**LEMBAR JAWABAN**

**UJIAN AKHIR SEMESTER**

**SEMESTER GENAP TAHUN AJARAN 2022/2023**

Mata Kuliah : Sistem Jaringan 2

Kelas : IT-501

Prodi : PJJ Informatika

Nama Mahasiswa : Hendro Gunawan

NIM : 200401072103

Dosen : Muhammad Ikhwani Saputra, S.Kom., M.Kom.

**Pertanyaan 1**

1. Buatlah resume jurnal dengan tema Sistem Jaringan, Jelaskan latar belakang jurnal tersebut, metode yang digunakan dan apa nilai tambah yang ditawarkan pada jurnal tersebut.

**Jawaban 1**

**Resume Jurnal dengan Tema Sistem Jaringan 2**

|  |  |  |
| --- | --- | --- |
| **Judul Jurnal** | **:** | MENGENAL SISTEM JARINGAN WIRELESS |
| **Volume & Halaman** | **:** | Volume (7) & Halaman 1-14 |
| **Edisi/Tahun** | **:** | Edisi Juli/2023 |
| **Penulis** | **:** | 1. Hendro Gunawan |
| **Abstrak** | **:** | Jaringan wireless yang paling populer saat ini adalah Wi-Fi (*Wireless Fidelity*) yaitu jaringan teknologi tanpa kabel seperti handphone dengan menggunakan teknologi radio sehingga pemakainya dapat mentransfer data dengan cepat dan aman. Wi-Fi tidak hanya dapat digunakan untuk mengakses internet, Wi-Fi juga dapat digunakan untuk membuat jaringan tanpa kabel di perusahaan. Karena itu banyak orang mengasosiasikan Wi-Fi dengan “Kebebasan” karena teknologi Wi-Fi memberikan kebebasan kepada pemakainya untuk mengakses internet atau mentransfer data dari ruang meeting, kamar hotel, kampus, dan kafe-kafe yang bertanda “*Wi-Fi Hotspot*”. Juga salah satu kelebihan dari Wi-Fi adalah kecepatannya yang beberapa kali lebih cepat dari modem kabel yang tercepat. Jadi pemakaian Wi-Fi tidak lagi harus berada di dalam ruang kantor untuk bekerja. Wi-Fi memiliki beragam standar 802.11 yang ditetapkan oleh IEEE. Untuk koneksi Wi-Fi antar perangkat, ada tiga jenis jaringan nirkabel yang ditetapkan oleh IEEE. Standarnya adalah 802.11a, 802. 11b, dan 802. 11g. Yang membedakan masing-masing standar adalah jangkauan frekuensi dan kecepatan transfernya. Kebanyakan perangkat yang dijual saat ini dilengkapi standar 802.11b, meskipun kecepatan transfer datanya lebih lambat dari pada kecepatan standar 802.11a. Pasalnya, kebanyakan instalasi Wi-Fi saat ini dibangun menggunakan standar 802.11b. |
| **Latar Belakang** | **:** | Di zaman modern seperti saat ini kemajuan teknologi khususnya teknologi telekomunikasi telah berkembang dengan pesat. Perkembangan ini sejalan dengan kemajuan teknologi jaringan komputer yang menghubungkan antara perangkat satu dengan perangkat yang lainnya. Kebutuhan perangkat telekomunikasi dewasa ini tidak hanya untuk komunikasi suara, tetapi sudah merupakan tuntutan untuk komunikasi data, gambar, dan video membentuk komunikasi multimedia. Komunikasi multimedia sudah menjadi keharusan dan ini dimungkinkan karena telah terjadinya konvergensi beberapa layanan seperti voice, data, gambar dan video. Telah banyak aplikasi layanan telekomunikasi yang banyak diminati *user* akibat dari konvergensi layanan yang terjadi. Aplikasi layanan telekomunikasi yang pada awalnya hanya layanan *fixed* sekarang ini telah dituntut untuk dapat diminati menggunakan perangkat bergerak seperti PDA, laptop dan Tablet. Beberapa aplikasi layanan multimedia yang sekarang banyak dinikmati antara lain adalah *m-learning*, *m-banking*, *m-shopping*, *e-medicine*, *e-government*, *telemedicine* dan lain-lain. Kemajuan teknologi telekomunikasi dan informatika biasa disebut *Informatics Communication Technology* (ICT) telah banyak membantu penguna dalam kehidupan sehari-hari. Semua itu tidak terlepas dari sebuah jaringan nirkabel *wireless* atau *wireless network* dimana terdapat sekumpulan komputer yang saling terhubung antara satu dengan yang lainnya dengan media yang digunakan yaitu udara/gelombang sebagai jalur lintas datanya. |
| **Tujuan Penelitian** | **:** | Adapun tujuan penelitian dalam pembuatan karya ilmiah ini adalah:  1. Mengenal wireless LAN   1. 2. Mengenal komponen utama jaringan Wi-Fi. 2. 3. Mengenal keamanan *wireless*. 3. 4. Mengenal kekurangan dan kelebihan *Wireless* LAN. |
| **Manfaat Penelitian** | **:** | Penelitian ini mempunyai manfaat sebagai berikut:  1. Karya ilmiah ini diharapkan dapat memberi pemahaman dan edukasi tentang sistem jaringan *wireless* LAN lebih baik kepada pembaca.  2. Dapat menjadi referensi dalam edukasi dalam mempelajari komponen utama jaringan Wi-Fi.  3. Pemaparan informasi tentang protokol keamanan jaringan *wireless*.  4. Mengetahui kelebihan dan kekurangan *Wireless* LAN. |
| **Metode** | **:** | Metode yang digunakan dalam pembuatan karya ilmiah ini berdasarkan sumber dari buku yang berkaitan dengan komunikasi data dan jaringan komputer serta beberapa referensi dari internet yang sudah memiliki reputasi.  Teknik analisis yang digunakan dalam pembuatan karya ilmiah ini menggunakan metode deskriptif yaitu penelitian yang mengutamakan pemaparan informasi secara deskriptif dengan menggambarkan keadaan yang ada berdasarkan data yang didapatkan. Teknik analisis deskriptif bertujuan untuk mempermudah dalam pemahaman suatu materi karena mengusung konsep penggambaran secara nyata terhadap data yang sudah dipilah atau keadaan yang terjadi. |
| **Hasil dan Pembahasan** | **:** | **3.1 WIRELESS LAN**  Sebelum mengenal apa itu Wi-Fi, perlu adanya pemahaman tentang apa itu Wireless LAN. Wireless LAN adalah salah satu jenis jaringan yang media transmisinya menggunakan wireless frekuensi radio, yang mana sinyal-sinyal yang dikirim menyebar ke seluruh *client-client* dari hasil *broadcast link* suatu alat yang sering disebut dengan *access point* (*Router*). Jaringan ini menjadi populer sehubungan dengan tidak adanya sistem pengkabelan antar komputer. Jaringan *wireless* yang sering digunakan saat ini adalah Wi-Fi atau WLAN. Berikut contoh sederhana bagaimana sistem kerja *wireless*, misalkan tiga buah komputer terhubung dengan *wireless*/Wi-Fi, dan anda telah melakukan konfigurasi *wireless router* maka ketika komputer mengirim data, maka data biner akan di kodekan ke dalam frekuensi radio dan ditransmisikan melalui *wireless router*, kemudian diterima di komputer lain dan didecodekan sinyal tersebut menjadi data biner. Untuk koneksi internet, tidak harus menggunakan kabel *broadband*/Modem ADSL, jika komputer anda dilengkapi Wi-Fi maka anda sudah bisa koneksikan ke komputer lain yang juga dilengkapi *wireless*.  **3.1.1 Mengenal Kecepatan Teknologi Jaringan Wi-Fi**  Wi-Fi atau *Wireless Fidelity* adalah satu standar *wireless Networking* tanpa kabel, hanya dengan komponen yang sesuai dapat terkoneksi ke jaringan. Teknologi Wi-Fi memiliki standar protokol yang ditetapkan oleh sebuah institusi internasional yang bersama *Institute of Electrical and Electronic Engineers* (IEEE), yang secara umum sebagai berikut:   * Standar IEEE 802. 11a yaitu Wi-Fi dengan frekuensi 5 GHz yang memiliki kecepatan 54 Mbps dan jangkauan jaringan 300 m. * Standar IEEE 802.11b yaitu Wi-Fi dengan frekuensi 2,4 Ghz yang memiliki kecepatan 11 Mbps dan jangkauan jaringan 100m. * Standar IEEE 802.11g yaitu Wi-Fi dengan frekuensi 2,4 Ghz yang memiliki kecepatan 54 Mbps dan jangkauan jaringan 300 m.   Teknologi Wi-Fi yang akan diimplementasikan adalah standar IEEE 802.11g karena standar kecepatan tersebut lebih cepat untuk proses transfer data dengan jangkauan jaringan lebih jauh serta dukungan vendor (perusahaan pembuat *hardware*). Perangkat tersebut bekerja di frekuensi 2,4 Ghz atau disebut sebagai pita frekuensi ISM (Industrial, Scientific, and Medical) yang juga digunakan oleh peralatan lain, seperti *microwave open*, *cordless phone*, dan *bluetooth*.  **3.1.2 Tipe Jaringan Wi-Fi**  Seperti halnya Ethernet-Lan (jaringan dengan kabel), jaringan Wi-Fi juga dikonfigurasikan ke dalam dua jenis jaringan:   * + - * 1. **Jaringan peer to peer/Ad Hoc Wireless LAN**   Komputer dapat saling melakukan komunikasi berdasarkan nama SSID (*Service Set Identifier*). SSID adalah nama identitas komputer yang memiliki komponen nirkabel.  undefined  ***Gambar 2. Desain Komunikasi Data Peer To Peer***  **b. Jaringan Server Based/Wireless Infrastructure**  Sistem infrastruktur membutuhkan sebuah komponen khusus yang berfungsi sebagai *acces point*.  TM UNIFI WIRELESS REPAIR & UPGRADE SERVICE: March 2014  **Gambar 3. Desain Komunikasi Data Antar Kabel dengan Nirkabel**  **3.2 KOMPONEN UTAMA JARINGAN WI-FI**  Terdapat empat komponen yang berfungsi menerima dan mengirimkan data dari WLAN:  *Access Point*, berfungsi mengkonversikan sinyal frekuensi radio (RF) menjadi sinyal digital yang akan disalurkan melalui kabel, atau disalurkan ke perangkat *wireless* LAN yang lain dengan dikonversikan ulang menjadi sinyal frekuensi radio.  *Wireless LAN Interface*, merupakan device yang dipasang di *Access-Point* atau di *Mobile*/*Desktop* PC, *device* yang dikembangkan secara massal adalah dalam bentuk PCMCIA (*Personal Computer* *Memory Card International Association*) *card*.  *Wired LAN*, merupakan jaringan kabel yang sudah ada, jika wired LAN tidak ada maka hanya sesama wireles LAN saling terkoneksi.  Mobile/Desktop PC, merupakan perangkat akses untuk klien, mobile PC pada umumnya sudah terpasang port PCMCIA sedangkan desktop PC harus ditambahkan PC Card PCMCIA dalam bentuk ISA (*Industry Standard Architecture*) atau PCI (*Peripheral Component Interconnect*) *card*.  Berikut komponen jaringan *Wireless* yang digunakan secara umum pada Teknologi WLAN.  MEDIOS DE RED INALÁMBRICOS  **Gambar 4. Komponen WLAN Network**  **3.3 KEAMANAN WIRELESS**  Teknologi komunikasi seluler berbasis GSM berkembang pesat sehingga dalam waktu beberapa tahun saja sudah melewati beberapa kapasitas telepon tetap seperti pengguna seluler *blackberry*. Hal ini dikarenakan untuk memenuhi kebutuhan pengguna jasa telekomunikasi yang cenderung lebih *mobile* (bergerak) dan ingin berbagai kemudahan, juga pada era *network*  yang selama ini dihubungkan kabel terasa mengganggu tuntutan mereka. Untuk itu, dikembangkan teknologi nirkabel untuk area network, yaitu *wireless* *local area* *network* (W-LAN). Teknologi ini sangat menunjang dan menjaga tingkat produktivitas di tengah mobilitas yang tinggi. W-LAN dikembangkan para pionir akar rumput tahun 1985 ketika regulator telekomunikasi Amerika Serikat, FCC, mengizinkan “sekerat” radio/*frekuensi* spektrum untuk  keperluan eksperimental. Berbagai penelitian dilakukan di laboratorium utama untuk membangun jaringan nirkabel yang menghubungkan berbagai macam peralatan dari komputer, mesin kas register, dan lain-lain.  Tahun 1997 lahir standar pertama, masih prematur, yang dikenal dengan IEEE 802.11b dan disebut *wireless fidelity* (Wi-Fi). Sekerat spektrum frekuensi radio tersebut adalah frekuensi 2,4 Gigahertz (GHz). Karena pola operasinya terbatas pada spot tertentu, maka layanan ini mempunyai sebutan populer, “hotspot”.  Secara bisnis skala dunia perkembangan layanan jasa *hot-spot* saat ini sedang menanjak. Dari mulai RT-RW Net *Hotspot* sampai ke usaha koperasi dunia seperti United Parcell *Service*, Starbucks, atau London Costa Coffee sudah mulai memanfaatkan layanan ini. Penggunanya di seluruh dunia meningkat sangat tajam, karena perangkat berbasis Wi-Fi sangat luas tersedia di pasar.  Walaupun demikian, Wi-Fi sendiri masih mengandung beberapa kelemahan dan tantangan seperti :  1. Keamanan menjadi masalah karena percobaan menunjukkan pengacakan terketatnya pun hanya 128-bit encription, sehingga dapat dengan mudah ditembus “penyusup (*hacking*)” menjadi satu hal yang dikhawatirkan.  2. Standar 802.11b pada 2,4 GHz hanya dapat dioperasikan untuk 3 kanal sekaligus agar tidak saling mengganggu di suatu lokasi. Kelemahan ini mungkin teratasi , bila terjadi migrasi ke standar yang lebih tinggi, yaitu 802.11 pada spektrum 5 GHz.  3. Wi-Fi juga mengakomodasi *limit mobility* karena tidak seperti jaringan seluler yang menyediakan *seamless transfer* dari satu base station ke lainnya. Namun, hal ini tidak begitu menjadi masalah karena pengguna laptop yang biasanya diam di suatu tempat. Hal ini akan menjadi masalah bagi pengguna PC kantung atau PDA *handheld*.  **3.3.1 Hotspot**  WiFi Hotspot Device at Rs 2500/unit | WiFi Hotspot Device | ID: 11737350188  **Gambar 5. Wi-Fi hotspot device**  W-LAN bukanlah mobile, tetapi dikembangkan untuk mendukung pengguna stasioner di dalam sebuah area yang kecil (*small reach*), yaitu hanya beberapa radius meter jaraknya dari *centric access point*, ini merupakan unsur inti pada setiap W-LAN. Akan tetapi W-LAN dapat juga mendukung para pemakai *mobile*, dengan menggunakan suatu publik W-LAN, yang sering direferensikan sebagai hot spot. Internet mengakses via *hotspot* yang *provisioned* oleh suatu WISP (*Wireless Internet Service Provider*), walaupun *hot spot* masih ditemukan hanya pada tempat yang konsentrasi pemakaian tinggi, seperti hall/aula konferensi, ruang bersantai pelabuhan udara, hotel atau café maka pemakai *mobile* yang tidak di dalam jangkauan jaringan (*wired* maupun *wireless intranet*), boleh menghubungkan ke internet via publik W-LAN dan boleh memanfaatkan *rate* data tinggi. Bagaimanapun, komunikasi *wireless* umum muncul suatu permasalahan: antara lain faktor keamanan. Demikian pula W-LAN tidak terkecuali, oleh karena itu permasalahan harus benar-benar dipelajari dan harus dikembangkan dalam mengatasinya. *Hot-Spot services* dirancang untuk kemudahan yang maksimal bagi pengguna wireless LAN, sehingga biasanya tidak menawarkan WEP atau WPA *encryption*, jika berhubungan dengan suatu *hot spot*, yang dianggap semua data yang dikirim mungkin *unencrypted*. Karena wireless LAN mengizinkan *peer-to-peer* koneksi, maka semua pengguna jaringan dapat saling melihat isi data pada masing-masing komputer bahkan file-file rahasia dapat diamati bila tidak dilindungi seperti informasi, angka-angka kartu kredit, IP address koneksi, isi *e-mail*, pesan tertentu yang akan dikirim dan file rahasia lainnya. Seseorang dengan mudah dapat melakukan pengrusakan misalnya dengan dimasukkan virus yang dapat menghentikan kegiatan komputer yang ada.  **3.3.2 Penyerangan Pada Hotspot**  Penggunaan *Wireless* LAN mempunyai faktor keunggulan yaitu selalu menyediakan sambungan jaringan tanpa harus memakai kabel. 50% dari 1000 perusahaan di Amerika Serikat menggunakan teknologi ini yang didasari oleh perkembangan teknologi dari standar 802.11x.  Akan tetapi sistem jaringan ini hampir kurang memadai dan kurang perhatian terhadap keamanan informasi. Keamanan dari sisem jaringan ini sangat menentukan suksesnya suatu kinerja bisnis dan merupakan faktor penting dalam mencapai tujuan perusahaan.  