

## **BAB II**

### **DASAR TEORI**

#### **2.1 TEKNOLOGI JARINGAN Wi-Fi**

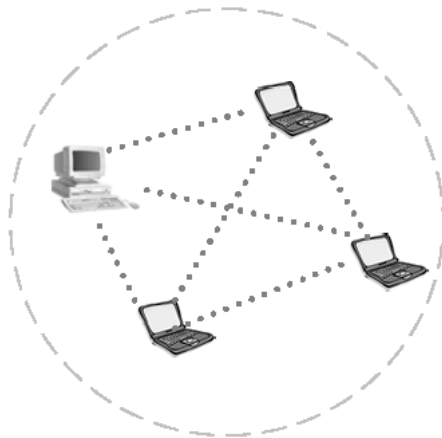
*Wireless Fidelity* (Wi-Fi) merupakan sekumpulan standar yang digunakan untuk Jaringan Lokal Nirkabel (*Wireless Local Area Network*, WLAN) berdasar pada spesifikasi *The Institute of Electrical and Electronics Engineer* (IEEE) 802.11. Fungsinya menghubungkan jaringan dalam satu area lokal secara nirkabel. Awalnya Wi-Fi digunakan untuk penggunaan perangkat nirkabel dan jaringan area lokal (LAN), namun saat ini lebih banyak digunakan untuk mengakses internet. Hal ini memungkinkan seseorang dengan komputer, dengan kartu nirkabel (*wireless card*) atau *personal digital assistant* (PDA) untuk terhubung dengan internet dengan menggunakan titik akses (*hotspot*) terdekat [3].

#### **2.1. ARSITEKTUR DASAR JARINGAN WIRELESS LAN**

Konfigurasi jaringan *wireless* LAN membentuk suatu arsitektur jaringan *wireless* LAN. Pada jaringan *wireless* LAN terdapat tiga konfigurasi jaringan. Tipe dari konfigurasi jaringan *wireless* LAN yaitu *Independent Basic Service Set*, *Extended Service Set*, *Basic Service Set*.

### 2.2.1 *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.

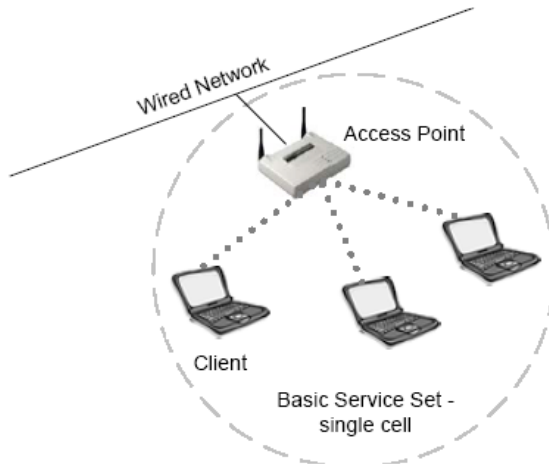


Gambar 2.1 *Independent Basic Service Set (IBSS)* [5]

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

### 2.2.2 *Basic Service Set* (BSS)

*Basic Service Set* (BSS) terdiri dari hanya satu *access point* dan satu atau lebih klien *wireless*, seperti ditunjukkan pada gambar 2.2. 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]



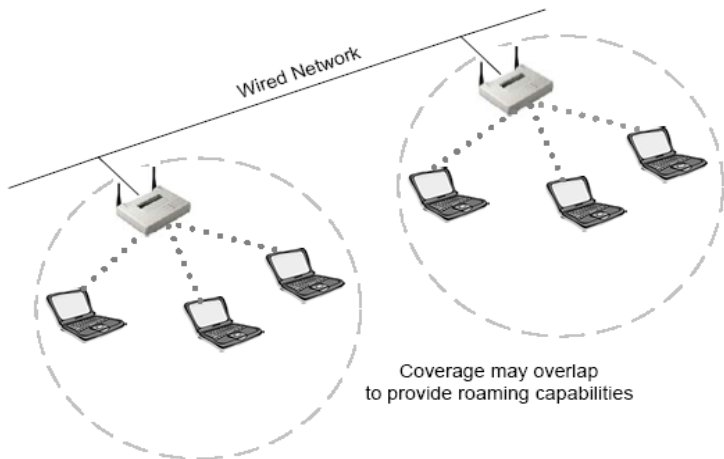
Gambar 2.2 *Basic Service Set (BSS)* [5]

