BAB II
DASAR TEORI

2.1. TEKNOLOGI *INFRARED, BLUETOOTH dan WIRELESS FIDELITY* (WiFi)

Teknologi *Infrared, Bluetooth, Wireless Fidelity* (WiFi) adalah suatu teknologi yang memungkinkan untuk melakukan interkoneksi data tanpa menggunakan media kabel. Antara satu teknologi dengan teknologi ini mempunyai standar masing-masing. [16]

2.1.1 *Infrared*

Teknologi *infrared* adalah teknologi pertama dan paling memasyarakat, sudah sangat umum yang terdapat dipengendali yang beredardi pasaran, misalnya *remote* tv. Prinsip kerjanya sangat sederhana, *processor* kecil pada remote akan menterjemahkan penekanan tombol menjadi intruksi bahasa mesin (bilangan biner) yang dikirimkan melalui *infrared* ke TV. Dan data diubah kembali menjadi instruksi yg dikenal TV. [16]. Konsorsium yang mengatur dan egurusi *infrared* adalah (IrDA) *Infrared* Data *Associate*, *infrared* memiliki panjang gelombang sekitar 875 nm. *Infrared* sebenarnya memiliki dua versi yaitu

versi 1.0 memiliki kecepatan dari 0,576 hingga 115,2 kbps, sementara versi 2.0 memiliki kecepatan 0,576 hingga 1,152 Mbps. Namun *infrared* memliki beberapa kekurangan yaitu [16]:

- Setiap *devices* harus terarah dan "bertatap muka" langsung karena *infrared* menggunakan sinyal terarah dan biasnya hanya 30 derajat.
- Teknologi yang cukup tua, kecepatan yang sangat terbatas
- Jarak yang sangat terbatas dan tidak flesibel, serta tidak *mobiles*

2.1.2 *Bluetooth*

Teknologi ini dipelopori oleh Ericsson yang saat ini mulai menggusur dominasi *infrared* untuk perangkat bergerak (HP, PDA), teknologi ini sudah dikembangkan oleh sebuah konsursium yaitu *bluetooth Special Interest Group* (SIG). Cakupan *Bluetooth* dapat mencapai 10 meter dan tidak terhalang flesibelitas media, berbeda dengan media lainya seperti *infrared* atau WiFi, *Bluetooth* memungkinkan koneksi antar piranti elektronik apa aja dan bukan hanya komputer. *Bluetooth* dapat dibuat membentuk PAN atar perangkat seperti

computer, HP, PDA Kamera, *bar-code reader*, perangkat *audio video* bahkan sampai perangkat dapur. [16]

Bluetooth bekerja dengan menggunakan signal radio pada frekuensi 2,4 Ghz yang sama dengan WiFi untuk menghindari interpretensi maka Bluetooth bekerja dengan cara *Frequency Hopping Spread Spectrum* (FHSS). *Frequency Hopping Spread Spectrum* adalah teknik *spread spectrum* yang menggunakan teknik lompatan frekuensi yang berubah-ubah pada sinyal *carrier* untuk membawa suatu data informasi. Sinyal *carrier* atau sinyal pembawa mengubah-ubah frekuensi, atau melompat menurut urutan yang bersifat *pseudorandom*.

Pada saat perangkat *Bluetooth* akan terkoneksi maka perangkat harus melakukan *hopping sequence* agar dapat saling mengenali, Secara teoritis kecepatannya 1 Mbps, namun kecepatan efektifnya hanya 721 Kbps, ini untuk standar Bluetooth 1.1, sedangkan untuk standar 1.0 mempunyai kecepatan hanya 420 Kbps. [16]

2.1.3 *Wireless Fidelity* (WiFi)

Wireless Fidelity, teknologi ini pada awalnya untuk menghilangkan permasalahan kabel dalam membangun sebuah jaringan komputer, WiFi bekerja pada frekuensi sama dengan *Bluetooth* yaitu pada 2,4 Ghz, namun bedanya *Bluetooth* menggunakan *Spread Spectrum Frequency Hopping* (SSFH), sedangkan WiFi menggunakan *Direct Sequence Spread Spectrum* (DSSS). *Direct Sequence Spread Spectrum* (DSSS) merupakan suatu metode untuk mengirimkan data dimana sistem pengirim dan penerima keduanya berada pada set frekuensi yang lebarnya adalah 22 MHz. Saluran yang lebar ini memungkinkan piranti untuk memancarkan lebih banyak informasi pada data rate yang lebih tinggi dibanding FHSS system yang ada sekarang. [16]

Intinya *spread* pada WiFi akan lebih stabil dan tentunya lebih cepat dibandingkan dengan *Bluetooth* . WiFi memiliki kelemahan yang sangat mengangu seperti masalah keamanan yang dapat di bajak ditengan jalan, dan rentan terhadap konflik dengan perangkat lain dalam waktu yang bersamaan. WiFi, dikenal dengan standar IEEE

802.11b, mulai luas dioperasikan dan beberapa operator di Amerika Serikat mengope-rasikannya secara hot spot di berbagai lokasi seperti Bandara kampus, hotel, *coffee shop* dll. [16]

Berikut ada bebrapa keunggulan yang dimiliki oleh teknologi WiFi.

a. Keunggulan Teknologi WiFi

Ada beberapa keunggulan dan kelemahan yang dimiliki oleh Jaringan WiFi antara lain sebagai berikut:

- WiFi dikembangkan tanpa kabel dan menggunakan gelombang radio dengan frekuensi 2,4 GHz. Selain itu WiFi dapat mengirim dan menerima kapasitas sampai 54Mbps.
- WiFi menggunakan jalur akses jaringan/*hotspot*, dapat berkomunikasi ke semua komputer dan laptop.
- Memungkinkan LAN untuk digunakan tanpa kabel, biasanya mengurangi biaya penyebaran jaringan dan ekspansi. Ruang di mana kabel tidak dapat dijalankan, seperti area outdoor dan bangunan bersejarah, dapat menggunakan LAN *Wireless*.

