BAB II
DASAR TEORI

2.1 Pendesainan Jaringan Nirkabel

Pembangunan sebuah jaringan nirkabel tidak bisa dilakukan tanpa ada perencanaan yang jelas. Menurut McCullough [2001:166] terdapat 6 fase pembangunan jaringan wifi. Penjelasan langkah - langkahnya terdapat pada poin – poin berikut ini.

a. Investigasi awal

   Pada fase proses desain, tujuan utamanya adalah mempelajari sebanyak - banyaknya tentang jaringan yang akan dibangun untuk memahami dan mengungkap masalah atau peluang yang ada. Dalam tahap ini dikumpulkan rencana dasar topologi, penggunaan jaringan, dan kemungkinan jadwal perawatan.

b. Analisa Lingkungan Sekitar

   Meskipun sistem nirkabel berurusan dengan fisik dan Data-Link layer (Layer 1 dan 2 dari model OSI), akan tetapi, tidak seperti jaringan kabel, akses ke jaringan nirkabel berlangsung melalui udara antara PC klien dan titik akses nirkabel (AP). Akibatnya, harus dipastikan bahwa pengguna mendapatkan akses pada tempat yang layak dalam jaringan Anda.

c. Desain Awal

   Pada proses ini, informasi yang ada harus disatukan dan di konsep untuk dijadikan sebuah topologi. Topologi jaringan yang baik akan memberikan pemahaman pada pembaca yang menyeluruh dari semua elemen lokasi fisik, jenis koneksi dan kecepatan mereka.

d. Finalisasi Desain

   Setelah menyelesaikan rancangan awal dan diterima oleh pelanggan dan setuju untuk melanjutkan, maka langkah yang terkahir adalah melakukan perincian desain. Perincian ini harus dilakukan sebelum mengimplementasikan desain Anda. Tujuan dalam tahap ini adalah untuk menyelesaikan perancangan dan mengetahui semua *software* pendukung dan peralatan yang diperlukan pada akhir *Bill of Material* (BOM).

e. Implementasi

Tahap ini melibatkan penginstalan, pengkonfigurasian, dan pengujian semua perangkat keras pendukung dan perangkat lunak yang telah ada dalam desain. Kunci dalam tahap proses ini adalah meminimalkan dampak pada jaringan dan penggunanya, sekaligus memaksimalkan upaya instalasi efektif yang diperlukan oleh desain jaringan baru

f. Pembuatan Dokumentasi

Pada proses ini adalah membuat sebuah dokumentasi dengan fokus utama adalah untuk menjaga vitalitas dan fungsi dari jaringan dengan menggabungkan semua informasi jaringan dan sistem yang relevan untuk referensi di masa mendatang. Meskipun dokumen pemikiran sebelumnya mungkin memerlukan beberapa modifikasi, banyak yang dapat diperoleh dari desain jaringan dan proses implementasi sebelumnya.

2.2 IP (Internet Protokol)

2.2.1 Pengertian IP

Internet Protocol (IP) merupakan protokol yang dapat mengetahui semua interkoneksi jaringan. IP bisa melakukan ini semua karena semua mesin di dalam jaringan mempunyai alamat *software* atau logikal yang disebut alamat IP. IP melihat alamat dari tiap paket kemudian dengan menggunakan *routing table* menentukan ke mana selanjutnya paket itu dikirim melalui jalur yang terbaik.

IP menerima segmen dari layer *Host – to – Host* kemudian memfragmentasi mereka menjadi datagram (paket – paket) jika diperlukan. IP lalu menata kembali datagram tersebut menjadi segmen pada sisi penerima data. Setiap paket atau diagram dilengkapi dengan alamat IP dari pengirim dan penerima. Setiap *router* (alat yang berada pada layer 3) yang menerima datagram membuat keputusan *routing* berdasarkan alamat IP tujuan paket tersebut. [CIS-05:85]

2.2.2 Pengalamatan IP (Internet Protokol)

Pengalamatan IP adalah pengidentifikasian dengan angka yang diberikan ke setiap mesin di dalam jaringan IP. Pengalamatan IP digunakan untuk menunjukkan lokasi spesifik dari alat di dalam jaringan.