Peralatan dari standar 802.11b mempunyai biaya yang rendah hal ini membuat teknologi tersebut begitu atraktif dan membuat para penyerang (*attacker*) mudah untuk melakukan serangan. Tetapi dengan manajemen yang baik dan setting yang bagus serta didukung oleh peralatan dan perlengkapan yang mendukung kemungkinan hal tersebut dapat diatasi. Risiko serangan yang mungkin akan terjadi pada standard 802.11b dapat dikategorikan sebagai berikut:  1. “*Insertion Attack*”  *Insertion Attack* didasari oleh adanya *device-device* yang bekerja tidak sesuai dengan prosedur baku (*unauthorized devices*) atau menciptakan jaringan *wireless* baru tanpa melalui proses pengamanan. Pada jenis serangan ini, seorang penyerang mencoba melakukan koneksi ke dalam jaringan *wireless* seorang klien menggunakan laptop atau PDA dan tablet, dan melakukan akses point tanpa otorisasi sebelumnya kemudian akses point dapat diubah untuk meminta sebuah *password* untuk seorang klien yang mengakses, jika tidak terdapat *password* untuk seorang klien yang mengakses, jika tidak terdapat *password*, orang tersebut (penyerang) berusaha masuk dan dapat melakukan koneksi ke dalam jaringan internal dengan mudah .  Meskipun beberapa akses point menggunakan *password* yang sama untuk semua akses klien, sebaiknya semua pengguna memakai *password* baru setiap kali melakukan akses point. Suatu perusahaan mungkin tidak selalu berhati-hati bahwa ada saja pegawai internal yang ada di dalam perusahaan secara tidak sadar telah menyebarkan kapabilitas dari *wireless* ke dalam jaringan, dalam hal ini perusahaan memerlukan suatu kebijaksanaan untuk memastikan konfigurasi pengamanan akses point.  2. *Interception* dan *Monitoring Traffic Wireless*  Sebagian jaringan tanpa kabel, ada kemungkinan terjadi pemotongan jalur *wireless*, penyerang harus berada pada suatu jangkauan jarak akses sekitar 300 kaki untuk tipe 802.11b. Supaya serangan bisa berjalan, penyerang bisa berada di mana saja, di mana terdapat kemungkinan koneksi jaringan bisa masuk. Keuntungan pemotongan jalur wireless ini adalah serangan tersebut hanya memerlukan penempatan dari suatu agen yang berfungsi memantau sistem yang mencurigakan. Semua itu memerlukan akses ke dalam aliran data di dalam jaringan.  Ada dua pertimbangan penting untuk tetap bekerja dalam radius atau jarak pada tipe 802.11b. Pertama, posisi antena didesain secara langsung, yang dapat meneruskan sinyal transmisi atau jarak penangkapan sinyal dari *device* 802.11b. Oleh karena itu jangkauan maksimum 300 kaki adalah suatu desain instalasi normal untuk tipe ini.  Kedua, desain pola lingkaran, pada pola ini sinyal sinyal dari 802.11b hampir selalu meneruskan sinyal di belakang batas area hal ini dimaksudkan untuk mengcover sinyal tersebut.  *Wireless packet analysis*, seorang penyerang melakukan capture terhadap jalur wireless menggunakan teknik yang sama dengan seorang user yang tidak didukung atau pekerja yang ceroboh di dalam jaringan kabel. Banyak cara untuk melakukan *capture,* bagian pertama, di mana data yang secara tipikal akan menyertakan user name dan password seorang yang memaksa masuk dan melakukan penyamaran sebagai seorang *user* legal, dengan menggunakan informasi dari hasil *capture* ini digunakan untuk melakukan pembajakan *user session command* yang tidak sesuai dengan prosedur resmi yang ada.  3. *Jamming*  “*Denial of Service Attack*/*DOS Attack*” mudah untuk diterapkan ke dalam jaringan *wireless*. Di mana jalur tidak dapat menjangkau klien atau akses point sebab jalur yang tidak resmi “membanjiri” frekuensi akses tersebut. Seorang penyerang dengan peralatan dan perlengkapan yang memadai dapat dengan mudah “membanjiri” dengan frekuensi 2,4 Ghz, membuat sinyal sampai rusak sampai jaringan *wireless* berhenti berfungsi. Dalam hal lain kawat telepon, monitor mini dan *device* lain yang beroperasi dengan frekuensi 2,4 Ghz dapat merusak jaringan *wireless* tersebut dengan menggunakan frekuensi ini. DOS *attack* ini dapat berasal dari luar area kerja *wireless*.  4**.** *Client-to-Client Attack*  Dua klien *wireless* dapat saling berkomunikasi satu sama lain dengan melakukan akses poin terlebih dahulu.Oleh karena itu *user* perlu untuk melakukan perlindungan terhadap klien tidak hanya sekedar melawan suatu ancaman eksternal tetapi juga melawan satu sama lain.  5. *File Sharing* dan Serangan melalui layanan TCP/IP  Layanan *wireless* *client* yang berjalan menggunakan pelayanan yang diberikan oleh TCP/IP seperti *web server*, atau *file sharing* terbuka untuk pemakaian yang sama dari kesalahan konfigurasi setiap *user* di dalam suatu jaringan yang menggunakan kabel.  6. DOS (*Denial of Service*)  Suatu *device wireless* yang “membanjiri” klien *wireless* lain dengan menggunakan paket palsu, menciptakan suatu DOS *attack*, IP atau MAC palsu, sengaja atau tidak dapat menyebabkan kerusakan pada jaringan.  7. Serangan “*Brute Force Attack*” terhadap *Password* seorang *user*  Sebagian besar akses point menggunakan suatu kunci tanggal atau *password* yang dimiliki oleh klien pada jaringan wireless. Serangan *Brute Force* ini mencoba melakukan uji coba terhadap kunci akses tersebut dengan memasukkan beberapa kemungkinan.  8. Serangan terhadap Enkripsi  Standar 802.11b menggunakan sebuah sistem enkripsi yaitu WEP (*Wireless Equivalent Privacy*). Tidak banyak peralatan siap tersedia untuk mengangkat masalah ini, tetapi perlu diingat bahwa para penyerang selalu dapat merancang alat yang dapat mengimbangi sistem keamanan yang baru.  **3.3.3 Konfigurasi Sistem Keamanan WI-Fi**  Banyak akses point bekerja dalam suatu konfigurasi yang tidak aman kecuali para administrator yang mengerti resiko penggunaan keamanan wireless dan konfigurasi masing-masing unit sebelum digunakan. Akses point ini akan berjalan pada risiko yang tinggi untuk diserang atau ada yang menyalahgunakan.  Bagian berikut ini menguji tiga akses point yang bisa dikatakan terbaru yaitu dari CISCO, Lucent dan 3Com. Meskipun masing-masing vendor mempunyai implementasi sendiri dalam menerapkan 802.11b. Menanggapi hal tersebut seharusnya para vendor mengembangkan produknya menjadi lebih aplikatif.  **1. Server Set ID (SSID)**  SSID adalah suatu identifikasi terhadap konfigurasi yang memungkinkan klien berkomunikasi dengan akses point yang tepat dan benar menggunakan konfigurasi tertentu. Hanya klien yang menggunakan SSID yang benar dapat melakukan komunikasi. SSID bekerja sebagai suatu “*single shared password*” antara akses point dengan klien. Akses point berjalan dengan default SSID jika tidak diubah, unit uni sangat mudah untuk diterapkan, berikut ini 3 *default password* umum SSID.  “**Tsunami**”  CISCO Aironet 340 series 11 MBPs DSSS Wireless LAN Access Point  CISCO Aironet 340 series 11 MBPs DSSS PCI Card dengan enkripsi 128 bit.  “**101**”  3Com AirConnect 11 MBPs Wireless LAN Access Point  3Com AirConnect 11 MBPs Wireless PCI Card.  “**Roam About Default Network Name**”  Avaya Orinoco As-2000 Akses Server (Lucent/Cabletron)  Avaya Orinoco PC Gold Card (Lucent/Cabletron)  SSID di udara berupa teks yang bersih jika WEP-nya disable membuat SSID-nya dapat di-*capture* melalui monitoring jalur jaringan. *Lucent* akses point dapat beroperasi di dalam akses mode aman. Pilihan ini memerlukan SSID baik klien atau akses point agar sesuai dan default sekuritinya harus dalam keadaan mati (*turn-off*).  Di dalam akses mode “ non-aman”, klien dapat terhubung ke akses point menggunakan konfigurasi SSID, SSID kosong atau konfigurasi SSIS dalam kondisi “*any*”.  **2. Wire Equivalent Privacy (WEP)**  WEP dapat dikonfigurasi sebagai berikut:   * *No encryption* * 40 bit enkripsi * 128 bit enkripsi   Tiga contoh sistem keamanan akses poin tersebut di atas mempunyai WEP-*turn off*, meskipun kekuatan dua kunci enkripsi (40 bit dan 128 bit) merupakan hal yang pokok namun enkripsi menggunakan 128 bit lebih efektif jika dibandingkan dengan 40 bits SNMP *Community Password*. Banyak akses point dalam wireless berjalan di atas SNMP agen. Jika pengelompokan kata (*community word*) tidak dilakukan dengan konfigurasi yang benar, seorang penyerang dapat membaca dan bahkan dapat membuat data baru yang sangat sensitif ke dalam akses point. Jika SNMP agent diterapkan di dalam *wireless* seorang klien maka risiko yang sama berlaku juga terhadap mereka.  Konfigurasi *Interface* masing-masing model akses point mempunyai *interface* sendiri untuk ditampilkan dan dimodifikasi dari konfigurasinya, berikut adalah *interface* yang sering dipakai, ada 3 pilihan:   * CISCO-SNMP, serial, Web, telnet * 3Com-SNMP, serial, Web, telnet * Lucent/Cabletron, SNMP, serial (no Web/telnet)   **3. Risiko Keamanan dari Sisi Klien**  Klien terhubung ke sebuah akses point yang menyimpan informasi yang sensitif untuk dicocokkan dan disampaikan. Informasi ini dapat diatur jika klien tidak melakukan konfigurasi dengan benar*. Software Cisco* untuk klien menyimpan SSID di dalam *registry*-nya Windows dan kunci WEP di dalam “*firmware*” di mana hal ini lebih sulit. *Software Lucent/Cablet*ron untuk klien sama menyimpan SSID di dalam *registry Windows*, kunci WEP disimpan di dalam *registry* *Windows* dengan tidak menggunakan enkripsi. Instalasi secara default, semua akses point dioptimalkan untuk membantu membuat sebuah jaringan yang berguna secepat dan semudah mungkin alhasil konfigurasi defaultnya dapat meminimize faktor keamanan di jaringan Wi-Fi. |
| **Kelebihan dan Kekurangan** | **:** | **3.4 KELEBIHAN DAN KEKURANGAN WIRELESS LAN**  Berikut adalah kelebihan dan kekurangan dari Wireless LAN.  **3.4.1 Kelebihan Wireless LAN**  1. Lebih mudah untuk menambah atau memindahkan workstation.  2. Lebih mudah untuk menyediakan konektivitas di daerah yang sulit untuk meletakkan kabel.  3. Instalasi lebih cepat dan mudah.  4. Akses ke jaringan bisa dari mana saja dalam jangkauan jalur akses.  5. Manfaat jangka panjang biaya dapat ditemukan dilingkungan yang dinamis yang memerlukan frekuensi gerak dan perubahan.  6. Memiliki mobilitas tinggi yang dapat meningkatkan kualitas layanan dan kualitas produktivitas.  7. Meskipun biaya investasi awal untuk perangkat keras Wireless LAN lebih mahal dari pada LAN, tapi biaya instalasi dan perawatan jaringan Wireless LAN lebih murah, sehingga secara total dapat menurunkan besar biaya kepemilikan.  8. Dapat menggunakan berbagai macam topologi jaringan komputer sesuai dengan kebutuhan.  **3.4.2 Kekurangan Wireless LAN**  1. Keamanan data kurang terjamin.  2. Biaya peralatan cukup mahal.  3. Adanya masalah propagasi radio misalnya seperti: terhalang, terpantul dan banyak sumber interferensi.  4. Kapasitas dari jaringan menghadapi keterbatasan spektrum.  5. Transfer data ke masing-masing komputer akan kurang dan lambat ketika jumlah komputer yang menggunakan jaringan meningkat.  6. Perangkat hanya akan beroperasi pada jarak terbatas dari jalur akses, dengan jarak yang ditentukan oleh standar yang digunakan dan *buildings* serta hambatan lainnya antara titik akses (*access point*) dan pengguna (*user*).  7. Sebuah kabel LAN yang paling mungkin dibutuhkan untuk menyediakan *backbone* ke *Wireless Lan*, *Wireless* LAN harus menjadi supplement untuk kabel LAN dan bukan solusi yang lengkap.  8. Jangka panjang efisiensi biaya lebih sulit untuk mencapai static environments yang membutuhkan few moves dan perubahan. |
| **Kesimpulan** | **:** | Berdasarkan pembahasan di atas, dapat disimpulkan bahwa jaringan komputer adalah hubungan antar komputer atau node dengan komputer lain melalui media jaringan komputer. Media jaringan komputer dibagi menjadi dua yaitu kabel dan nirkabel. Dimana pada jaringan terdapat kabel UTP, coaxial dan serat optik. Dimana dalam penyusunan jaringan komputer terdapat berbagai macam topologi yang mempengaruhi kinerja dari jaringan komputer itu sendiri. Sedangkan pada jaringan nirkabel, memanfaatkan media elektromagnetik, gelombang frekuensi, dan sinyal cahaya. Di mana jaringan nirkabel lebih praktis dan sangat mudah ditemui pada saat ini. Selain itu juga terdapat protokol sebagai media penghubung internal bukan fisik yang menjamin keberhasilan dan keamanan saat data tersebut melalui proses transmisi dari komputer satu ke komputer yang lainnya.  Selain itu dalam transmisi data terdapat jenis kanal seperti *simplex* atau satu arah komunikasi, *half duplex* semi dua arah komunikasi dan *full duplex* dua arah komunikasi antar node. Jenis cara transmisi mulai dari unicast (*one to one*), broadcast (*one to all*) dan *multicast*. |
| **Saran untuk Penelitian Selanjutnya** | **:** | 1. Peneliti selanjutnya diharapkan untuk mengkaji lebih banyak sumber ataupun referensi terkait objek yang diteliti agar hasil penelitiannya lebih lengkap lagi. 2. Objek penelitian ini diharapkan dapat diperluas lagi dan tidak terbatas pada bidang transisi data melainkan bidang lainnya seperti manajemen jaringan komputer dengan menggunakan *Cisco Packet Tracer* untuk memperoleh hasil yang maksimal.  3. Peneliti selanjutnya disarankan agar meningkatkan ketelitian, baik dalam segi kelengkapan data maupun proses pencarian informasi.  4. Penelitian selanjutnya diharapkan mengambil informasi lebih akurat dengan melakukan wawancara narasumber yang kompeten.  5. Untuk keakuratan data, disarankan bagi peneliti selanjutnya untuk mengambil referensi dan sumber data yang baru, minimal yang terbit lima tahun yang lalu, memiliki ISSN atau nomor seri, dan jelas siapa publishernya.  6. Penelitian selanjutnya diharapkan untuk menggunakan lebih banyak sumber data baik dari buku maupun dari internet dan jurnal lainnya.  7. Bagi peneliti selanjutnya diharapkan untuk dapat menjaga sikap dan tingkah laku, serta mematuhi setiap peraturan selama proses penelitian agar dapat menjaga nama baik Universitas.  8. Penelitian selanjutnya dapat menggunakan hasil penelitian ini, namun tetap harus mengembangkan sumber data dan referensi terbaru untuk memperoleh hasil penelitian yang berkualitas.  9. Penelitian selanjutnya diharapkan untuk berhati-hati selama proses penelitian karena banyak tantangan dalam pengumpulan sumber data.  10. Penelitian selanjutnya diharapkan menggunakan bahasa Indonesia dengan baik dan benar agar pembaca dapat memahami kalimat yang ada di dalam jurnal penelitian tersebut. |
| **Nilai Tambah Yang Ditawarkan** | **:** | Nilai tambah yang ditawarkan dalam jurnal ini yaitu area *network* yang selama ini dihubungkan dengan menggunakan kabel masih terasa mengganggu. Untuk itu, dikembangkanlah teknologi *nirkabel* (tanpa kabel) untuk area *network*, yaitu *Wireless Local Area Network* (W-LAN). Teknologi ini sangat menunjang dan menjaga tingkat produktivitas di tengah mobilitas yang tinggi. |
| **Daftar Pustaka** | **:** | Gunawan Wibisono, G. D. (2008). *MOBILE BROADBAND Tren Teknologi Wireless Saat ini dan Masa Datang.* Bandung: INFORMATIKA.  Maslan, A. (2020). *Jaringan Komputer dan Simulasi CISCO Packet Tracer.* Yogyakarta: CV BUDI UTAMA. |
| **Link Jurnal** | **:** | <https://docs.google.com/document/d/1AkMAnHB8eYm2Ca0-8gwlY2EaNvdqhs0v/edit?usp=sharing&ouid=101456110840209175777&rtpof=true&sd=true> |