- WiFi jaringan dukungan roaming, di mana sebuah stasiun klien *mobile* seperti komputer laptop dapat berpindah dari satu jalur akses

Dari perbedaan tersebut diatas dengan kelebihan yang dimilik oleh teknologi WiFi, maka penulis mengambil topik bahasan mengenai teknologi WiFi.

2.2. *WIRELESS LOCAL AREA NETWORK* (WLAN)

Wireless Local Area Network (WLAN) atau jaringan nirkabel merupakan suatu jaringan area lokal tanpa menggunakan kabel yang mana media transmisinya menggunakan *radio frekuensi* (RF), untuk menyalurkan koneksi jaringan ke seluruh pengguna pada area disekitarnya [1].

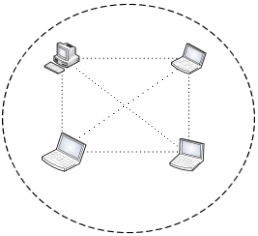
Jangkauan areanya misalnya berjarak dari ruangan kelas ke seluruh kampus atau dari kantor ke kantor yang lain dan berlainan gedung. Piranti yang umumnya digunakan untuk jaringan WLAN termasuk di dalamnya adalah *Personal Computer* (PC), Laptop, telepon seluler, dan lain sebagainya. Banyak kegunaan dari teknologi WLAN. Contohnya, pengguna *mobile* bisa menggunakan telepon seluler mereka untuk mengakses *electronic-mail* (*e-mail*) [1].

2.3. STRUKTUR JARINGAN *WIRELESS*

Dalam sebuah jaringan untuk menghubungkan unsur penyusun jaringan dikenal dengan istilah topologi atau struktur dasar jaringan *wireless network*, pada jaringan *wireless* topologi tersebut terdiri atas 3 tipe yaitu, *Independent Basic Service Set*, *Extended Service Set*, *Basic Service Set*.

2.3.1 *Independent Basic Service Set* (IBSS)

Independent Basic Service Set (IBSS) merupakan konfigurasi jaringan yang setara dengan *'peer-to peer' Ethernet* LAN untuk kantor – kantor kecil, misalnya digunakan di dalam ruangan konferensi atau pameran perdagangan. Implementasi IBSS ini umumnya hanya mencakup wilayah terbatas dan umumnya tidak dihubungkan ke jaringan apapun yang lebih besar. Konfigurasi independen ini juga disebut jaringan *'ad-hoc'* (khusus), pada konfigurasi independen semua stasiun harus tetap berada dalam lingkaran dengan radius sekitar 300 kaki (100 meter) [4]. Arsitektur jaringan IBSS dapat dilihat pada gambar 2.1.



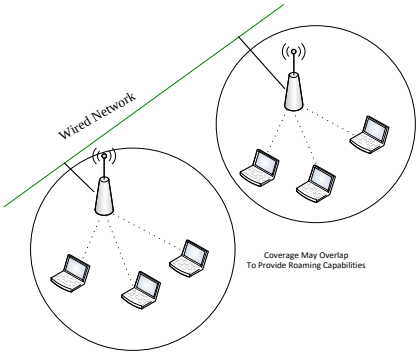
Gambar 2.1 *Independent Basic Service Set* (IBSS) [5]

Dalam menciptakan jaringan IBSS, perlu dilakukan instalasi *Network Interface Card* (NIC) nirkabel, selanjutnya memilih *channel* radio yang digunakan untuk kelompok jaringan tersebut. Di Amerika disediakan spektrum frekuensi yang cukup untuk tiga buah *channel* yang dapat ada bersama-sama dalam satu loaksi, namun dengan syarat, *channel* – *channel* tersebut harus saling terpisah pada rentang 25 MHz untuk mencegah terjadinya interferensi [4].

2.3.2 *Extended Service Set* (ESS)

Konfigurasi yang, yakni ESS, terdiri dari beberapa sel BSS yang dapat dihubungkan dengan *backbone* jaringan kabel ataupun jaringan nirkabel lainnya. Ketika menciptakan jaringan ESS, yang harus dilakukan yaitu instalasi AP dan *Network Interface Card* (NIC) nirkabel, mengatur

pengarahnya ke mode infrastruktur dan meyakinkan bahwa semua komponen diatur ke penggunaan nomor identifikasi (ESSID) yang sama. *Network Interface Card* (NIC) merupakan kartu penyesuai *Ethernet* atau token ring yang dimasukan ke slot bus ekspansi komputer *notebook* ataupun PC [4]. Jaringan LAN nirkabel dengan mode infrastruktur ini dapat dilihat pada gambar 2.2.