Alamat IP adalah alamat *software*, bukan alamat *hardware* – yang terpatri ke dalam *Network Interface Card* (NIC) dan digunakan untk menemukan *host* pada jaringan lokal. Pengalamatan IP ditujukan untuk memungkinkan *host* pada jaringan yang berbeda, tanpa memperdulikan tipe dari LAN yang digunakan oleh *host* yang berpartisipasi. [CIS-05 : 97]

IP *address* berupa bilangan biner 32 bit dan ditulis sebagai 4 urutan bilangan desimal yang dipisahkan dengan tanda titik. Format penulisan IP adalah : xxxxxxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx, dengan x adalah bilangan biner 0 atau 1. Dalam implementasinya IP *address* ditulis dalam bilangan desimal dengan bobot antara 0 – 255 (nilai desimal mungkin untuk 1 byte). IP *address* terdiri dari bagian jaringan dan bagian *host*, tapi format dari bagian-bagian ini tidak sama untuk setiap IP *address*.

Jumlah bit alamat yang digunakan untuk mengidentifikasi jaringan, dan bilangan yang digunakan untuk mengidentifikasi *host* berbeda-beda tergantung kelas alamat yang digunakan. Dalam jenis pengalamatan IP secara *classfull*, ada tiga kelas alamat utama, yaitu kelas A, kelas B, dan kelas C. Dengan memeriksa beberapa bit pertama dari suatu alamat *software* IP bisa dengan cepat membedakan kelas *address* dan strukturnya. [TCP-11: 04]

Tabel 2.1. Kelas IP *Address* [BOS-10 : 01]

Kelas	**Oktet Pertama**	**Subnet**	**Jumlah *Host***	**Catatan**
Kelas A	1 – 126	Net.H.H.H	16.777.214	Umum
Kelas B	128 – 191	Net.Net.H.H	65.534	Umum
Kelas C	192 – 223	Net.Net.Net.H	256	Umum
Kelas D	224 – 239	Unknown	Unknown	Multicast
Kelas E	240 – 255	Unknown	Unknown	InterNIC

Classless addressing disebut juga sebagai pengalamatan tanpa kelas. Classless addressing Saat ini mulai banyak diterapkan, yakni dengan mengalokasikan IP address dalam notasi Classless Inter Domain Routing (CIDR). Istilah lain yang digunakan untuk menyebut bagian IP address yang menunjuk suatu jaringan secara lebih spesifik disebut juga dengan Network Prefik. Biasanya dalam menuliskan network prefix suatu kelas IP address digunakan tanda garis miring (slash) "/" diikuti dengan angka yang menunjukkan panjang network prefix dalam bit. [MUB-06 : 2]

2.3 *Standard* 802.11

Standar IEEE 802.11 mendefinisikan *Medium Access Control (MAC)* dan *Physical (PHY)* untuk jaringan nirkabel. Standar tersebut menjelaskan jaringan lokal dimana peralatan yang terhubung dapat saling berkomunikasi selama berada dalam jarak yang dekat satu sama lain. Standar ini hamper sama dengan *IEEE 802.3* yang mendefinisikan *Ethernet*, tapi ada beberapa bagian yang khusus untuk transmisi data secara nirkabel. [802-11 : 01]

Pada Standar 802.11 mendefinisikan tiga tipe dari *physical layer* yaitu *Frequency Hopping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum (DHSS) dan* infra merah. Infra merah jarang sekali dipakai karena jangkauannya yang sangat dekat. Tidak semua dari keluarga 802.11 menggunakan *Physical Layer* yang sama dan mendapatkan kecepatan transmisi data yang sama. Berikut ini adalah tabel standar dari jenis 802.11 yang paling sering digunakan.