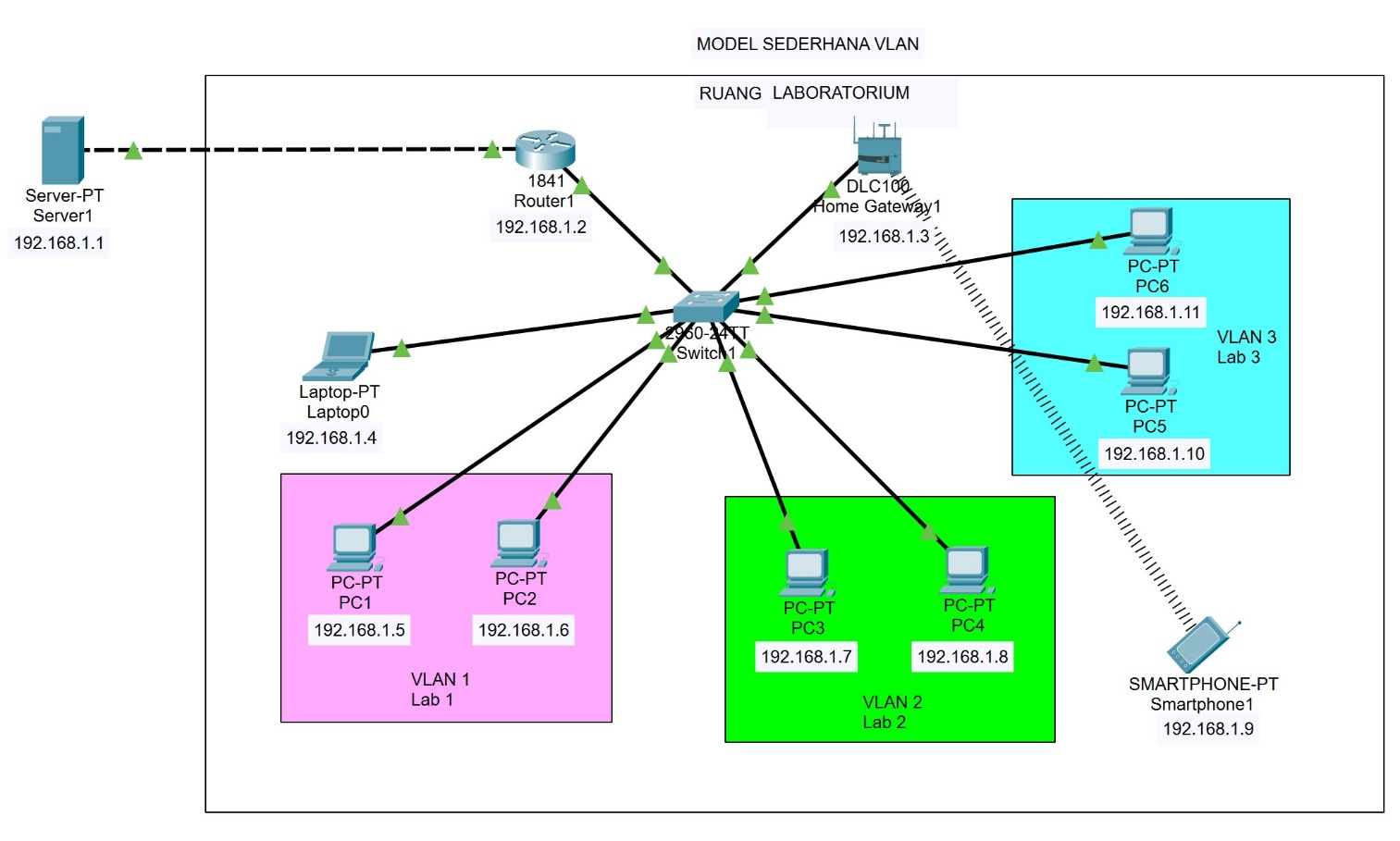
**Pertanyaan 2**

2. Jelaskan dan gambarkan tentang VLAN. Buatlah Model sederhana VLAN dengan packet tracer

**Jawaban 2**

**VLAN: Pengertian, Fungsi dan Cara Kerjanya**

**2.1 Pendahuluan**

****

**Gambar 2.1. Model sederhana VLAN dengan menggunakan cisco packet tracer**

Seiring dengan perkembangan teknologi, sistem jaringan dan *networking* juga tak luput dari pembaruan fungsi. Salah satu informasi yang perlu diketahui adalah VLAN atau *Virtual Local Area Network*. Kehadiran VLAN itu sendiri mampu membuat kita bisa melakukan manajemen kontrol terhadap lalu lintas traffic data, kemudian bereaksi lebih cepat ketika dibutuhkan relokasi. Jika dibandingkan dengan LAN, jaringan versi virtual ini otomatis mampu memberikan fleksibilitas tinggi untuk menunjang proses adaptasi dan perubahan karena administrasinya sudah disederhanakan.

**2.2 Apa Itu VLAN (Virtual Local Area Network)?**

*Virtual Local Area Network* atau VLAN adalah sekumpulan perangkat yang ada di satu atau lebih jaringan LAN dan dikonfigurasikan oleh perangkat lunak sehingga dapat berkomunikasi antara satu dengan lainnya seolah-olah berada di saluran yang sama.

VLAN sendiri sebenarnya merupakan sebuah jaringan yang berada di dalam *Local Area Network* (LAN) sehingga dalam satu jaringan LAN bisa terdiri atas lebih dari satu jaringan VLAN.

Secara umum, konfigurasi jaringan *Virtual Local Area Network* (VLAN) dilakukan oleh perangkat lunak atau *software*. Alhasil, hal ini mampu memberikan keuntungan ketika perangkat berpindah tidak perlu melakukan setup jaringan lagi.

**2.3 Fungsi VLAN**

Fungsi Virtual Local Area Network atau VLAN adalah mengakomodir konfigurasi pada jaringan komputer fisik menjadi beberapa domain siaran. Meski memiliki domain siaran berbeda, jalur yang dihasilkan oleh VLAN tersebut masih melewati perangkat penghubung yang sama. Biasanya dikonfigurasikan dengan mikrotik atau cisco. Teknologi WLAN juga memungkinkan beberapa LAN virtual untuk saling berdampingan dalam jaringan LAN fisik. Metodenya sendiri biasanya menggunakan switch bukan *router* seperti pada konfigurasi LAN biasa.

**2.4 Manfaat VLAN**

Berikut ini merupakan beberapa manfaat VLAN yang bisa Anda dapatkan, dari berbagai manfaat tersebut diharapkan Anda bisa mempertimbangkan apakah ingin menggunakan VLAN atau tetap memanfaatkan jaringan LAN tradisional.

* + - 1. **Menambah Keamanan**

LAN atau *Local Area Network* merupakan sebuah jaringan private yang tidak bisa diakses oleh sembarang user. Dari segi keamanan, LAN tentu sangat maksimal karena setiap akses harus mendapat *permission* atau izin dari administrator jaringan. Adapun VLAN (*Virtual Local Area Network*) sendiri konsepnya hampir sama seperti LAN konvensional, hanya saja jaringan yang digunakan kini sudah bersifat nirkabel sehingga bisa diakses di mana saja. Faktor keamanan sendiri menjadi sangat penting bagi sebuah bisnis atau perusahaan karena ada berbagai data sensitif yang harus dijaga. VLAN dapat bermanfaat untuk membatasi akses ke berbagai data sensitif tersebut sehingga mengurangi potensi penyalahgunaan akses dari orang tidak bertanggung jawab.

* + - 1. **Efisiensi Biaya**

Sebagaimana kita ketahui, untuk menggunakan LAN diperlukan jaringan kabel yang cukup banyak sehingga membutuhkan biaya pemasangan yang lumayan besar. Dengan VLAN (*Virtual Local Area Network*) Anda tetap akan mendapatkan fasilitas dan fitur-fitur dari LAN tanpa harus repot-repot menyiapkan kabel. Hal ini tentu sangat efektif dan efisien karena perusahaan bisa menghemat biaya pembelian kabel LAN ketika ada komputer baru yang ingin dihubungkan. Selain itu, sistem jaringan VLAN juga tidak menggunakan router dimana membutuhkan lebih banyak pemrosesan, tapi memakai switch yang jauh lebih mudah penggunaannya.

* + - 1. **Tidak Perlu Mengatur Ulang Jaringan Komputer**

Agar bisa tetap terkoneksi ke jaringan LAN, maka setiap komputer yang dipindahkan harus diatur ulang. Hal ini tentu membutuhkan banyak waktu karena harus dilakukan mulai dari awal. Nah, dengan memanfaatkan jaringan VLAN Anda dapat memindahkan komputer kapan saja dan dimana saja tanpa harus mengatur ulang jaringan LAN. Pasalnya, komputer yang dipindahkan akan tetap terhubung dengan jaringan VLAN.

* + - 1. **Peningkatan Kinerja Yang Lebih**

Dari segi kinerja, VLAN dapat membuat layer datar dua jaringan menjadi beberapa grup kerja logis guna mengurangi beban traffic pada jaringan. Hal ini bertujuan untuk memisahkan antara jaringan non esensial dan jaringan penting sehingga performanya semakin optimal.

* + - 1. **Memudahkan Administrasi**

Manfaat VLAN berikutnya adalah penyederhanaan proses administrasi. Dengan adanya jaringan VLAN sebuah komputer server tidak perlu datang langsung ke area komputer server untuk masuk ke jaringan. Semua komputer bisa terkoneksi dan menjangkau server dari tempat lain, adapun keberadaan komputer server memudahkan administrator untuk melakukan pengaturan dan kontrol terhadap jaringan agar lebih aman.

**2.5 Jenis-Jenis VLAN**

Berdasarkan fungsinya, VLAN dibedakan menjadi beberapa jenis. Berikut ini penjelasan selengkapnya.

**VLAN Default**

VLAN default adalah sebutan untuk menamai konfigurasi sejak sakelar pertama kali dinyalakan. Jenis VLAN ini masih standar dengan semua *port switch* yang tersedia dan terhubung dalam fungsi dasar.