Gambar 2.2 *Extended Service Set* (ESS) [5]

Secara logika, ada beberapa cara untuk menjelajah, bergantung pada caranya AP diatur pada awalnya. Kasus awal yang paling sederhana adalah saat berbagai AP memiliki ESSID yang sama dan berada dalam subjaringan pada LAN yang sama. Yang menjadi agak rumit adalah ketika

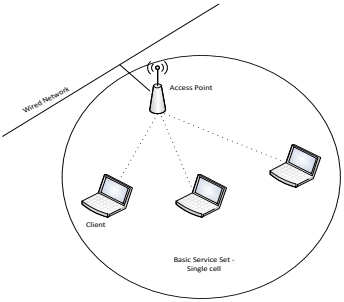
AP yang berbeda dengan ESSID yang sama, tetapi berada pada subjaringan yang berbeda. Beberapa AP dapat juga berasal dari jaringan logika yang berbeda pada sebuah jaringan LAN tunggal melalui penggunaan ESSID yang berbeda [4].

2.3.3 *Basic Service Set* (BSS)

Basic Service Set (BSS) terdiri dari hanya satu *access point* dan satu atau lebih klien *wireless*, seperti ditunjukkan pada gambar 2.3. BSS menggunakan model infrastruktur suatu model yang memerlukan penggunaan dari suatu *access point* dan di mana semua lalu lintas *wireless* menyilang. Transmisi yang diijinkan tidak secara langsung *client-to client* [5].

Masing-Masing klien *wireless* harus menggunakan *access point* untuk berkomunikasi dengan klien *wireless* lainnya atau *host* manapun pada jaringan itu. BSS meliput *singel cell*, atau RF area, di sekitar *access point* dengan data yang bermacam-macam nilai *zone* (lingkaran-lingkaran konsentris) tentang kecepatan data berbeda yang diukur dalam Mbps. Kecepatan data dalam lingkaran-lingkaran konsentris ini akan tergantung pada teknologi yang digunakan. Jika BSS terdiri

dari peralatan 802.11b, kemudian lingkaran-lingkaran konsentris akan membuat kecepatan data 11, 5.5, 2, dan 1 Mbps. Suatu BSS mempunyai satu *Service Set IDentifier* (SSID) yang berbeda [5].



Gambar 2.3 *Basic Service Set* (BSS) [5]

2.4. MODE JARINGAN *WIRELESS*

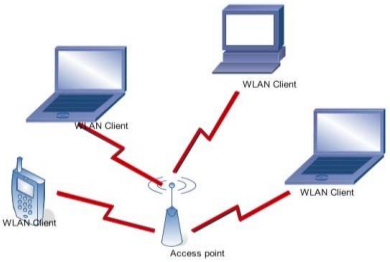
Mode jaringan *wireless* berbeda dengan jaringan kabel, pada jaringan *wireless* menggunakan *channel* frekuensi yang sama dan SSID yang menunjukkan identitas dari *wireless device.*

Pada jaringan *wireless* mempunyai dua mode yang dapat digunakan yaitu mode infrastruktur dan mode *Ad-Hoc*.

2.4.1 Mode Infrasturktur

Pada mode infrastruktur ini akan ada *access point* yang berfungsi untuk menjembatani komunikasi utama pada jaringan *wireless*. [6]

Access point mengirimkan data pada PC dengan jangkauan tertentu pada suatu area. Penambahan dan pengaturan letak *access point* dapat memperluas jangkauan dari jaringan WLAN. Pada mode infrastruktur inilah yang akan ditrapkan pada penelitian untuk uji coba interfernsi *channel* pada jaringan *wireless.* Contoh jaringan ini dapat dilihat pada gambar 2.4. [6]

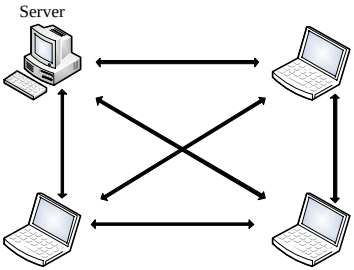


Gambar 2.4 Jaringan Infrastruktur[13]

2.4.2 Mode *Ad-Hoc*

Pada jaringan ini komputer dihubungkan secara langsung tanpa melalui perantara atau sering disebut dengan model koneksi *peer-to-peer* pada jaringan konvensional. Contoh dari penggunaan

jaringan ini adalah digedung perkantoran yang tidak terlalu besar. Kekurangan dari mode *ad-hoc* yaitu komputer tidak dapat berkomunikasi dengan komputer pada jaringan yang menggunakan kabel, selain itu juga sudah disebutkan sebelumnya bahwa jaringan ini terbatas pada jarak jangkauan. [6]



Gambar 2.5 Mode *Ad-Hoc*[6]

2.5. KOMPONEN PENDUKUNG *WIRELESS NETWORK*

Ada beberapa komponen yang digunakan pada jaringan *wireless*, yaitu sebagai berikut:

1. *Access Point* (AP)

   Pada jaringan *wireless*, diperlukan alat untuk mentransmisikan data yaitu *Access Point* dan terhubung dengan jaringan LAN melalui kabel. *Access Point* berfungi sebagai pengirim dan penerima data dan sebagai *buffer* data antara WLAN dengan *wired* LAN. Selain itu akses *point* juga dapat melayani

beberapa jumlah *user*, untuk jarak sampai beberapa meter tergantung pada metode akses yang digunakan. *Access Point* mengonversi sinyal frekuensi radio menjadi sinyal digital atau sebaliknya. Komponen tersebut bertindak layaknya sebuah hub/switch pada jaringan Ethernet. Dapat dilihat contoh akses *point* pada gambar 2.6.[3]