Tabel 2.2. Standarisasi jenis 802.11 [802-11 : 4]

STANDAR IEEE	NAMA	DESKRIPSI
802.11a	Wifi5	Standar 802.11a (disebut WiFi 5) memungkinkan *bandwidth* yang lebih tinggi (54 Mbps *throughput* maksimum, 30 Mbps dalam praktek). Standar 802.11a mengandung 8 saluran radio di pita frekuensi 5 GHz .
802.11b	Wifi	Standar 802.11b saat ini yang paling banyak

		digunakan satu. Menawarkan *throughput* maksimum dari 11 Mbps (6 Mbps dalam praktek) dan jangkauan hingga 300 meter di lingkungan terbuka. Ia menggunakan rentang frekuensi 2,4 GHz, dengan 3 saluran radio yang tersedia
802.11g		Standar 802.11g menawarkan *bandwidth* yang tinggi (54 Mbps *throughput* maksimum, 30 Mbps dalam praktek) pada rentang frekuensi 2,4 GHz. Standar 802.11g juga kompatibel dengan standar 802.11b, yang berarti bahwa perangkat yang mendukung standar 802.11g juga dapat bekerja dengan 802.11b.

802.11b paling banyak digunakan saat ini, karena cepat dan mudah diimplemtasikan, dan tersedia banyak sekali produk yang tersedia dipasaran. Mendukung kecepatan transmisi data sampai 11Mbps, tetapi jika sinyal radio melemah, maka kecepatan akan diturunkan ke 5.5 Mbps, 2 Mbps, dan 1 bps untuk menjamin agar komunikasi tidak terputus. 802.11b seringkali disebut juga *WiFi (Wireless Fidelity)* karena *Wi-Fi Alliance* yang bertanggung jawab untuk pengetesan dan sertifikasi untuk dapat bekerja dengan produk jaringan yang berdasarkan 802.11 lainnya. [802-11 : 4]

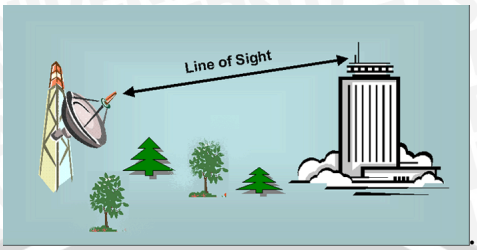
2.4 Parameter *Radio Point to Point*

2.4.1 *Line of Sight*

Istilah *Line of Sight* sering kali disingkat sebagai LOS, sangat mudah untuk dimengerti jika berbicara tentang cahaya tampak. Jika titik B dapat dilihat dari titik A dengan tidak ada penghalang antara A dan B, maka itulah kondisi yang disebut *Line of Sight*.

Konsep *Line of Sight* menjadi lebih kompleks jika menggunakan gelombang mikro. Ingat bahwa sebagian besar karakteristik perambatan gelombang elektromagnetik tergantung pada panjang gelombangnya. Hal ini kira-kira mirip dengan pelebaran gelombang pada saat gelombang tersebut berjalan. Panjang gelombang cahaya sekitar 0.5 mikrometer, sementara gelombang mikro yang digunakan dalam jaringan wireless mempunyai

panjang gelombang beberapa centimeter. Konsekuensinya, pancaran gelombang mikro akan lebih lebar.

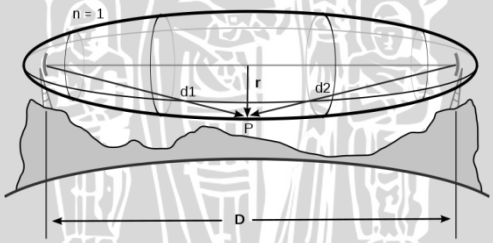


Gambar 2.1 Line of Sight

Jadi *Line of Sight* yang dibutuhkan agar dapat terjadi sambungan wireless yang optimal antara A dan B sebetulnya lebih dari sekedar garis lurus yang tipis akan tetapi lebih berbentuk cerutu atau sebuah elips. [WND-11 : 23]

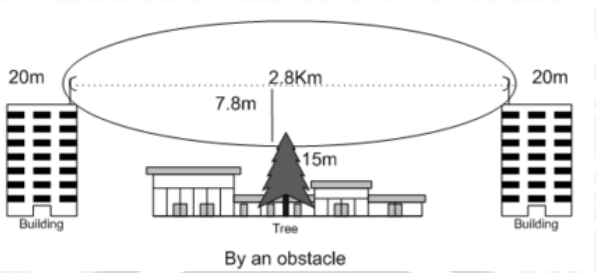
2.4.3 *Fresnel Zone*

Konsep *Fresnel Zone* adalah pusat banyak bidang pencitraan. Dalam pencitraan tomografi, yang melintang resolusi spasial dapat dibatasi oleh ukuran dari *Fresnel Zone* pertama, biasanya didefinisikan hanya untuk monokromatik radiasi. [PEA-02:1]