Masing-Masing klien *wireless* harus menggunakan *access point* untuk berkomunikasi dengan klien *wireless* lainnya atau *host* manapun pada jaringan itu. BSS meliputi *single 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]

### **2.2.3 *Extended Service Set (ESS)***

Konfigurasi yang ketiga, 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 pengarahannya 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 dimasukkan ke slot bus ekspansi komputer *notebook* ataupun PC [4]. Jaringan LAN nirkabel dengan mode infrastruktur ini dapat dilihat pada gambar 2.3.



Gambar 2.3 *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 MODE JARINGAN WIRELESS LAN

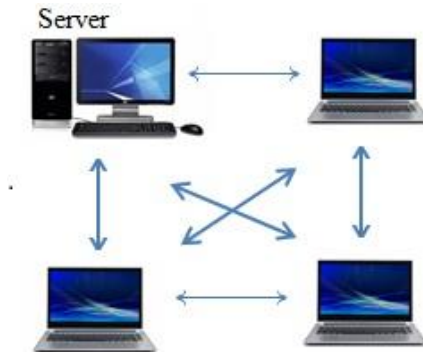
*Wireless Local Area Network* hampir sama dengan jaringan LAN, akan tetapi setiap *node* pada WLAN menggunakan *wireless device* untuk berhubungan dengan jaringan. *Node* pada WLAN menggunakan *channel* frekuensi yang sama dan SSID yang menunjukkan identitas dari *wireless device*. [15]

Berbeda dengan jaringan kabel, jaringan *wireless* mempunyai dua mode yang dapat digunakan yaitu infrastruktur dan *Ad-Hoc*. Konfigurasi mode infrastruktur yaitu komunikasi antar masing-masing PC melalui sebuah *access point* pada WLAN atau LAN. Komunikasi mode *Ad-Hoc* yaitu komunikasi secara langsung antara masing-masing komputer dengan menggunakan piranti *wireless*. Penggunaan kedua mode ini tergantung dari kebutuhan untuk berbagi data atau kebutuhan yang lain dengan jaringan berkabel. [15]

### 2.3.1 Mode *Ad-Hoc*

*Ad-Hoc* adalah mode jaringan WLAN yang sangat sederhana, karena pada mode *ad-hoc* tidak memerlukan *access point* untuk *host* dapat saling berinteraksi. Setiap *host* cukup memiliki *transmitter* dan *reciever wireless* untuk berkomunikasi secara langsung satu sama lain seperti tampak pada gambar 2.4. Kekurangan dari mode *ad-hoc* yaitu komputer tidak dapat berkomunikasi dengan

komputer pada jaringan yang menggunakan kabel. Selain itu, daerah jangkauan pada mode ini terbatas pada jarak antara kedua komputer tersebut.[15]