Gambar 2.6 *Access Point* [13]

2. *Extension Point*

   Extension point hanya berfungsi seperti *repeater* atau pengulang sinyal, untuk *client* di tempat yang lebih jauh. Syarat agar antara *access point* dapat berkomunikasi satu dengan yang lain, yaitu dengan *setting channel* di masing-masing AP harus sama. Selain itu *Service Set Identifier* (SSID) yang digunakan juga harus sama. [3]

3. Antena

   Antena merupakan alat untuk mentransformasikan sinyal radio yang merambat pada sebuah konduktor

menjadi gelombang elektromagnetik yang merambat diudara. Ada beberapa tipe antena yang dapat mendukung implementasi WLAN, yaitu: antena *omnidirectional* dan antena *directional*. [15]

4. *Wireless* LAN *Card*

   Wireless LAN *Card* dapat berupa *Personal Computer Memory Card International Association* (PCMCIA), *USB Card* atau *Ethernet Card*. PCMCIA digunakan untuk *notebook*, sedangkan yang lainnya digunakan pada komputer *desktop*. WLAN *Card* ini berfungsi sebagai *interface* antara sistem operasi jaringan *client* dengan *format interface* udara ke *access point.*[15]

2.6. TEKNOLOGI JARINGAN *WIRELESS FIDELITY* (WiFi)

Wireless Fidelity (WiFi) adalah sekumpulan standar yang digunakan untuk Jaringan lokal nirkabel (*Wireless Local Area Networks* – WLAN) yang didasari pada spesifikasi IEEE 802.11. Standar terbaru dari spesifikasi 802.11a atau 802.11b, dimana masing-masing spesifikasi terbaru tersebut menawarkan banyak peningkatan mulai dari luas cakupan yang lebih jauh hingga kecepatan transfernya. Dimana IEEE adalah sebuah organisasi profesional yang bergerak di seluruh dunia, dibidang peningkatan teknologi. [7]

Wireless Fidelity (WiFi) adalah koneksi tanpa kabel dengan mempergunakan teknologi radio sehingga pemakainya dapat mentransfer data dengan cepat serta dapat menghemat biaya yang dipergunakan. WiFi tidak hanya dapat digunakan untuk mengakses internet, WiFi juga dapat digunakan untuk membuat jaringan tanpa kabel di perusahaan. Karena itu banyak orang mengasosiasikan WiFi dengan Kebebasan karena teknologi WiFi memberikan kebebasan kepada pemakainya untuk mengakses internet atau mentransfer data dari ruang meeting, kamar hotel, kampus, dan tempat umum yang bertanda WiFi *Hotspot*. Pada awalnya WiFi ditujukan untuk pengunaan perangkat nirkabel dan jaringan area lokal (LAN), tetapi saat ini lebih banyak digunakan untuk mengakses internet. Hal ini memungkinan seseorang dengan komputer dengan kartu nirkabel (*wireless card*) atau *Personal Digital Assistant* (PDA) untuk terhubung dengan internet dengan menggunakan *access point* terdekat. [7]

Sebelum *wireless network* berkembang pesat seprti saat ini, *Institude of Electrical and Electronics Engineers* (IEEE) telah menyusun suatu aturan standar untuk mensertifikasi teknologi yang akan muncul. Sertifikasi IEEE memastikan bahwa suatu produk yang

menggunakan suatu teknologi akan kompatibel dengan produk lain yang menggunakan teknologi yang sama. Standar-standar tersebut adalah :

2.6.1 Standar WiFi 802.11a

Akhir tahun 1999, IEEE mengeluarkan standar 802.11a yang menetapkan operasi pita 5 GHz menggunakan *Orthogonal Frequency Multiplexing* (OFDM) dengan *transfer rate* mencapai 54 Mbps. 802.11a beroperasi sampai 54 Mbps pada pita 5 GHz menggunakan OFDM. [7]

Keuntungan utama 802.11a yaitu ditawarkannya daya tampung paling tinggi dengan 12 *channel no–overlapping* terpisah. Keuntungan lain dari 802.11a adalah pita 5 GHz tidak terlalu penuh sehingga memampukan *user* mencapai tingkatan performa yang lebih tinggi. Sebagian besar perangkat *interfering* seperti *microwave oven* dan *cordles phone* beroperasi pada pita 24 GHz.

Kelemahan 802.11a adalah rentangnya yang terbatas. Kekurangan tersebut membutuhkan sejumlah besar *access point* untuk sepenuhnya melindungi sebuah fasilitas yang sebanding dengan sistem 802.11b. Apabila dibandingkan operasi 802.11a dan 802.11b, maka *user* 802.11a memiliki

transfer rate yang lebih tinggi pada rentang yang sama dengan *user* 802.11b sampai *user* 802.11a kehilangan konektivitas.[7]

2.6.2 Standar WiFi 802.11b

Standarisasi 802.11b, yang merupakan ekstensi kecepatan tinggi, ke standar *direct sequence* awal pada pita 2.4 GHz dengan kecepatan data sampai dengan 11 Mbps. *Access point* 802.11b dan radio NIC telah tersedia sejak tahun 1999 sehingga, sebagian LAN *nirkabel* yang dipasang saat ini adalah 802.11b yang selalu mengalah. Keuntungan yang didapat dari 802.11b yaitu kelengkapan panjang rentangnya. 802.11b memungkinkan pengguna mampu mencapai jarak 300 kaki pada sebagian besar fasilitas *indoor*. Rentang yang tinggi mengizinkan penyebaran LAN *nirkabel* dengan jumlah *access point* yang sedikit agar dapat melindungi sebuah fasilitas yang sebanding dengan 802.11a [7]