Gambar 2.2 *Fresnel Zone* [FRE-11 : 1]

Zona Fresnel yang terjadi dalam pembuatan jaringan nirkabel cukup banyak, akan tetapi konsentrasi yang diperlukan cukup pada zona pertama karena sinyal terkuat terdapat pada daerah ini. Jika daerah ini diblokir oleh obstruksi, misalnya pohon atau bangunan, maka sinyal yang diterima receiver akan berkurang. Untuk itu diperlukan kepastian bahwa zona ini harus bebas dari penghalang. Sehingga dalam pembangunan jaringan nirkabel harus diperiksa bahwa daerah *Zona Fresnel* bebas dari pemblokan sinyal minimal 60 persen oleh halangan yang ada. [VIA-11 : 1]



Gambar 2.3 Pemblokan sinyal oleh halangan pada *Fresnel Zone*

[FRE-11 : 1]

Penghitungan daerah *Fresnel Zone* adalah dengan menggunakan rumus [BUT-09:05]

$$r = 17{,}31 \times \sqrt{\frac{d}{4f}}$$

Keterangan :

r = radius dari zona dalam meter,

d = jarak *link* total dalam meter

f = frekuensi dalam MHz.

2.5 *Virtual Private Network* (VPN)

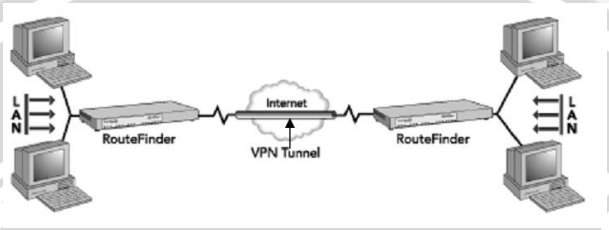
2.5.1 Pengertian VPN

VPN adalah konsep yang menggunakan internet sebagai transit untuk lalu lintas jaringan pribadi, biasanya dalam bentuk terenkripsi. Hal ini juga kadang - kadang disebut sebagai data jaringan yang menggunakan internet daripada *leased line* untuk koneksi. Keamanan dijamin oleh sarana sambungan terowongan di mana informasi seluruh paket (isi dan header) dienkripsi dan dikemas. Karena ini paling sering didefinisikan, *virtual private network* (VPN) memungkinkan dua atau lebih jaringan pribadi untuk dapat terhubung melalui jaringan publik yang diakses.

2.5.2 Sistem Kerja VPN

Organisasi yang menggunakan internet untuk pembangunan jaringan pribadi, mengamankan koneksi antara kantor cabang dan / atau

karyawan. Setiap pengguna *remote* menghubungkan ke ISP lokal dengan cara yang sama yang digunakan untuk akses internet: *dial-up*, kabel, DSL, ISDN, T1 atau nirkabel. Sebuah proses yang disebut "*tunneling*" yang digunakan untuk membawa data melalui Internet. Namun, *tunneling* sendiri tidak menjamin keprivasian. Untuk mengamankan transmisi *tunneling* terhadap intersepsi, semua lalu lintas melalui VPN dienkripsi untuk keamanan.



Gambar 2.4. VPN melalui Internet [VPN-11 : 01]

Pada dasarnya, *tunneling* adalah proses menempatkan seluruh paket data dalam paket lain (yang menyediakan informasi *routing*) dan mengirimkannya melalui Internet. Jalan yang dilalui dalam perjalanan paket disebut terowongan. Untuk terowongan yang akan didirikan, baik terowongan klien dan terowongan server harus menggunakan protokol *tunneling* yang sama. Hal yang membuat *Virtual private network* "secara *virtual private*" adalah *tunnel* / terowongan. Meskipun jaringan organisasi diakses melalui internet, pengguna tidak benar-benar "pada" internet, tetapi pengguna sebenarnya "ada pada" jaringan perusahaan / organisasi pengguna. Seperti halnya lalu lintas internet, terowongan data paket VPN perusahaan dapat mengambil jalur yang berbeda antara dua *endpoint*. Yang membuat transmisi terowongan VPN adalah bahwa sebenarnya hanya penerima pada ujung lain dari transmisi pengguna yang dapat melihat ke dalam pelindung enkripsi pengguna.