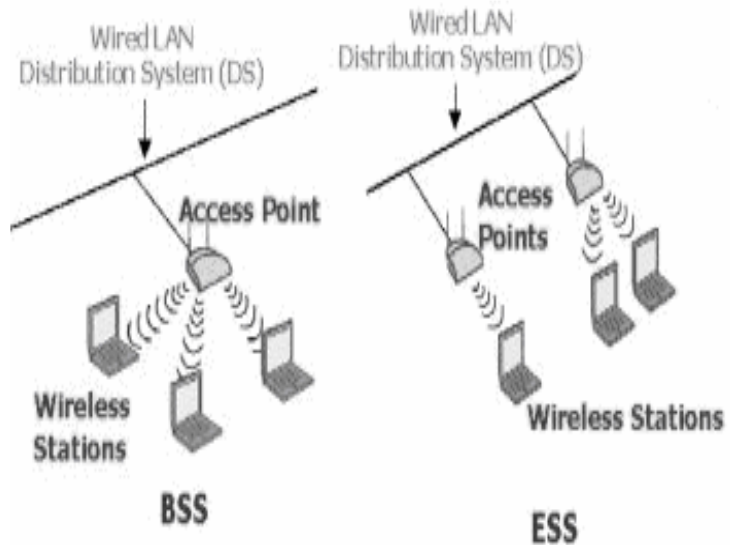


Gambar 2.4 Mode Jaringan *Ad-Hoc*

### 2.3.2 Mode Infrastruktur

Apabila komputer pada jaringan *wireless* akan mengakses jaringan kabel atau berbagi printer contohnya, maka jaringan *wireless* tersebut harus menggunakan mode infrastruktur (gambar 2.5).[15] Pada mode *infrastruktur access point* berfungsi melayani komunikasi utama pada jaringan *wireless*. *Access point* mengirimkan data pada PC dengan jangkauan tertentu pada suatu area. Penambahan dan pengaturan letak *access point* dapat memperluas jangkauan dari jaringan WLAN.[15]





Gambar 2.5 Mode Jaringan Infrastruktur[15]

## 2.4 PERKEMBANGAN STANDAR JARINGAN WI-FI 802.11

*Wireless Fidelity* (Wi-Fi) merupakan sekumpulan standar yang digunakan untuk Jaringan Lokal Nirkabel, *Wireless Local Area Networks* (WLAN) didasari pada spesifikasi *Institute of Electrical and Electronics Engineer* (IEEE) 802.11. Standar terbaru dari spesifikasi 802.11a atau 802.11b, dimana setiap spesifikasi terbaru tersebut menawarkan banyak peningkatan dari segi luas cakupan yang lebih jauh sampai dengan kecepatan transfernya.[7] IEEE adalah organisasi profesional yang bergerak

di seluruh dunia dalam bidang peningkatan teknologi untuk meningkatkan harkat kemanusiaan. Sebelumnya IEEE bergerak dalam bidang elektroteknika. Namun meluasnya dan saling berkaitnya bidang-bidang ilmu yang menjadi minat pengembangan IEEE membuat organisasi ini memposisikan diri untuk bergerak dalam teknologi-teknologi lain yang terkait, dan saat ini disebut IEEE saja.[7] *Wireless Fidelity* (Wi-Fi) adalah koneksi tanpa kabel dengan mempergunakan teknologi radio sehingga pemakainya dapat mentransfer data dengan cepat serta dapat menghemat biaya yang dipergunakan. 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 tempat umum yang bertanda *Wi-Fi Hotspot*. Pada awalnya Wi-Fi ditujukan untuk penggunaan perangkat nirkabel dan jaringan area lokal (LAN), tetapi saat ini lebih banyak digunakan untuk mengakses internet. Hal ini memungkinkan seseorang dengan komputer dengan kartu nirkabel (*wireless card*) atau *Personal Digital Assistant* (PDA) untuk terhubung dengan internet dengan menggunakan *access point* terdekat. [7]