Kelemahan dari 802.11b yaitu adanya kemungkinan interferensi RF dari perangkat radio lain. Misalnya, *cordless phone* 2.4 GHz yang mudah berinteferensi dengan LAN nirkabel 802.11b sehingga dapat menurunkan performa

terhadap *user*. *Microwave oven* dan perangkat-perangkat lain yang beroperasi pada pita 2.4 GHz juga dapat menyebabkan interferensi [7]

2.6.3 Standar WiFi 802.11g

IEEE mengesahkan standar 802.11g yang kompatibel dengan 802.11b pada tahun 2003 dengan meningkatkan performanya mencapai 54 Mbps pada pita 2.4 GHz dengan menggunakan menggunakan modulasi sinyal OFDM, sehingga lebih resistan terhadap interferensi dari gelombang lainnya.

Orthogonal Frequency Division Multiplexing adalah teknologi yang baru saja mulai mencapai LAN *nirkabel* (WLAN) dalam bentuk perangkat IEEE 802.11g yang beroperasi di 5 GHz band. OFDM adalah sebuah "*multi-carrier*" skema modulasi. Data dibagi di antara beberapa berdekatan "*Subcarriers*". [7]

Kelebihan 802.11g memiliki cepat kecepatan maksimum, jangkauan sinyal yang baik dan tidak mudah terhambat. Selain itu kelebihan dari 802.11g lainnya yaitu standar tersebut merupakan kompatibel terbalik dari 802.11b. Perusahan dengan keberadaan jaringan 802.11b

biasanya dapat meng-*upgrade access point*-nya menjadi 802.11g melalui peningkatan *firmware* sederhana. [7]

Kelemahan 802.11g, seperti kemungkinan interferensi RF dan keterbatasan tiga *Channel non-overlapping*, masih berlaku pada 802.11g dikarenakan pengerjaan di pita 2.4 GHz. Sebagai hasilnya, jaringan 802.11g memiliki pembatas kapasitas sebanding dengan 802.11a [7].

2.6.4 Standar WiFi 802.11n

IEEE 802.11n-2009 merupakan sebuah perubahan standar jaringan *nirkabel* 802.11-2.007 IEEE untuk meningkatkan *throughput* lebih dari standar sebelumnya, seperti 802.11b dan 802.11g, dengan peningkatan *data rate* maksimum dalam lapisan fisik OSI dari 54 Mbit/s ke maksimum 600 Mbit/s dengan menggunakan empat ruang aliran di lebar saluran 40 MHz [7].

IEEE 802.11n didasarkan pada standar 802.11 sebelumnya dengan menambahkan *Multiple-Input Multiple-Output* (MIMO) dan 40 MHz ke lapisan saluran fisik. MIMO merupakan teknologi yang menggunakan beberapa antena untuk menyelesaikan informasi lebih lanjut secara

koheren dari pada menggunakan satu antena. Dua manfaat penting MIMO adalah menyediakan keragaman antena dan spasial *multiplexing* untuk 802.11n [7].

Tabel 2.1 Standarisasi *wireless* [7]

802.11 *Network Standards*						
802.11 Protocol	***Frequency* (GHz)**	***Data Rate***	***Approximate Indoor Range***		***Approximate Outdoor Range***	
		Maximum	***Meters***	***Feet***	***Meters***	***Feet***
a	5	54 Mbps	35	115	120	390
b	2,4	11 Mbps	38	125	140	460
g	2,4	54 Mbps	38	125	140	460
n	2,4/5	300 Mbps	70	230	250	820

2.7. *CHANNEL* FREKUENSI WiFi 2,4 GHz

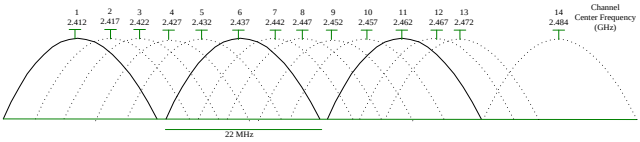
Organisasi internasional *International Telecomunications Union* (ITU) membagi frekuensi 2, 4 GHz menjadi 14 *channel* namun setiap negara mempunyai kebijakan tertentu terhadap *channel* ini. Amerika hanya mengijinkan penggunaan *channel* 1 – 11, Eropa hanya menggunakan 1 – 13 sedangkan di Jepang menggunakan semua *channel* yang tersedia yaitu 1 – 14, untuk Indonesia belum ada kebijakan tetapi AP di Indonesia jumlah *channel* yang dimiliki kebanyakan yaitu 11-13. [8]

Pembagian frekuensi *channel* yang dapat digunakan dapat di lihat pada tabel frekuensi 2.2 berikut ini:

Tabel 2.2 *Channel* frekuensi [8]

Channel	Frekuensi (Mhz)	*Channel*	Frekuensi (Mhz)
1	2412	8	2447
2	2417	9	2452
3	2422	10	2457
4	2427	11	2462
5	2432	12	2467
6	2437	13	2472
7	2442		

Pada komunikasi penggunaan *wireless*, apabila penggunaan *channel* 1 dan *channel* 2 secara bersamaan akan menimbulkan interferensi yang akan menimbulkan rusaknya data – data yang dikirim. Agar tidak terjadi interferensi, maka diperlukan strategi penggunaan *channel* yang baik.



