

UTS JARINGAN KOMPUTER

1. Jaringan komputer adalah kumpulan dua atau lebih perangkat komputer yang saling terhubung untuk berbagi data dan sumber daya, seperti file, printer, atau koneksi internet. Jaringan ini memungkinkan komunikasi antar perangkat dalam area yang sama (seperti jaringan lokal atau LAN) maupun jarak jauh (seperti jaringan luas atau WAN).

2. OSI Layer (Open Systems Interconnection Layer) adalah model konseptual yang menguraikan bagaimana data dapat ditransfer dari satu perangkat ke perangkat lain dalam jaringan melalui lapisan-lapisan tertentu. OSI Layer terdiri dari 7 lapisan yang masing-masing memiliki fungsi tertentu untuk memudahkan komunikasi dan interoperabilitas antar perangkat dari berbagai vendor dan platform.

Berikut tujuh komponen OSI Layer beserta penjelasan nya :

- **Physical Layer (Lapisan Fisik)**

Lapisan pertama yang berfungsi untuk mengirimkan data dalam bentuk sinyal elektrik atau optik melalui media fisik (seperti kabel atau gelombang radio). Physical Layer menangani aspek fisik dari koneksi jaringan, seperti voltase, pin, kabel, dan topologi jaringan.

- · **Data Link Layer (Lapisan Data Link)**

Mengatur proses transfer data antar perangkat dalam jaringan yang sama, mendeteksi dan memperbaiki kesalahan yang terjadi pada Physical Layer. Data Link Layer juga mengatur pengalamatan perangkat pada jaringan lokal dengan menggunakan MAC Address.

- · **Network Layer (Lapisan Jaringan)**

Bertugas untuk menentukan jalur (routing) dan mengatur pengalamatan logis (seperti IP address) agar data dapat dikirim antar jaringan berbeda. Network Layer memastikan bahwa data mencapai tujuan akhir, bahkan jika melalui beberapa titik atau jaringan.

- · **Transport Layer (Lapisan Transport)**

Bertanggung jawab untuk memastikan pengiriman data antar aplikasi pada komputer yang berbeda dengan cara yang handal. Transport Layer mengontrol aliran data, fragmentasi, dan memastikan bahwa paket data

tiba tanpa kehilangan atau duplikasi. Contoh protokol di lapisan ini adalah TCP (Transmission Control Protocol) dan UDP (User Datagram Protocol).

- **Session Layer (Lapisan Sesi)**

Mengelola dan memelihara sesi atau koneksi antar aplikasi. Lapisan ini bertugas untuk membuka, mengelola, dan menutup sesi komunikasi antara perangkat-perangkat yang terhubung. Misalnya, jika terjadi kegagalan koneksi, Session Layer akan mencoba memulihkan sesi tersebut.

- **Presentation Layer (Lapisan Presentasi)**

Berfungsi sebagai penerjemah data yang akan dikirim atau diterima, memastikan data dapat dipahami oleh perangkat yang berbeda. Presentation Layer menangani enkripsi, dekripsi, dan kompresi data, sehingga menjaga keamanan dan efisiensi pengiriman.

- **Application Layer (Lapisan Aplikasi)**

Lapisan paling atas yang berhubungan langsung dengan aplikasi pengguna, seperti email, web browser, atau layanan transfer file. Application Layer menyediakan antarmuka bagi pengguna untuk berkomunikasi dengan perangkat jaringan, serta memproses permintaan layanan dari pengguna ke jaringan.

- **Physical Layer (Lapisan Fisik)**

Lapisan pertama yang berfungsi untuk mengirimkan data dalam bentuk sinyal elektrik atau optik melalui media fisik (seperti kabel atau gelombang radio). Physical Layer menangani aspek fisik dari koneksi jaringan, seperti voltase, pin, kabel, dan topologi jaringan.

- **Data Link Layer (Lapisan Data Link)**

Mengatur proses transfer data antar perangkat dalam jaringan yang sama, mendeteksi dan memperbaiki kesalahan yang terjadi pada Physical Layer. Data Link Layer juga mengatur pengalamatan perangkat pada jaringan lokal dengan menggunakan MAC Address.

- **Network Layer (Lapisan Jaringan)**

Bertugas untuk menentukan jalur (routing) dan mengatur pengalamatan logis (seperti IP address) agar data dapat dikirim antar jaringan berbeda. Network Layer memastikan bahwa data mencapai tujuan akhir, bahkan jika melalui beberapa titik atau jaringan.

- **Transport Layer (Lapisan Transport)**

Bertanggung jawab untuk memastikan pengiriman data antar aplikasi

pada komputer yang berbeda dengan cara yang handal. Transport Layer mengontrol aliran data, fragmentasi, dan memastikan bahwa paket data tiba tanpa kehilangan atau duplikasi. Contoh protokol di lapisan ini adalah TCP (Transmission Control Protocol) dan UDP (User Datagram Protocol).

- **Session Layer (Lapisan Sesi)**

Mengelola dan memelihara sesi atau koneksi antar aplikasi. Lapisan ini bertugas untuk membuka, mengelola, dan menutup sesi komunikasi antara perangkat-perangkat yang terhubung. Misalnya, jika terjadi kegagalan koneksi, Session Layer akan mencoba memulihkan sesi tersebut.