Oleh karena itu *Virtual Private Networks* (VPN) memungkinkan sebuah bisnis untuk menggunakan internet sebagai jaringan berdedikasi sendiri . Hal ini memungkinkan karyawan, kantor cabang, dan pelanggan terpilih, untuk berbagi informasi dan melakukan tugas – tugas administrasi rutin, rahasia dan aman dari setiap lokasi. [VPN-11 : 01]

2.5.3 OpenVPN

OpenVPN adalah *opensource* server VPN yang mudah untuk diatur dan digunakan dengan *opensource* VPN klien. Pengguna dapat dengan mudah mengekspor konfigurasi file dari OpenVPN untuk diimpor ke berbagai *opensource* dan komersial klien. OpenVPN juga terintegrasi ke dalam beberapa paket router *firmware* termasuk yang populer DD-WRT, OpenWRT, dan Tomat. Sistem OpenVPN tidak kompatibel dengan penyedia VPN komersial yang populer, tetapi menyediakan *opensource* dan alternatif bebas untuk menyiapkan VPN untuk model komersial yang mahal dan tertutup. [OPE-11: 1]

Dalam OpenVPN terdapat metode pengiriman data yaitu metode TUN dan metode TAP. TUN adalah sebuah *device point to point IP Link*, dimana implementasi OpenVPN menggunakan *routing*. Hal ini dikarenakan metode TUN akan me–*routing* seluruh klien yang terhubung ke server. Sedangkan TAP adalah sebuah *device virtual ethernet*, dimana implementasi OpenVPN menggunakan *bridging* sehingga mampu menangkap *frame Ethernet* yang tentu saja berbeda dengan TUN. Dengan menggunakan *bridging*, VPN Klien bisa mendapatkan IP yang satu subnet dengan VPN Server. (MAR-06:32)

OpenVPN merupakan aplikasi VPN satu – satunya yang mampu untuk mentransmit data antar klien sehingga memudahkan kita untuk saling berinteraksi. Beberapa kelebihan dari OpenVPN adalah sebagai berikut :

a. Mendukung Layer 2 dan Layer 3
b. Koneksi OpenVPN dapat di-*tunnel*-kan melewati hampir setiap *firewall*
c. Dukungan dan pengkonfigurasian *proxy*
d. Tidak ada masalah dengan NAT (*Network Address Translation*)
e. Penginstalan yang mudah pada semua platfrom

Cara kerja OpenVPN dalam mengantarkan data adalah OpenVPN mendengarkan perangkat TUN / TAP dan mengambil jalur lalu lintas data. Data yang akan dikirim dienkripsi kemudian dikirim ke klien VPN yang

lain. Oleh klien OpenVPN yang lain proses penerimaan data, kemudian data didekripsi, dan diberikan ke perangkat jaringan virtual, di mana data ditunggu oleh aplikasi.

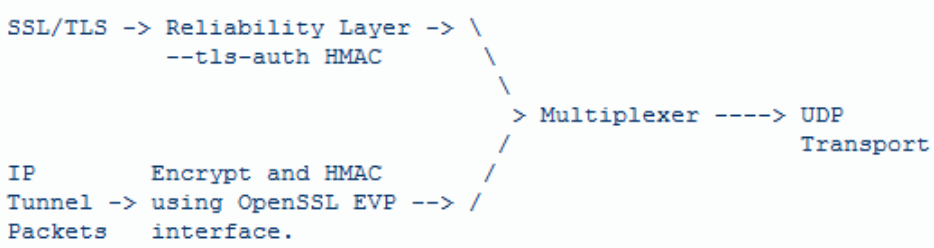
2.5.4 Sistem Keamanan OpenVPN

Aplikasi OpenVPN memiliki dua mode autentikasi :

a. Static Key - menggunakan kunci statis berbagi
b. TLS - menggunakan SSL/TLS dan sertifikat untuk otentikasi dan pertukaran kunci