Gambar 2.7 Alokasi Frekuensi 14 *Channel* [8]

2.8. INTERFERENSI

Interferensi adalah gangguan yang terjadi disebabkan adanya sinyal lain yang frekuensinya sama dan daya sinyal pengganggu tersebut cukup besar. Ukuran yang digunakan untuk menilai kualitas sinyal terhadap

gangguan interferensi dinyatakan dengan C/I (dB) = *Carrier to Noise Ratio.* [17] Interferensi juga dapat dikatakan, sinyal-sinyal yang berkompetisi dalam frekuensi yang saling tumpang tindih dapat mengubah atau menghapuskan sinyal. Interferensi menjadi perhatian khusus untuk media kabel, namun bagi media tanpa kabel interferensi juga menjadi masalah yang cukup besar. [2]

Dalam dunia telekomunikasi dan IT ada hal yang tidak mungkin dihindari yaitu gangguan/ Interferensi, namun dengan batasan toleransi tertentu masih dapat diterima.

Ada beberapa jenis kategori Interferensi:

1. *Interferensi Cross polarisasi* adalah gangguan disebabkan dari pengguna frekuensi yang sama dan power yang dipancarkan/*Transmitter*. [2]
2. Interferensi *Adjacent-Channel* adalah Interferensi yang diakibatkan oleh sinyal-sinyal pada frekuensi yang berdekatan. Interferensi jenis ini terjadi karena filter penerima yang tidak sempurna yanng mengakibatkan frekuensi lain masuk kedalamnya. Interferensi ini akan menjadi masalah yang serius bila kanal yang bersebelahanan dari pengguna tersebut mentransmisikan informasi pada frekuensi yang sangat dekat dengan frekwensi pengguna. Fenomena ini

disebut sebagai efek *near-far* dimana daya dari transmitter yang terdekat mengganggu kerja dari *receiver* ketika menerima sinyal dari *transmitter* yang jauh. Efek dari *adjacent channel interference* dapat diperkecil dengan proses filterisasi yang baik dan pembagian kanal (*channel assignment*) yang baik. *Channel assignment* dilakukan dengan memberikan jarak frekwensi pemisah yang cukup besar antara satu kanal dengan kanal yang lainnya. [17]

3. *Interferensi Co-Channel (antar channel)* adalah gangguan disebabkan oleh frekuensi *channel* atau tidak ada jarak antar kedua frekuensi *(Guard band).*[2] . Interferensi *Co-channel* tidak dapat diatasi dengan cara meningkatkan SNR. Hal ini karena penambahan daya pancar pengirim justru akan menaikkan interferensi dengan sel *co-channel* tetanggga. Untuk mengurangi interferensi *co-channel* maka sel-sel ko-kanal harus dipisahkan sejauh jarak minimal tertentu yang akan mengurangi pengaruh perambatan. [17] Untuk mengurangi interferensi *co-channel*, maka sel-sel yang sama tersebut harus dipisahkan tiap-tiap selnya sehingga jaraknya minimum agar memberikan isolasi antar sel yang cukup pada propagasi gelombangnya. Untuk ukuran sel yang sama, terpisah

dari daya pancar, *co-channel* interferens menjadi fungsi radius sel (R), dan jarak ke titik pusat terhadap *co-channel* sel yang terdekat (D). Dengan menaikkan rasio D/R, jarak antar *co-channel* sel maka daerah yang dilayani akan naik. Interferensi antar sel tersebut diminimalisasi dengan menaikkan isolasi dari RF energi dari *co-channelnya*. Parameter Q, disebut *co-channel reuse ratio*, sangat terkait dengan ukuran cluster.

$$\mathbf{Q = D / R}$$

Semakin kecil nilai parameter Q maka kapasitasnya akan membesar. Sedangkan menaikkan nilai Q akan memperbaiki kualitas transmisi. Optimasi antara kedua hal tersebut sangat diperlukan dalam desain selular di lapangan atau secara riil. *Co-channel Interference.* Penggunaan frekuensi yang sama atau *frequency reuse* menunjukkan bahwa pada area yang terdapat beberapa sel menggunakan frekuensi yang sama. Sel ini disebut *co-channel cells*, sedangkan interferensi antar sinyal dari sel ini disebut *co-channel interference*. Tidak seperti halnya mengatasi *noise thermal* yaitu dengan menaikkan SNR, *co-channel* interferns tidak dapat diatasi dengan cara menaikkan daya *transmit* dari *transmitter*. Hal ini karena dengan menaikkan daya

pancar transmitter akan menginterferensi sel-sel tetangganya. [17]

Pada penelitian kali ini interferensi yang berkaitan adalah *interferensi co-channel* yaitu penggunaan *channel* yang sama dan tidak mempunyai jarak.

