Kelompok Bab 4 :

1) **Irham Johar Permana (A11.2020.12652)**
2) **Dandi Mahendra Putra Firdaus (A11.2021.13684)**
3) **Avissa Aurellia Amadea (A11.2020.12572)**
4) **Helmi Azkia (A11.2022.14733)**

Jawaban Pertanyaan dari Presentasi Bab 4

1. Bagaimana cara membuat jaringan yang etis dan sustainble agar lebih mudah dan efisien Ketika digunakan?

   - Menentukan topologi jaringan komputer sesuai dengan kebutuhan jaringan pada tempat tertentu.
   - Menentukan alat dan bahan membuat jaringan komputer seperti :
     - Komputer merupakan host yang digunakan sebagai alat komunikasi dan pengolah data dimana pengguna akan bisa bertukan informasi melalui komputer tersebut.
     - Switch adalah pembagi jaringan yang akan terhubung ke komputer host sehingga switch ini mempunyai peran sangat penting dalam jaringan komputer.
     - Kabel jaringan berfungsi untuk menghubungkan antara switch dengan komputer host. Kabel yang digunakan pada jaringan ini adalah kabel UTP dengan model straight.
     - Konektor RJ 45 digunakan untuk menghubungkan kabel dengan port RJ 45 yang ada pada komputer.
     - Tang Krimping berfungsi untuk krimping kabel dengan konektor RJ 45.
     - LAN Tester berfungsi untuk melakukan pengecekan terhadap koneksi kabel.
   - Prosedur kerja dalam membangun jaringan komputer :
     1) Langkah pertama yang harus dilakukan adalah menentukan letak dari switch dan komputer karena nanti akan berpengaruh pada panjang pendeknya kabel yang akan digunakan.
     2) Selanjutnya adalah potong kabel sesuai dengan ukuran yang dibutuhkan. Karena nanti semua komputer akan terhubung ke switch maka pastikan letak switch bisa dijangkau oleh semua komputer.
     3) Langkah ketiga adalah kriping kabel dan konektor meggunakan tang krimping. Pastikan urutan kabel sudah benar yaitu straight yang artinya antara ujung kabel 1 dan ujung kabel satunya mempunyai urutan yang sama.
     4) Cek koneksi kabel dengan LAN Tester
     5) Selanjutnya hubungkan kabel ke komputer dan switch sehingga komputer bisa saling terhubung
     6) Beri Ip Address pada komputer dengan network yang sama. Misalnya: komputer 1: IP - 192.168.1.2 netmask - 255.255.255.0, Komputer 2: IP - 192.168.1.3 netmask - 255.255.255.0
     7) Kemudian cek koneksi jaringan dengan melakukan ping ke alamat host yang dituju.

2. Bagaimana VPN memberikan keamanan tambahan?
   - VPN menyembunyikan dan mengubah alamat IP Address dan lokasi yang sebenarnya.
   - Proses yang mengacak layanan jaringan dikenal sebagai proses enkripsi.
   - VPN menempatkan data internet ke dalam sebuah kapsul untuk mengirimkannya melalui terowongan untuk situs web tertentu, yang dapat dijelajahi pengguna.

   Cara kerja VPN:

   - **Enkripsi Data** : Saat pengguna terhubung ke VPN, data yang dikirim dari perangkat mereka dienkripsi sehingga tidak dapat dibaca oleh pihak yang tidak berwenang yang mencoba memantau aktivitas online pengguna.
   - **Identifikasi Pengguna** : Sebelum pengguna dapat mengakses jaringan VPN, mereka harus memasukkan nama pengguna dan kata sandi atau kredensial lainnya untuk mengidentifikasi diri mereka dan memastikan bahwa hanya pengguna yang sah yang dapat terhubung ke jaringan VPN.
   - **Koneksi ke Server VPN** : Setelah pengguna teridentifikasi, perangkat mereka terhubung ke server VPN yang terletak di tempat lain di dunia. Koneksi ini dilakukan melalui internet atau jaringan publik lainnya.
   - **Pengiriman Data** : Setelah terhubung ke server VPN, pengguna dapat mengirim dan menerima data melalui koneksi internet yang aman. Data dikirim melalui server VPN, yang menambah lapisan keamanan tambahan dan menyembunyikan alamat IP pengguna asli.
   - **Dekripsi Data** : Setelah data sampai ke server VPN, data tersebut didekripsi sehingga dapat diakses oleh pengguna. Ini dilakukan oleh server VPN sebelum data dikirim ke alamat tujuan aslinya.
   - **Keluar dari Jaringan VPN** : Setelah pengguna selesai menggunakan jaringan VPN, mereka harus keluar dari jaringan dan memutus koneksi internet terlebih dahulu. Ini penting untuk memastikan bahwa tidak ada data pengguna yang tersimpan di server VPN atau risiko keamanan lainnya.

3. Menurut sumber tertentu IPV6 sudah dirilis sejak tahun 1998 namun mengapa belum banyak diterapkan terutama di Indonesia?
   - Belum banyaknya translator jaringan IPv4 ke jaringan IPv6.
   - Kelambanan penyelenggara jasa akses Internet (ISP) untuk mulai mengimplementasikan IPv6 ke dalam jaringannya karena adanya penambahan investasi pada sistem inti.
   - Minimnya sistem operasi dari server-server yang mendukung konten berbasis IPv6.
   - Kurangnya dana yang dibutuhkan untuk migrasi dari IPv4 ke IPv6.
   - Penggunaan IPv6 cukup sulit diterapkan di Indonesia.

4. Bagaimana caranya agar IP Address lebih aman ketika digunakan?
   Cara yang paling mudah untuk menghindari hacking dari IP address adalah dengan menggunakan
   - Menggunakan Server Proxy berbasis web untuk menghindari filter konten yang dipasang oleh pihak lain.

- Menggunakan VPN (virtual private network) dapat memberi keamanan ekstra ketika menggunakan internet sebab VPN menyembunyikan identitas alamat IP Address dan lokasi asli pengguna sehingga hacking IP Address menjadi sulit.
- Menggunakan IP Address Hide Software dapat menyembunyikan IP Address secara otomatis dan tidak ada yang bisa melacak lokasi atau mengawasi aktivitas online.

5. Apa saja kelemahan dari kolaborasi virtual?
   a. Terjadinya miss-communication yang menyebabkan kesalahpahaman informasi dan komunikasi yang tidak efektif antar anggota.
   b. Terisolasi dari lingkungan sosial yang menyebabkan rasa kesepian serta kurangnya dukungan sosial sehingga dapat mempengaruhi kesejahteraan mental dan emosional.
   c. Kesulitan dalam pengelolaan tim disebabkan karena waktu kerja yang berbeda dan zona waktu yang berbeda sehingga menyulitkan koordinasi dan kolaborasi.
   d. Ketergantungan pada teknologi dan jaringan internet.
   e. Terhambat masalah teknis yang dapat mengganggu produktivitas karyawan dan kinerja perusahaan secara keseluruhan.