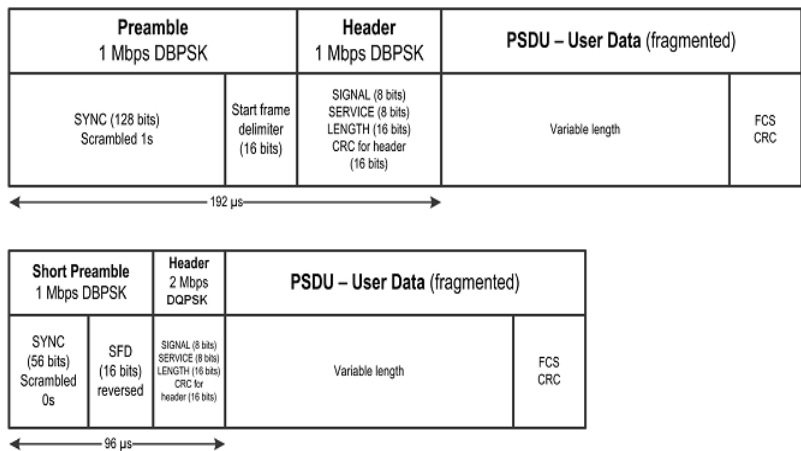
### 2.4.1 Standar Wi-Fi 802.11a

Di akhir tahun 1999, IEEE mengeluarkan 802.11a yang menetapkan operasi pita 5 GHz menggunakan *Orthogonal Frequency Multiplexing* (OFDM) dengan kecepatan data maksimal 54 Mbps, dengan rentang sampai 100 kaki atau 30,48 meter, tergantung pada kecepatan data sesungguhnya [7]. Keuntungan utama 802.11a adalah ditawarkannya daya tampung paling tinggi dengan 12 *Channel no – overlapping* terpisah. Penggunaan tersebut merupakan pilihan yang bagus untuk mendukung konsentrasi tinggi *user* dan aplikasi performansi yang lebih tinggi seperti *video streaming*. Selain itu, untuk meningkatkan sistem 802.11b. Masalah utama pada 802.11a adalah *coverage* area yang terbatas. Hal tersebut membutuhkan sejumlah *access point* yang banyak. Jika membandingkan 802.11a dan 802.11b, maka *user* 802.11a memiliki kecepatan data yang lebih tinggi. Masalahnya adalah 802.11a dan 802.11b/g tidak kompatibel karena perbedaan frekuensi kerjanya. Sebagai contoh, *user* yang dilengkapi dengan *radio card* 802.11b tidak dapat berasosiasi dengan *access point* 802.11a, dengan demikian juga sebaliknya. Para vendor mengatasi masalah tersebut dengan mengenalkan *radio card milimode* yang mengimplementasikan baik 802.11a maupun 802.11b [7].

### 2.4.2 Standar Wi-Fi 802.11b

Bersama dengan 802.11a, IEEE mengesahkan 802.11b, yang merupakan ekstensi kecepatan tinggi, dengan menggunakan *direct sequence* dengan frekuensi 2.4 GHz dengan kecepatan data sampai dengan 11 Mbps. Kelebihan dari 802.11b adalah pada sisi *coverage area*, 802.11b memungkinkan *user* mampu mencapai jarak hingga 300ft pada indoor. Kelemahan dari 802.11b adalah *user* dibatasi sampai tiga *Channel non overlapping* pada pita 2.4 GHz. Standar 802.11 menetapkan 14 *Channel* (hanya *Channel* 1 sampai 11 yang tersedia di Amerika Serikat) untuk mengonfigurasi *access point*. Walaupun demikian, masing-masing *channel* menempati kira-kira sepertiga dari keseluruhan pita 2.4 GHz saat mengirim sebuah sinyal. Sebagian besar perusahaan hanya menggunakan channel 1, 6, dan 11 untuk memastikan *access point* tidak berinterferensi satu sama lain. Hal tersebut membatasi kapasitas 802.11b sehingga menjadikannya paling sesuai untuk mendukung aplikasi performa medium, seperti *e-mail* [7]. Kelemahan dari 802.11b adalah adanya kemungkinan interferensi dari perangkat radio lain. Sebagai contoh, *cordless phone* 2.4GHz mudah berinterferensi dengan WLAN 802.11b sehingga dapat menurunkan performa terhadap *user* dan

perangkat-perangkat lain yang beroperasi pada pita 2.4 GHz juga dapat menyebabkan interferensi. 802.11b menggunakan teknik *Direct Sequence Spread Spectrum* (DSSS) untuk mengirimkan sinyal informasi. Hal ini membuat 802.11b lebih kuat terhadap interferensi dibandingkan dengan *frequency modulation* [7].