Pada mode kunci statis, sebuah kunci berbagi dihasilkan dan dibagi antara kedua pengguna OpenVPN (server - klien) sebelum *tunnel* dimulai. Kunci statis ini berisi 4 kunci independen yaitu HMAC (*Hash-based Message Authentication Code*) pengirim, HMAC penerima, enkripsi dan dekripsi. HMAC adalah konstruksi spesifik untuk menghitung kode otentikasi pesan (*Message Authentcation Code / MAC*) yang melibatkan fungsi hash kriptografi dalam kombinasi dengan kunci rahasia. Secara *default* pada mode kunci statis, kedua *host* akan menggunakan kunci HMAC yang sama dan kunci enkripsi / dekripsi.

Pada mode SSL/TLS, sebuah *session* SSL dibangun dengan otentikasi dua arah (klien - server). Jika otentikasi SSL/TLS otentikasi sukses, maka enkripsi/dekripsi dan sumber material kunci HMAC secara acak dihasilkan oleh OpenSSL fungsi RAND_bytes dan ditukar melalui koneksi SSL/TLS. Kedua sisi koneksi memberikan sumber material acak. Mode ini tidak pernah menggunakan kunci secara dua arah apapun, bahkan kunci - kunci tersebut dihasilkan dari sumber material acak menggunakan fungsi TLS PRF. Jika metode kunci 2 digunakan, kunci dihasilkan secara langsung dari fungsi OpenSSL Rand_bytes. Metode kunci ini digunakan secara *default* pada OpenVPN 2.0



Gambar 2.5. Aliran data melalui UDP [OPP-11:1]

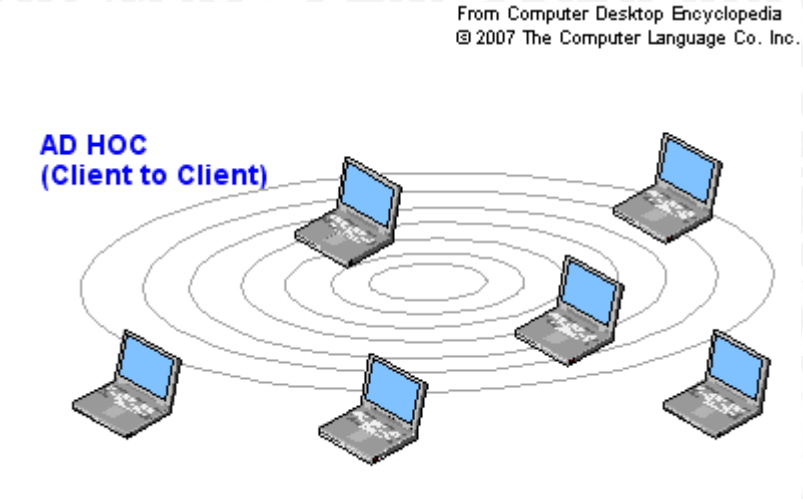
Model ini memiliki keuntungan bahwa SSL/TLS melihat transpot layer yang dapat diandalkan selama pengalih IP paket melihat sebuah transport layer yang tidak dapat diandalkan tentu saja kedua komponen ingin melihat. Keandalan dan otentikasi layer yang secara komplit bebas dari salah satunya, contohnya nomor sekuensial dimasukkan ke dalam amplop HMAC yang ditandai dan tidak digunakan untuk proses otentikasi. [OPP-11:1]

2.6 Topologi Jaringan

Topologi pada dasarnya adalah peta dari sebuah jaringan. Topologi jaringan pada umumnya terbagi lagi menjadi dua, yaitu topologi secara fisik (*physical topology*) dan topologi secara logika (*logical topology*). Topologi secara fisik menjelaskan bagaimana susunan dari kabel dan komputer dan lokasi dari semua komponen jaringan. Sedangkan topologi secara logika menetapkan bagaimana informasi atau aliran data dalam jaringan.