**Data VLAN**

Jenis VLAN yang satu ini memiliki fungsi utama untuk mengatur lalulintas data yang terjadi dalam sebuah jaringan VLAN.

**VLAN Suara**

Secara garis besar, VLAN suara adalah jaringan yang sudah mendukung layanan VoIP dan sudah dirancang khusus untuk menunjang kebutuhan komunikasi berbasis suara.

**Management VLAN**

Sesuai namanya,, jenis VLAN yang satu ini adalah sistem jaringan *Virtual Local Area Network* yang dikonfigurasikan untuk kebutuhan saklar management.

**VLAN Asli**

VLAN asli adalah jaringan VLAN yang dikembalikan ke *port* jika tidak memiliki tag atau tidak ada di bagasi.

**2.6 Cara Kerja VLAN**

Secara umum, cara kerja VLAN yakni menghubungkan semua perangkat komputer dalam lebih dari satu jaringan *Local Area Network*. Jaringan VLAN menyediakan akses data ke semua *client* komputer yang terhubung ke *switch* dan diberi ID yang sama. Server VLAN pada dasarnya membuat domain broadcastnya sendiri, memisahkan jaringan fisik menjadi beberapa jaringan logis. Di atas kertas, lalu lintas komunikasi VLAN diatur oleh server, kemudian switch memastikan bahwa data pergi dan diakses ke proses selanjutnya seperti LAN pada umumnya.

**2.7 Kesimpulan**

Itulah penjelasan terkait apa itu VLAN lengkap dengan manfaat dan cara kerjanya. VLAN adalah salah satu teknologi jaringan yang bisa digunakan untuk mengoptimalkan koneksi antar jaringan komputer perusahaan. Ada banyak keuntungan dan manfaat dari VLAN yang bisa didapatkan jadi sangat cocok bagi Anda yang ingin mengoptimalkan *networking* di perusahaan yang sedang berkembang. Terlepas dari itu, selain menggunakan LAN atau VLAN, di masa pandemi seperti sekarang ini Anda juga bisa memanfaatkan VPN sebagai layanan untuk mengamankan jaringan.

VPN atau *Virtual Private Network* berfungsi untuk mengenkripsi jaringan internet ketika mengakses data-data sensitif perusahaan dari jarak jauh. Teknologi ini mampu meminimalisir adanya interupsi atau gangguan dari pihak-pihak yang tidak bertanggung jawab sehingga file rahasia Anda tetap terjaga.

File cisco packet tracer: <https://drive.google.com/file/d/1_dBWOJV0VTTPiZkFTk6YR8KqgwbgYl6f/view?usp=sharing>

**Pertanyaan 3**

3. Jelaskan dan fungsi dari *Core Switch*, *Distribution Switch* dan *Switch Access*, kemudian anda gambarkan model tersebut secara sederhana.

**Jawaban 3**

**Switch**

**3.1 Pengertian Switch**

*Switch* adalah perangkat jaringan yang digunakan untuk menghubungkan perangkat komputer dan perangkat jaringan lainnya. Ada beberapa jenis *Switch* yang digunakan dalam jaringan, termasuk *Core Switch*, *Distribution Switch*, dan *Acces Switch*. Ketiga jenis *Switch* ini memainkan peran yang berbeda dalam jaringan, dan penting untuk memahami perbedaan antara mereka.

**3.2 Jenis-JenisSwitch**

**3.2.1 Core Switch**

*Core Switch* adalah switch yang terletak di pusat jaringan dan bertanggung jawab untuk menghubungkan semua jaringan di dalam organisasi atau perusahaan. *Core switch* adalah perangkat jaringan yang digunakan untuk menghubungkan beberapa *switch* dan *router* dalam sebuah jaringan. Perangkat ini berada di lapisan paling atas dalam arsitektur jaringan dan bertanggung jawab untuk mengatur lalulintas data antara jaringan lokal (LAN) dan jaringan luas (WAN).

*Core Switch* sering disebut juga sebagai “*backbone switch*” karena fungsinya sebagai tulang punggung jaringan. *Core switch* adalah salah satu jenis perangkat jaringan yang digunakan untuk mengatur lalu lintas data dalam sebuah jaringan komputer. Core switch biasanya terletak di pusat jaringan dan berfungsi untuk menghubungkan beberapa switch dan *router* untuk membuat jaringan lebih terorganisir dan efisien.

*Core Switch* harus memiliki kecepatan yang sangat tinggi, keandalan yang tinggi, dan fitur yang canggih untuk menjaga ketersediaan jaringan dan memastikan bahwa jaringan selalu berjalan dengan optimal. *Core Switch* juga harus mampu mengelola lalu lintas jaringan yang sangat besar dan memprioritaskan data penting di seluruh jaringan.

**3.2.1.1 Kelebihan Core Switch**

**1. Kecepatan**: *Core Switch* mampu mengirimkan data pada kecepatan yang sangat tinggi karena memiliki prosesor yang sangat kuat.

**2. Ketersediaan**: Dalam sebuah jaringan, *Core Switch* mampu memberikan ketersediaan tinggi dengan memastikan bahwa ada jalur cadangan untuk menghindari terjadinya *downtime*.

**3. Scalability**: *Core Switch* dapat diperluas sesuai dengan kebutuhan jaringan dengan menambahkan modul tambahan.

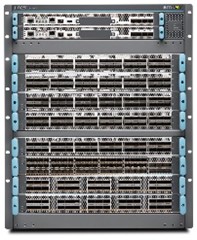
**3.2.1.2 Jenis-jenis Core Switch**

**a. *Fixed Core Switch***: jenis *Core Switch* yang dirancang untuk digunakan dalam jaringan kecil dan menengah, dan memiliki jumlah *port* yang terbatas.



***Gambar 3.1 Fixed Core Switch***

* 1. ***Modular Core Switch***: jenis *Core Switch* yang memiliki slot yang dapat ditempati oleh modul tambahan untuk meningkatkan jumlah *port*.



***Gambar 3.2 Modular Core Switch***

* 1. ***Chassis Core Switch***: jenis *Core Switch* yang memiliki slot yang dapat ditempati oleh modul tambahan dan dirancang untuk digunakan dalam jaringan yang lebih besar.



***Gambar 3.3 Chassis Core Switch***

**3.2.2 Distribution Switch**

*Distribution Switch* adalah *switch* yang terletak diantara *Core Switch* dan *Access Switch*, bertindak sebagai titik fokus utama untuk menghubungkan semua perangkat pada jaringan. *Distribution Switch* bertanggung jawab untuk mengatur lalu lintas jaringan dan untuk memastikan bahwa data dapat diprioritaskan untuk mengoptimalkan kinerja jaringan. *Distribution Switch* juga harus memiliki kecepatan yang cukup tinggi untuk mengelola lalu lintas data yang melewatinya.

**3.2.3 Access Switch**

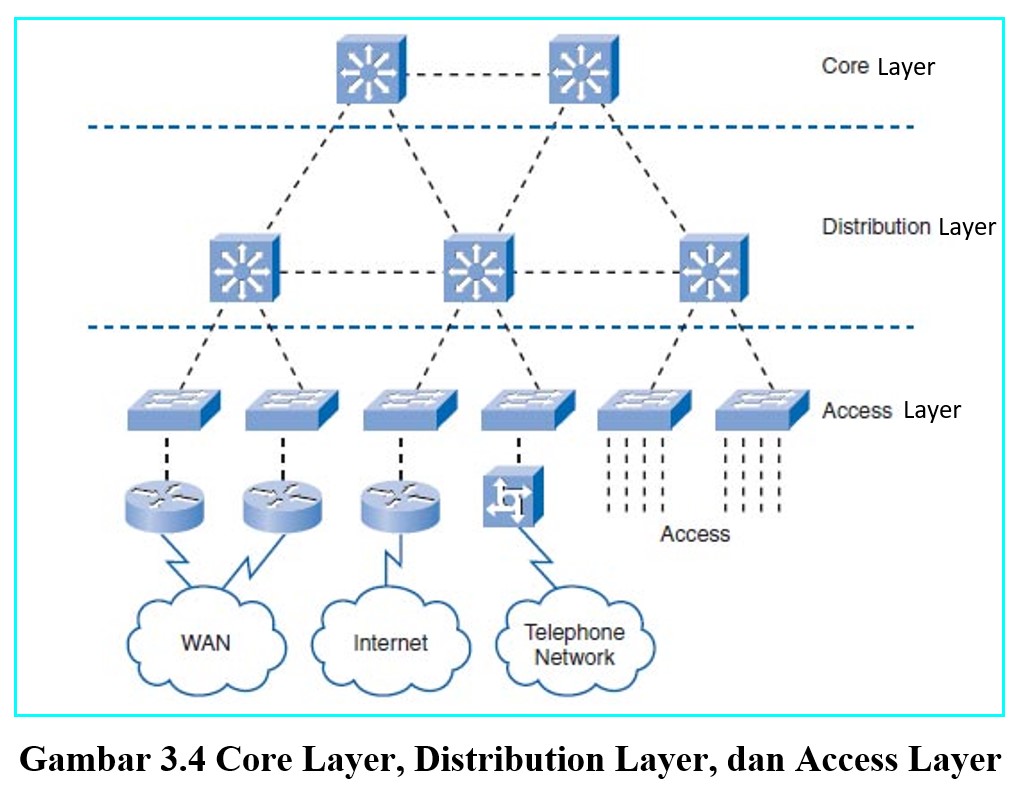
*Acces Switch* adalah *switch* yang terhubung langsung ke perangkat yang digunakan oleh pengguna akhir seperti laptop, printer, atau telepon. *Access Switch* mengatur lalu lintas jaringan untuk perangkat-perangkat ini dan memberikan akses ke jaringan organisasi. *Access Switch* biasanya memiliki kecepatan yang lebih rendah dibandingkan dengan *Distribution Switch* dan *Core Switch*, karena perangkat-perangkat yang terhubung ke *Access Switch* umumnya memerlukan *throughput* data yang lebih sedikit.