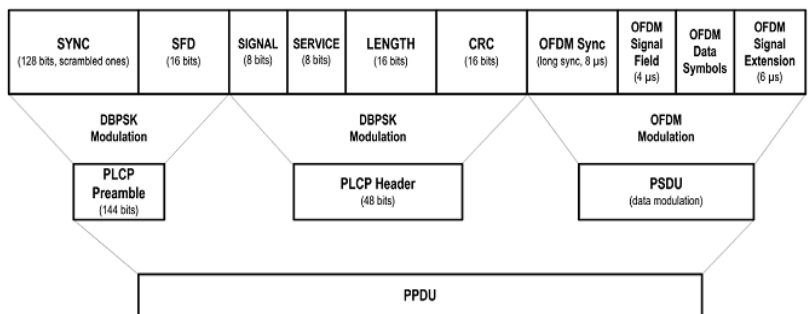
Gambar 2.6 Struktur frame transmisi DSSS 802.11b (long and short preambles)[4]

Gambar 2.6 menunjukkan struktur frame transmisi pada WLAN 802.11b. Pada awalnya preamble dan header yang ditransmisikan dengan data rate 1Mbps, menggunakan modulasi DBPSK, sedangkan 802.11b dengan data rate 2Mbps menggunakan modulasi DQPSK. Saat standar resmi dirilis dengan menggunakan *Complementary Code Keying*

(CCK), hal ini digunakan untuk data rate 5.5 Mbps dan 11Mbps. Standar ini juga menambahkan short preamble sebesar 56-bit (long preamble 128-bit). [4]

### 2.4.3 Standar Wi-Fi 802.11g

IEEE mengesahkan standar 802.11g yang kompatibel dengan 802.11b pada tahun 2003 dengan meningkatkan performanya dengan kecepatan *data rate* maksimal 54 Mbps pada frekuensi 2.4 GHz dengan menggunakan teknik *Orthogonal Frequency Division Multiplexing* (OFDM). Standar ini menggunakan OFDM, sehingga lebih tahan terhadap interferensi dari perangkat radio lain.

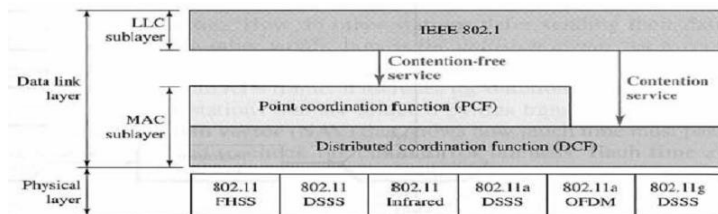


Gambar 2.7 Frame struktur transmisi DSSS-OFDM 802.11g (long preamble PPDU format)[4]

### 2.4.4 Standar Wi-Fi 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]

## 2.5 DATA LINK LAYER



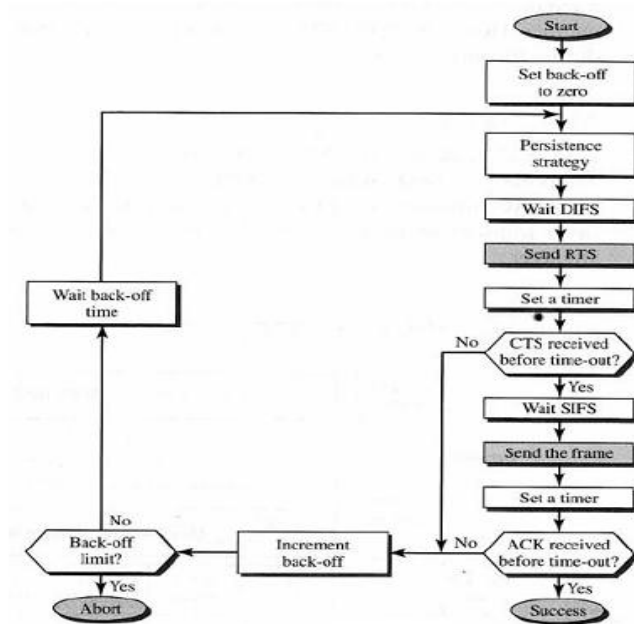
Gambar 2.8 *Frame MAC WLAN*

### 2.5.1 *Distributed Coordinated Function (DCF)*

DCF menggunakan metode akses *Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA)*, dalam hal ini WLAN tidak dapat mengimplimentasikan *collision detection (CSMA/CD)*, seperti pada jaringan *wireline*. Hal ini disebabkan karena:

1. *Collision detection* sebuah *station* harus mampu mengirim dan menerima isyarat tabrakan (*collision*) data pada saat yang sama. Hal ini pasti menyebabkan *hardware station* yang tak murah serta memerlukan *bandwidth* lebih banyak lagi.
2. Tabrakan mungkin tidak terdeteksi karena masalah adanya *station* yang tersembunyi (*hidden node*).
3. Jarak antara *station-station* saling berdekatan.