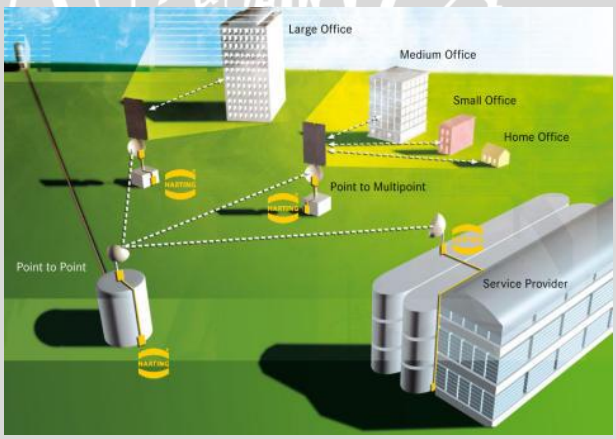
Wireless Fidelity (WiFi) memiliki dua jenis topologi jaringan yang khusus yaitu topologi *ad hoc* dan topologi infrastruktur. Penggunaan topologi ini disesuakan dengan kebutuhan jaringan yang akan digunakan.

Topologi *ad hoc* adalah topologi *WiFi* dimana komputer maupun *mobile station* terhubung secara langsung tanpa menggunakan AP. Jadi komunikasi langsung dilakukan me!alui masing – masing perangkat *wireless* yang terdapat pada komputer atau perangkat komunikasi lainnya. Prinsip kerja *ad hoc* sarna dengan prinsip kerja *peer to peer*. [DIG-11: 1]



Gambar 2.6 Topologi *Adhoc* [IMA-11:1]

Topologi infrastructure adalah topologi *WiFi* dimana komputer-komputer maupun *mobile stasions* dalam suatu jaringan terhubung melalui AP. Jadi setiap komputer maupun *mobile station* yang hendak berhubungan satu sama lain harus melewati AP terlebih dahulu, baru kemudian dapat menggunakan sumber daya yang ada pada jaringan. [DIG-11: 1]



Gambar 2.7 Topologi Infrasturktur [HAR-11:1]

2.7 Parameter QoS (*Quality of Service*)

QoS (*Quality of Service*) mengacu pada kemampuan sebuah jaringan untuk mendukung layanan yang lebih baik untuk memilih lalu lintas jaringan melalui berbagai teknologi, seperti *Ethernet* dan jaringan

802.1.Tujuan utama dari QoS adalah untuk mendukung prioritas termasuk *bandwidth* yang aktual, pengontrolan *jitter* dan *latency*. (INT-12:49-1).

Penelitian ini menggunakan 3 (tiga) parameter QoS yang diujikan dalam 2 (dua) jenis pengujian yaitu *Troughput*, *Delay*, dan *Packet Loss* pada Pengujian LOS (*Line Of Sight*) dan Pengujian Metode OpenVPN. Adapun pengertian dari masing – masing parameter tersebut adalah sebagai berikut :

a. *Throughput*, adalah kecepatan (rate) transfer data efektif, yang diukur dalam Bps, [DIK-11:309]. Pernyataan ini mendukung logika bahwa semakin besar *troughput* suatu aplikasi dalam jaringan maka semakin baik pula hal tersebut. Nilai Toughput didapatkan dari rumus berikut :

$$Troughput\ (Bps) = \frac{Ukuran\ File\ yang\ diterima\ (B)}{Waktu\ Aktual\ Pengiriman\ (s)}$$

[DEW-03:2]

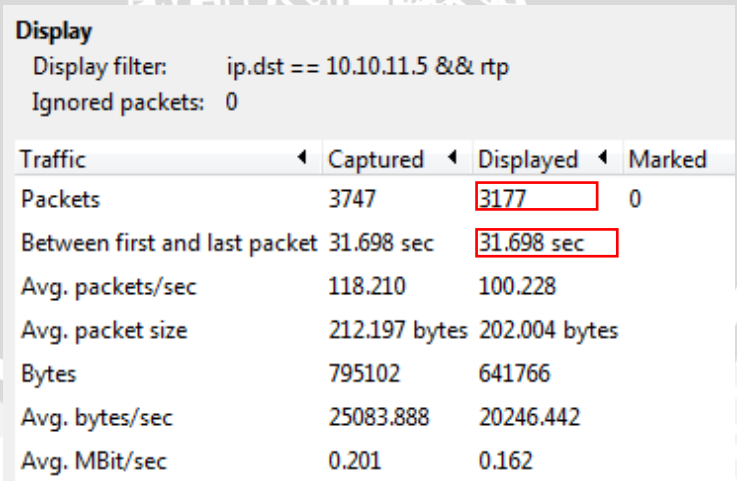
Tabel 2.3. Beberapa contoh aplikasi dan *throughput* [WND-11 : 70]