2.9. MODEL PROTOKOL JARINGAN

Dalam komunikasi antara dua *network device* atau lebih, diperlukan sebuah standar yang saling dimengerti antara satu dengan yang lain, dalam sebuah jaringan istilah ini disebut dengan protokol. TCP/IP terdiri dari dua protokol utama yaitu *Transmission Control protocol* dan *Internet Protokol*.[13]

Protokol ini menggunakan skema pengalamatan alamat IP yang mengizinkan hingga beberapa ratus juta komputer untuk dapat saling berhubungan satu sama lainnya. Terdapat beberapa elemen umum TCP/IP diantaranya :

1. IP *address* merupakan sebuah struing unik dalam angka desimal yang dibagi dalam empat segmen. Tiap-tiap segmen bisa ditulis angka yang terdiri dari 0 hingga 255 yang mepresentasikan 8 bit alamat tiap segmen atau 32 bit untuk keseluruhan.[2]
2. *Netmask* atau *subnet mask* adalah tanda yang fungsinya membagi alamat IP yang menunjukan

subnetwork. Misal IP kelas C memiliki *netmask* standar adalah 255.255.255.0. [2]

3. *Network address* mepresentasikan porsi jaringan dari alamt IP, misalnya host 12.128.1.2 di jaringan kelas A memiliki *network* address 12.0.0.0. *Host* jaringan yang menggunakan IP pribadi seperti 192.168.1.100 akan menggunakan *network address* 192.168.1.0. *Network address* tersebut menjelaskan bahwa jaringan termasuk dibagian kelas C 192.168.1.0. [2]
4. *Broadcast address* merupakan alamat IP yang memungkinkan data jaringan dikirimkan secara simultan ke semua *host* disebuah *subnetwork*. *Broadcast address* standar untuk jaringan IP adalah 255. 255. 255. 255. Namun *broadcast* ini tidak bisa digunakan karena terblok oleh *router*. Alamat *broadcast* biasanya diset untuk *subnetwork* tertentu saja misal IP 192.168.1.1 akan memiliki alamat *broadcast* 192.168.1.255. [2]
5. *Gateway address* adalah alamat IP yang harus dilewati oleh semua komputer di jaringan yang ingin berkomunikasi dengan *host* di jaringan lain.
6. *Name server address* menunjukan IP *address* dari *domain name service* yang bertujuan menerjemahkan nama *hostname* ke alamat IP.[5]

2.10. PARAMETER PERFORMANSI JARINGAN

Performansi jaringan sangat membantu menjaga dan meningkatkan kapabilitas jaringan, apakah itu jaringan-jaringan kompleks, jaringan perusahaan kecil, *Internet Service Provider* (ISP), atau jaringan-jaringan *enterprise*. Performansi jaringan memberikan jaminan dan layanan yang lebih baik terhadap trafik-trafik jaringan dalam beragam teknologi, Sasaran utama performansi jaringan tidak lain memberikan layanan jaringan yang lebih baik dan dapat di prediksi. Parameter performansi diantaranya, *signal level, throughput,* dan *packet loss* serta *latency*.

2.10.1 *Throughput*

Throughput merupakan jumlah bit yang berhasil dikirim pada suatu jaringan, dilihat dari berapa banyak paket data yang berhasil dikirimkan dalam kurun waktu satu detik. *Throughput* diukur dalam waktu tertentu dan dalam kondisi jaringan tertentu yang digunakan untuk mentransfer file dari ukuran tertentu. Rumus yang digunakan untuk mencari *throughput* adalah :

$$Throughput = \sum \frac{Data\ yang\ dikirim\ (bit)}{Waktu\ pengiriman\ (s)}\ (Bps)$$

Biasanya *throughput* dikaitkan dengan *bandwidth* karena memiki rumus yang sama.

Namun, *bandwidth* lebih menyerupai sebagai kapasitas maksimal dari transfer data. Sedangkan, *throughput* menyatakan kapasitas aktual yang dapat diperoleh berdasarkan kecepatan yang sebenarnya. *Throughput* dipengaruhi oleh faktor perangkat jaringan, topologi jaringan, jumlah pengguna jaringan, induksi listrik dan cuaca.

Parameter *throughput* pada jaringan *wireless* LAN mempunyai batasan maksimal sesuai dengan teknologi WLAN yang digunakan dan berdasarkan jarak jangkauan keberadaan dari *user*. Pada penelitian skripsi ini menggunakan teknologi WLAN 802.11, nilai maksimal dari parameter *throughput* pada teknologi WLAN 802.11b dapat dilihat pada tabel 2.3. [10]

Tabel 2.3 *Throughput* maksimal IEEE 802.11 [10]

Jarak (*Feet*)	**Jarak (m)**	**802.11b (Mbps)**	**802.11g (Mbps)**
10	3,048	5,8	24,7
50	15,24	5,8	24,7
100	30,48	5,8	19,8
150	45,72	5,8	12,4
200	60,96	3,7	4,9
250	76,2	1,6	1,6
300	91,44	0,9	0,9

2.10.2 *Latency*

Latency merupakan waktu yang dibutuhkan data untuk menempuh jarak dari asal ke tujuan.[6] Nilai *latency* dapat disebabkan oleh kualitas komponen jaringan seperti kabel, *router*, dan *switch*. Serialisasi *delay*, *routing* dan *switching latency*, dan *queuing* dan *buffer management*.

$$Latency = \frac{Packet\ length\ (bit)}{link\ bandwith}\ (s)$$

Perhitungan untuk mencari nilai *latency* menggunakan rumus persamaan tersebut diatas. Perhitungan *latency* didapatkan dengan membagi panjang paket atau jumlah bit paket yang dikirimkan dibagi dengan *bandwidth* lintasan yang tersedia dalam *bit per second*. Nilai *latency* mempunyai satuan *second*. [11]. Berdasarkan ITU-T standarisasi nilai *latency* seperti pada tabel 2.4.