- **Presentation Layer (Lapisan Presentasi)**

Berfungsi sebagai penerjemah data yang akan dikirim atau diterima, memastikan data dapat dipahami oleh perangkat yang berbeda. Presentation Layer menangani enkripsi, dekripsi, dan kompresi data, sehingga menjaga keamanan dan efisiensi pengiriman.

- **Application Layer (Lapisan Aplikasi)**

Lapisan paling atas yang berhubungan langsung dengan aplikasi pengguna, seperti email, web browser, atau layanan transfer file. Application Layer menyediakan antarmuka bagi pengguna untuk berkomunikasi dengan perangkat jaringan, serta memproses permintaan layanan dari pengguna ke jaringan.

3. DHCP Server adalah layanan atau perangkat yang secara otomatis mengelola dan memberikan konfigurasi jaringan, seperti alamat IP, subnet mask, gateway, dan DNS, kepada perangkat yang terhubung ke suatu jaringan.

4. DHCP Client adalah perangkat atau komputer yang meminta konfigurasi jaringan dari DHCP Server untuk mendapatkan alamat IP dan informasi jaringan lainnya secara otomatis.

5. 1. IP Class A

- **Rentang Alamat:** 1.0.0.0 hingga 126.0.0.0
- **Format:** N.H.H.H (N = Network, H = Host), di mana bagian pertama menunjukkan jaringan, dan tiga bagian lainnya menunjukkan host.
- **Subnet Mask Default:** 255.0.0.0
- **Jumlah Jaringan dan Host:**
 - Kelas A memiliki sedikit jaringan, tetapi tiap jaringan mendukung banyak host (hingga 16 juta perangkat).

- **Penggunaan:** Biasanya digunakan oleh organisasi sangat besar, seperti pemerintah atau perusahaan besar.

Contoh Alamat IP Class A: 10.0.0.1

2. IP Class B

- **Rentang Alamat:** 128.0.0.0 hingga 191.255.0.0
- **Format:** N.N.H.H (N = Network, H = Host), dengan dua bagian pertama menunjukkan jaringan dan dua bagian terakhir menunjukkan host.
- **Subnet Mask Default:** 255.255.0.0
- **Jumlah Jaringan dan Host:**
 - Kelas B mendukung lebih banyak jaringan dibanding Kelas A, dengan setiap jaringan mendukung hingga 65 ribu host.
- **Penggunaan:** Digunakan oleh organisasi berukuran menengah hingga besar, termasuk universitas dan perusahaan besar.

Contoh Alamat IP Class B: 172.16.0.1

3. IP Class C

- **Rentang Alamat:** 192.0.0.0 hingga 223.255.255.0
- **Format:** N.N.N.H (N = Network, H = Host), di mana tiga bagian pertama menunjukkan jaringan, dan bagian terakhir menunjukkan host.
- **Subnet Mask Default:** 255.255.255.0
- **Jumlah Jaringan dan Host:**
 - Kelas C memiliki banyak jaringan, tetapi setiap jaringan mendukung hanya hingga 254 host.
- **Penggunaan:** Umumnya dipakai untuk jaringan kecil, seperti di kantor kecil atau jaringan rumah.

6. Firewall adalah sistem keamanan jaringan yang dirancang untuk memantau dan mengendalikan lalu lintas data yang masuk dan keluar dari suatu jaringan berdasarkan aturan keamanan yang telah ditetapkan. Fungsinya adalah untuk melindungi jaringan dari akses yang tidak sah, serangan berbahaya, dan potensi ancaman lain dengan menyaring lalu lintas data dan mengizinkan hanya data yang aman atau yang memenuhi aturan tertentu.

7. NAT (Network Address Translation) adalah teknik yang digunakan dalam jaringan komputer untuk mengubah atau menerjemahkan alamat IP dari perangkat dalam jaringan lokal (private IP) menjadi alamat IP publik sebelum data dikirim ke internet.

8. Routing adalah proses pengiriman data dari satu jaringan ke jaringan lain melalui perangkat yang disebut router. Router menentukan jalur terbaik bagi data untuk mencapai tujuannya dengan mempelajari peta jaringan, atau "topologi," yang menghubungkan berbagai jaringan. Proses routing memastikan bahwa data atau paket informasi sampai ke tujuan yang benar dengan cara yang efisien, bahkan jika ada banyak jalur berbeda di antara perangkat yang terlibat.

STUDI KASUS :

1. Persiapkan Perangkat Pastikan Router dapat terhubung ke internet dan siapkan laptop yang memiliki fungsi VPCS (Virtual PC Simulator) jika digunakan dalam Cisco Packet Tracer.

2. Konfigurasi Router Hubungkan Router ke internet dengan menyambungkan port WAN router ke sumber internet. Konfigurasi WAN lalu konfigurasi NAT (Network Address Translation) jika router akan menerjemahkan Alamat IP privat ke Alamat public.

3. Konfigurasi LAN pada Router Atur IP Lan pada Router dan aktifkan DHCP Server di Router agar perangkat yang terhubung secara otomatis mendapatkan alamat IP.

4. Koneksikan Laptop ke Router Sambungkan laptop menggunakan kabel ethernet atau melalui Wi-Fi tergantung jenis koneksi yang diinginkan.

5. Verifikasi Koneksi Periksa IP di Laptop, cek apakah laptop telah menerima IP dari router dengan cara ipconfig pada

Command Prompt di Windows atau ifconfig pada Linux. Tes koneksi ke Router dengan ping alamat IP router dari laptop.