**3.3 Perbedaan Antara Core Switch, Distribution Switch, dan Access Switch**

Perbedaan utama antara *Core Switch*, *Distribution Switch* dan *Access Switch* terletak pada posisi dan peran mereka dalam jaringan. *Access Switch* terhubung langsung ke perangkat pengguna akhir, *Distribution Switch* terletak di antara *Core Switch* dan *Access Switch* dan *Core Switch* terletak di pusat jaringan. *Access Switch* bertanggung jawab untuk mengatur lalu lintas jaringan dan memprioritaskan data, sedangkan *Core Switch* bertanggung jawab untuk menghubungkan semua jaringan dan mengelola lalu lintas jaringan yang sangat besar.

**3.4 Kesimpulan**

Sebagai kesimpulan ,*Core Switch*, *Distribution Switch* dan *Access Switch* adalah tiga jenis *Switch* yang berbeda dalam jaringan. *Core Switch* bertanggung jawab untuk menghubungkan semua jaringan dan mengelola lalu lintas jaringan yang sangat besar dan dapat menjaga ketersediaan, kecepatan dan keamanan jaringan, serta mengelola lalu lintas jaringan yang sangat besar dengan efektif dan efisien. *Distribution Switch* bertanggung jawab untuk mengatur lalulintas jaringan dan dan memprioritaskan data, *Access Switch* bertanggung jawab untuk mengatur lalu lintas jaringan untuk perangkat pengguna akhir. Penggunaan *Core Switch*, *Distribution Switch* dan *Access Switch* dapat memberikan manfaat yang signifikan untuk perusahaan atau bisnis dalam mengelola jaringan mereka. Namun, untuk memastikan bahwa perangkat jaringan tersebut berjalan dengan optimal, dibutuhkan penanganan dan manajemen yang tepat. Hal ini termasuk pemasangan, pengaturan dan pemeliharaan perangkat jaringan. Oleh karena itu, kami merekomendasikan jasa manajemen jaringan, maintenance, wiring manajemen, instalasi CCTV, fiber optik, mikrotik, router, server dari perusahaan yang terpercaya.



***Gambar 3.4 Core Layer, Distribution Layer, dan Access Layer***

**Pertanyaan 4**

4. Jelaskan teknologi VPN (*Virtual Private Network*) dan gambarkan fungsi dalam implementasi VPN?

**Jawaban 4**

**Virtual Private Network (VPN)**

Teknologi *Virtual Private Network* (VPN) adalah sebuah metode yang digunakan untuk menciptakan jalur komunikasi aman dan terenkripsi antara perangkat (seperti komputer, *smartphone*, atau tablet) dan jaringan lain melalui internet atau jaringan publik. Dengan menggunakan VPN, pengguna dapat mengakses sumber daya jaringan secara pribadi dan aman seolah-olah mereka terhubung langsung ke dalam jaringan lokal, meskipun sebenarnya mereka berada di lokasi yang berbeda secara geografis.

**4.1 Fungsi VPN**

Fungsi utama dalam implementasi VPN adalah sebagai berikut:

* + - 1. **Keamanan dan Enkripsi Data**

VPN menggunakan teknologi enkripsi yang kuat untuk melindungi data yang dikirim antara perangkat pengguna dan server VPN. Dengan demikian, data sensitif seperti informasi login, rincian keuangan, atau informasi pribadi akan tetap terlindungi dari ancaman potensial seperti penyusup atau peretas.

* + - 1. **Privasi dan Anonimitas**

VPN menyembunyikan alamat IP asli pengguna dengan menggantinya dengan alamat IP server VPN. Ini membuat aktivitas online pengguna menjadi lebih anonim dan mempersulit pelacakan aktivitas mereka oleh pihak ketiga, termasuk penyedia layanan internet (ISP).

* + - 1. **Bypass Pembatasan Geografis**

Beberapa konten dan layanan online mungkin dibatasi berdasarkan lokasi geografis. Dengan menggunakan VPN, pengguna dapat mengubah alamat IP mereka sehingga terlihat seolah-olah mereka berada di wilayah lain yang tidak terkena pembatasan tersebut. Ini memungkinkan akses ke konten yang sebelumnya tidak dapat diakses.

* + - 1. **Akses Jarak Jauh ke Jaringan Perusahaan**

VPN memungkinkan karyawan yang bekerja dari jarak jauh untuk terhubung dengan jaringan perusahaan secara aman. Dengan cara ini, mereka dapat mengakses file, aplikasi, dan sumber daya jaringan internal lainnya seperti yang mereka lakukan saat berada di kantor fisik.

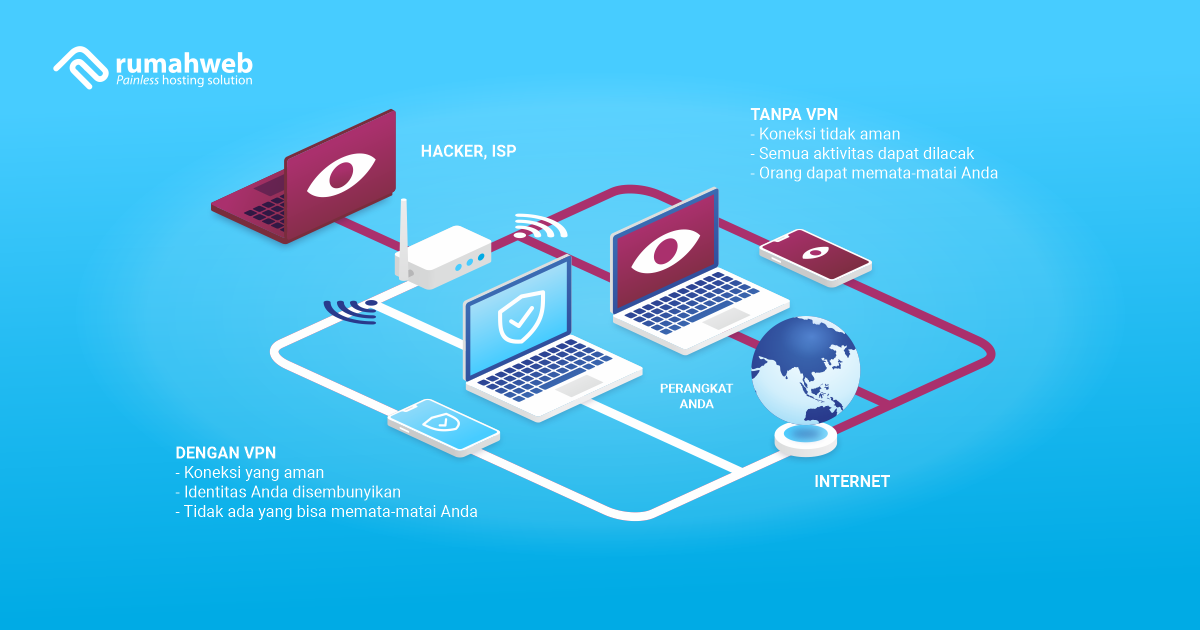
* + - 1. **Keamanan di Jaringan Wi-Fi Publik**

Saat terhubung ke jaringan Wi-Fi publik seperti di kafe, bandara, atau tempat umum lainnya, ada risiko keamanan karena informasi sensitif dapat diakses oleh pihak yang tidak berwenang. Menggunakan VPN di jaringan Wi-Fi publik dapat memberikan tingkat keamanan tambahan, karena data yang dikirimkan dan diterima akan terenkripsi.