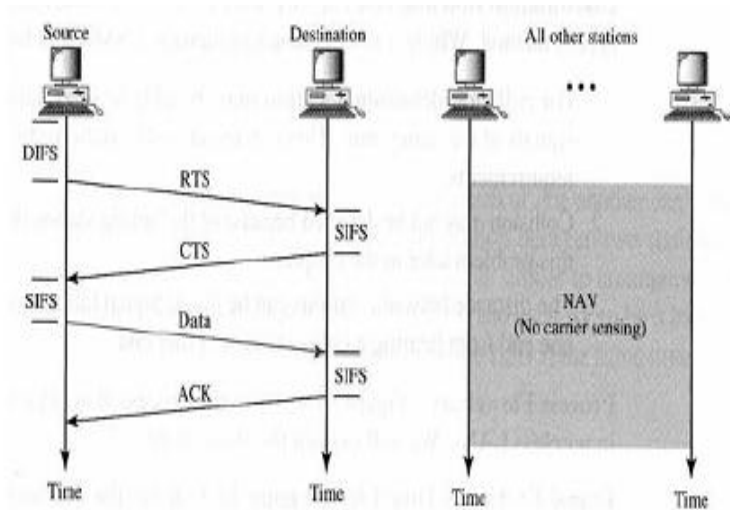


Gambar 2.9 Flowchart CSMA/CA pada WLAN[3]

Berikut penjelasan dari gambar 2.9:

1. Sebelum mengirim *frame* data, *station* sumber men-sense medium dengan mengecek sinyal *carrier* frekuensi pembawa.
  - a. Digunakan strategi pemantauan terus-menerus dengan *back-off* sampai dirasakan bahwa kanal sedang sepi (*idle*).

- b. Setelah *station* sumber merasakan adanya *idle*, *station* itu menunggu beberapa saat, dinamakan *Distributed Interframe Space* (DIFS); kemudian *station* sumber itu mengirim sebuah *frame* permintaan untuk mengirim, *Request to Send* (RTS)
2. Ketika menerima RTS dan kemudian diam beberapa saat dinamakan *Short Interframe Space* (SIFS), *station* tujuan mengirim sebuah *frame* kontrol, yang disebut *Clear to Send* (CTS) kepada *station* sumber. *Frame control* mengindikasikan bahwa *station* tujuan itu siap menerima data.
3. *Station* sumber mengirim data setelah diam beberapa saat selama SIFS.
4. *Station* tujuan setelah menerima data dan diam beberapa saat (selama SIFS) mengirimkan tanda terima *Acknowledgement* (ACK) untuk memberitahukan bahwa *frame* telah diterima. ACK ini diperlukan pada protocol ini karena *station* sumber tidak mempunyai piranti untuk mengecek keberhasilan bahwa data sampai tujuan.



Gambar 2.10 Proses pertukaran data[3]

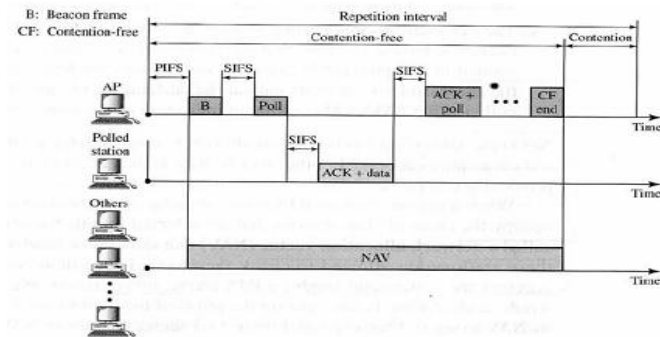
Ketika sebuah *station* mengirim *frame* RTS, itu sudah termasuk proses selang waktu yang dibutuhkan untuk memakai kanal. Station-station yang lain kemudian akan membangkitkan timer, dinamakan dengan *Network Allocation Vector* (NAV), untuk kemudian berdiam diri selama waktu itu. Setelah diam selama NAV, barulah mereka mengecek kembali kekosongan kanal. Setiap kali sebuah *station* mengakses kanal dan mengirim RTS, *station-station* yang lain akan mulai mengaktifkan NAVnya. Maka sebelum sebuah *station* men-sense apakah kanal kosong, terlebih dahulu ia mengecek NAVnya apakah sudah sampai