APLIKASI	**BW / PENGGUNA**	**CATATAN**
Web	50-100+ kbps	*Web browser* hanya menggunakan jaringan bila ada data yang diminta. Komunikasi adalah asinkron, sehingga *lag* sampai jumlah tertentu masih dapat di tolerir
Streaming audio	96-160 kbps	Setiap pengguna layanan streaming audio akan menggunakan bandwith yang relatif besar secara konstan selama direquest.
Voice over IP (VoIP)	24-100 kbps	VoIP menggunakan *bandwidth* yang konstan untuk setiap pengguna selama panggilan. *Bandwidth* yang digunakan adalah dua arah dan sama besarnya.
Streaming	64-200 kbps	*Streaming video* memerlukan *throughput*

video		yang tinggi dan latensi rendah untuk bekerja dengan benar.
Peer-to-peer aplikasi *file sharing*	0-tidak terbatas Mbps	Aplikasi ini cenderung menghabiskan semua *bandwidth* yang tersedia dengan cara mengirim ke sebanyak dan secepat mungkin klien.

b. *Delay*, adalah waktu tunda saat paket yang diakibatkan oleh proses transmisi dari satu titik lain yang menjadi tujuannya. [DIK – 11 : 312]. Pernyataan ini mendukung logika bahwa semakin kecil *delay* maka semakin bagus nilai suatu jaringan. Nilai *Delay* dalam aplikasi Wireshark diambil dari data Time.Delta yang ditampilkan dari oleh setiap frame data. Jika data yang diambil lebih dari 1 (satu) frame maka total waktu yang diterima dibagi dengan total waktu yang diterima. Nilai ini bisa diambil dengan data yang ditunjukkan oleh aplikasi Wireshark. Rumusnya akan seperti ini :

$$Delay = \frac{Total\ waktu\ yang\ dilakukan\ untuk\ pengiriman\ paket}{Jumlah\ total\ paket\ yang\ dikirim}$$



Gambar 2.7. Data yang ditampilkan oleh aplikasi Wireshark

Menurut Diktat TI Telkom yang mengutip rekomendasi ITU - T G.114 tentang *delay* maka nilai *delay* dibagi atas 3 (tiga) range. Hal ini ditunjukkan oleh tabel berikut.

Tabel 2.4. Rekomendasi ITU – T G.114 [DIK – 11 : 314]

No.	Range	Deskripsi
1.	0 – 150 msec	Masih dapat diterima oleh sebagaian besar pengguna aplikasi
2.	150 – 400 mse	Diterima asalkan administrator menyadari transmisi waktu dan dampaknya pada transmisi kualitas pengguna aplikasi
3.	> 400 msec	Tidak dapat diterima untuk jaringan umum

c. *Packet Loss*, adalah banyaknya paket yang hilang selama proses transmisi dari sumber ke tujuan. Nilai *packet loss* selama proses transmisi dari sumber ke tujuan adalah sebagai berikut :

$$Packet\ Loss = \frac{Packet\ Transmited - Packet\ Received}{Packet\ Transmitted} \times 100\%$$

[HAY-10:02]

Menurut [DIK-11:311], kategori penilaian terhadap *Packet Loss* dibagi menjadi 4 (empat) yaitu Sangat Bagus, Bagus, Sedang, dan Jelek. Untuk lebih jelasnya perhatikan tabel berikut :

Tabel 2.5 Kategori Penilaian *Packet Loss* [DIK-11:312],

No.	Prosentase	Kategori
1.	0 %	Sangat Bagus
2.	3 %	Bagus
3.	15 %	Sedang
4.	25%	Jelek