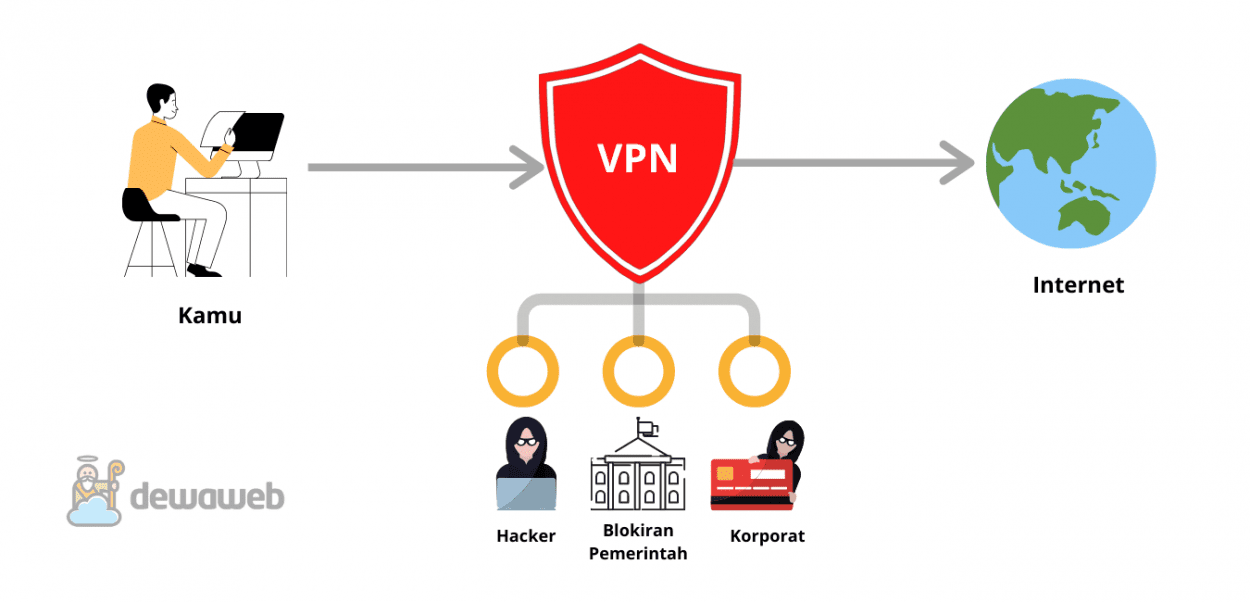
* + - 1. **Menghindari Penyensoran Internet**

Di beberapa negara, ada pembatasan akses ke situs web tertentu atau layanan internet. Dengan menggunakan VPN, pengguna dapat mengakses konten yang diblokir dan menghindari penyensoran internet yang diberlakukan oleh pemerintah atau badan tertentu.

Secara keseluruhan, VPN memberikan solusi aman dan fleksibel untuk mengakses dan mengirimkan data melalui internet, serta memberikan tingkat privasi dan anonimitas yang lebih tinggi bagi pengguna. Meskipun VPN memiliki banyak manfaat, penting untuk diingat bahwa tidak semua layanan VPN diciptakan sama, dan memilih penyedia VPN yang terpercaya dan tepercaya sangatlah penting untuk memastikan keamanan dan kerahasiaan data Anda.



***Gambar 4.1 Fungsi VPN***



***Gambar 4.2 Cara Kerja VPN***

**Pertanyaan 5**

Jelaskan tentang *Network security* dan bagaimana pendapat anda terkait implementasi *network security* yang baik ?

**Jawaban 5**

**Network Security**

*Network security* adalah disiplin keamanan yang berfokus pada melindungi integritas, kerahasiaan, dan ketersediaan data serta sumber daya dalam sebuah jaringan komputer. Tujuan dari *network security* adalah untuk mencegah akses yang tidak sah, perlindungan terhadap perangkat dan infrastruktur jaringan dari serangan, serta mengurangi risiko kehilangan data atau gangguan operasional yang dapat merugikan organisasi atau individu.

* 1. **Pentingnya Network Security**

**1. Melindungi Data Sensitif**: Informasi penting seperti data pelanggan, informasi keuangan, dan rahasia bisnis harus dilindungi dari akses yang tidak sah atau pencurian.

1. **Mencegah Serangan dan Ancaman**: Ancaman seperti peretasan, virus, malware, dan serangan DDoS (*Distributed Denial of Service*) dapat menyebabkan kerusakan besar pada jaringan dan sistem.
2. **Kepatuhan Hukum dan Regulasi**: Banyak industri menghadapi peraturan ketat tentang keamanan data dan privasi, dan *network security* membantu organisasi untuk mematuhi peraturan ini.
3. **Kerahasiaan Komunikasi**: *Network security* juga melibatkan enkripsi data untuk melindungi kerahasiaan dan integritas pesan yang dikirimkan melalui jaringan.
4. **Kontinuitas Bisnis**: Upaya network security juga termasuk dalam perencanaan dan pemulihan bencana, sehingga jaringan dapat tetap berfungsi dengan baik meskipun menghadapi gangguan.

**5.2 Implementasi Network Security yang Baik**

**1. Firewal**l: Menggunakan firewall untuk memantau dan mengendalikan lalu lintas jaringan. *Firewall* berfungsi sebagai filter untuk mengizinkan atau memblokir lalu lintas berdasarkan aturan dan kebijakan yang telah ditetapkan.

**2.** **Pembaruan Keamanan**: Selalu pastikan bahwa semua perangkat, sistem operasi, dan perangkat lunak di jaringan selalu diperbarui dengan patch keamanan terbaru. Ini membantu mengurangi risiko dari kerentanan yang telah diketahui.

**3**. **VPN (Virtual Private Network)**: Menggunakan VPN untuk mengamankan komunikasi dan data saat berkomunikasi melalui jaringan publik atau ketika bekerja dari lokasi eksternal.

**4.** **Kontrol Akses**: Terapkan pengendalian akses yang ketat dengan memberikan hak akses yang tepat kepada pengguna dan perangkat yang berwenang untuk mengakses sumber daya jaringan tertentu.

**5.** **Enkripsi**: Pastikan data sensitif dienkripsi baik saat berada dalam penyimpanan maupun dalam perjalanan melalui jaringan.

**6.** **Monitoring dan Analisis**: Menerapkan sistem pemantauan dan analisis keamanan untuk mendeteksi aktivitas yang mencurigakan atau anormal yang dapat mengindikasikan upaya peretasan atau serangan.

* + - 1. **Pelatihan Keamanan**: Melibatkan seluruh personel dalam pelatihan keamanan untuk meningkatkan kesadaran tentang risiko keamanan dan praktik terbaik.
      2. **Rencana Pemulihan Bencana**: Memiliki rencana pemulihan bencana yang terperinci untuk mengatasi serangan atau gangguan yang dapat terjadi pada jaringan.
      3. **Audit Keamanan**: Secara berkala melakukan audit keamanan untuk mengevaluasi keefektifan kebijakan dan sistem keamanan yang ada.
      4. **Kesadaran Tentang Ancaman**: Terus menerus memantau dan meningkatkan pemahaman tentang tren keamanan terkini dan ancaman yang berkembang.

Pendekatan terbaik dalam implementasi *network security* adalah adopsi pendekatan berlapis, dengan menggabungkan berbagai lapisan pertahanan dan menggunakan berbagai teknologi keamanan untuk melindungi jaringan secara keseluruhan. Selain itu, penting untuk memiliki rencana *respons insiden* yang efektif, sehingga jika terjadi pelanggaran keamanan, tanggapan yang cepat dan tepat dapat dilakukan untuk mengurangi dampak dan mengembalikan jaringan ke keadaan yang aman.

**Referensi**

Nogroho, A. (2021, Juli 30). *VLAN: Pengertian, Fungsi dan Cara Kerjanya*. Diambil kembali dari Qwords.com: https://qwords.com/blog/vlan-adalah/. Diakses pada 28 Juli 2023.

Zaky, A. (2023, Februari 27). *Apa Itu Core Switch dan Fungsinya dalam Jaringan?* Diambil kembali dari Generalsolusindo.com: https://generalsolusindo.com/apa-itu-core-switch-dan-fungsinya-dalam-jaringan/. Diakses pada 29 Juli 2023.

Dewaweb. (2022, Oktober 13). *Apa itu VPN? Fungsi, Cara Menggunakan, Kelebihan dan Kekurangannya*. Diambil kembali dari Dewaweb.com: https://www.dewaweb.com/blog/apa-itu-vpn/. Diakses pada 29 Juli 2023.

Pugguh, A. (2021, Juli 14). *Apa itu VPN? Pengertian, Fungsi dan Cara Kerjanya*. Diambil kembali dari Rumahweb.com: https://blog.rumahweb.com/vpn-adalah/. Diakses pada 29 Juli 2023.

**Link File**

https://drive.google.com/file/d/1S4ug1OD-OCkCSLx\_DcuaGdBwpALCQjAo/view?usp=sharing



TERIMA KASIH

**Tabel Nilai**

|  |  |  |
| --- | --- | --- |
| **Nilai** | **Tanda Tangan Dosen Pengampu / Tutor** | **Tanda Tangan Mahasiswa** |
|  | **(** **Muhammad Ikhwani Saputra, S.Kom.,M.Kom. )** | **(Hendro Gunawan)** |
|  | Diserahkan pada Tanggal: | Tanggal Mengumpulkan: |
|  |  | 29/07/2023 |