ylt=Awrg0drSx01mWR4BEidXNyoA;_ylc=X1MDMjc2NjY3OQRfcgMyBGZyA21jYWZlZQRmcjIDc2ItdG9wBGdwcmlkA1RRSUJQRG9LU0p1bEhMeGprTjlwakEEbl9yc2x0AzAEbl9zdWdnAzEEb3JpZ2luA3NlYXJjaC55YWhvby5jb20EcG9zAzAEcHFzdHIDBHBxc3RybAMwBHFzdHJsAzI1BHF1ZXJ5A2xhdGFyJTIwYmVsYWthbmclMjBzdWJuZXR0aW5nBHRfc3RtcAMxNzE2MzczNzM5?p=latar+belakang+subnetting&fr=mcafee&type=E210US885G0&fr2=sb-top&iscqry=>

<https://www.academia.edu/12163344/MAKALAH_JARINGAN_KOMPUTER_tentang_SUBNETTING>

<https://www.dewaweb.com/blog/pengertian-osi-layer/>

<https://www.dewaweb.com/blog/apa-itu-port/>

<https://codingstudio.id/blog/port-adalah/>

<https://kumparan.com/berita-terkini/pengertian-mac-address-dan-fungsinya-pada-jaringan-komputer-1ydONjymlmj/4>

<https://www.dewaweb.com/blog/pengertian-dan-jenis-ip-address/>

<https://dosenit.com/jaringan-komputer/subnetting>