Tabel 2.4 Standarisasi *Latency* versi ITU-T.[11]

Kategori	***Latency* (ms)**
Baik	< 150
Cukup	150 – 400
Buruk	> 400

2.10.3 *Packet loss*

Packet loss merupakan sejumlah paket data yang hilang selama proses trannsmisi paket data.

[6] *Packet loss* dapat disebabkan oleh berbagai kemungkinan diantaranya *congestion* atau disebabkan karena berlebihan antrian dalam jaringan, *node* atau kerja melebihi kapasitas *buffer*, memori terbatas pada *node*, *policing* atau kontrol jaringan. Untuk memastikan bahwa jumlah *traffic* yang mengalir ke jumlah *bandwidth*, jika jumlah *traffic* yang mengalir dalam jaringan melebihi kapasitas *bandwidth*, *policing control* akan menghapus kelebihan *traffic* yang ada. Perhitungan untuk mencari nilai *packet loss* menggunakan persamaan sebagai berikut. [12]

$$Packet\ loss = \frac{paket\ dikirim - paket\ diterima}{paket\ dikirim}\ x\ 100\%$$

Nilai *packet loss* diklasifikasikan berdasarkan versi *Europe Telecomunication Standard Institute* (ETSI) dapat dilihat pada table 2.5

Tabel 2.5 Standarisasi *packet loss* [12]

Kategori	***Packet Loss* (%)**
Sangat baik	0 ≤ 3%
Baik	3 ≤ 15 %
Cukup	15 ≤ 25 %
Buruk	≥ 25 %

2.10.4 *Signal level*

Pengujian *signal* level dilakukan untuk mengetahui seberapa kuat sinyal yang diterima oleh komputer *client* dengan menggunakan *software* LinSSID. Selain itu *software* LinSSID juga dapat menampilkan hasi *quality signal* yang diterima. Dan dapat menampilkan penempatan *channel* yang digunakan.

2.11. PERANGKAT LUNAK PENDUKUNG

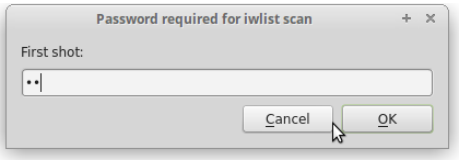
Dalam penelitian skripsi kali ini memerlukan beberapa *software* pendukung untuk mengetahui beberapa parameter performansi yang di perlukan salah satu perangakt lunak yang digunakan adalah LinSSID.

1. LinSSID

   LinSSID adalah perangkat lunak yang berfungsi untuk melihat jaringan WiFi dan dapat menganalisa informasi dari jaringan WiFi secara *real time*. Selain itu berfungsi untuk mengetahui frequency, *channel*, mac *address, mode, signal*, dan *chipper* atau jenis otentikasi dari semua SSID yang ada di sekitar lingkungan pengguna WiFi. *Software* ini bisa di gunakan untuk optimalisasi jaringan WiFi karena biasanya semakin banyak signal WiFi maka semakin

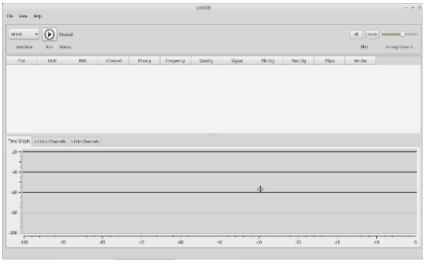
besar potensi jaringan WiFi mengalami interferensi, sehingga dengan menggunakan *software wireless scanner* ini akan dapat mengetahui *frequency* dan *channel* yang digunakan oleh LinSSID WiFi lain agar tidak mengalami interferensi dengan SSID WiFi yang terhubung pada komputer.

Cara kerja LinSSID ini cukup mudah, tidak perlu *connect* ke WiFi terlebih dahulu yaitu hanya perlu membukanya kemudian mulai *scanning* SSID WiFi yang ada di sekitar lingkungan dan secara otomatis *software* ini akan bekerja dan menampilkan semua informasi dari SSID WiFi yang terhubung dan juga LinSSID WiFi yang lain. Pertama kali saat membuka LinSSID akan muncul tampilan berikut ini yaitu *password required for iwlist scan,* kemudian masukkan *password root* terlebih dahulu.



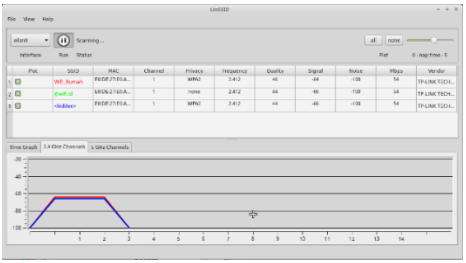
Gambar 2.8 Tampilan LinSSID

Setelah memasukkan password root maka akan muncul tampilan LinSSID yang ditunjukkan gambar 2.10.



Gambar 2.9 Tampilan awal LinSSID

Dalam LinSSID terdapat beberapa *tools*, yaitu *file*, *view*, dan *help*. Pada tools *file* berisi *preference* dan menu *exit*. Sedangkan untuk *tools view* berfungsi untuk menampilkan apa-apa saja yang ingin diketahui dari WiFi yang terhubung pada laptop, yaitu SSID, MAC, *Channel*, *Mode*, *Security*, *Privacy*, *cipher*, *frequency*, *quality*, *signal*, *noise*, *vendor*, *min signal*, *max signal*, *Mbps*, *firts seen*, *last seen*, serta *protocol*.



Gambar 2.10 Tampilan LinSSID setelah di aktifkan