waktunya *men-sense*. Tabrakan terjadi ketika masih dalam proses akan mengirim data (*handshaking*). Dua atau lebih *station* mungkin mengirim RTS pada saat yang sama. Dan *frame-frame* kontrol itu akan bertabrakan di kanal. Karena tak ada mekanisme deteksi tabrakan (*collision detection*), sebuah *station* sumber hanya akan menduga bahwa telah terjadi tabrakan ketika ia tak menerima RTS dari *station* tujuan, kemudian mekanisme *back-off* diterapkan, dan sumber berusaha mengirim *frame* RTS lagi.

### 2.5.2 *Point Coordination Function (PCF)*

PCF merupakan metode akses pilihan yang hanya dapat diimplementasikan pada jaringan infrastruktur, bukan pada *ad-hoc*. PCF diterapkan di atas DCF dan digunakan untuk transmisi yang bersifat *time-sensitive*. PCF adalah tersentralisir, berupa metode akses polling bebas. *Access Point (AP)* membuat semacam tiket untuk *station-station* yang dapat diberi *polling*. *Station-station* itu diberi hak mengirim data secara bergiliran, untuk mengirim data ke AP. Untuk memberi prioritas pada PCF di atas DCF. Berarti bahwa apa bila pada saat yang sama sebuah *station* ingin menggunakan hanya DCF, sedangkan AP ingin memakai PCF, maka prioritas diberikan pada AP (yang akan memakai PCF) [3]. Namun adanya prioritas lebih pada PCF atas DCF dapat menyebabkan *station-station* yang

hanya mampu memakai DCF tidak dapat mengakses medium. Untuk mencegah hal ini, sebuah *repetition interval* dibuat untuk meng-cover baik lalu lintas PCF maupun DCF. *Repetition interval* ini berulang secara terus-menerus, dimulai dari sebuah frame control yang dinamakan *beacon frame*. Ketika para *station* mendengar adanya *beacon frame*, mereka akan mengaktifkan NAV untuk durasi waktu periode *repetition interval*. Gambar 2.11 menunjukkan sebuah contoh mengenai *repetition interval*.



Gambar 2.11 *Repetition interval*[3]

Selama *repetition interval*, *Point Controller* (PC) dapat mengirim sebuah *frame poll*, menerima data, mengirim ACK, menerima ACK, atau mengerjakan kombinasi semua itu. Pada akhir waktu *Contention Free*

(CF), PC mengirim *frame* CF end (*contention-free end*) agar *station-station* dengan *contention based* dapat menggunakan medium.

## 2.6 LAYANAN

### 2.6.1 *Hypertext Transfer Protocol (HTTP)*

*Hypertext Transfer Protocol (HTTP)* adalah sebuah protokol jaringan lapisan aplikasi yang digunakan untuk sistem informasi terdistribusi, kolaboratif, dan menggunakan hipermedia. Penggunaannya banyak pada pengambilan sumber daya yang saling terhubung dengan tautan, yang disebut dengan dokumen hiperteks, yang kemudian membentuk *World Wide Web* [9].

### 2.6.2 *File Transfer Protocol (FTP)*

*File Transfer Protocol (FTP)* adalah sebuah protokol Internet yang berjalan di dalam lapisan aplikasi yang merupakan standar untuk pengiriman berkas komputer antar mesin-mesin dalam sebuah antarjaringan. FTP merupakan salah satu protokol internet yang paling awal dikembangkan, dan masih digunakan hingga saat ini untuk melakukan pengunduhan (*download*) danunggahan (*upload*) berkas-berkas komputer antara klien FTP dan server FTP [9].

### 2.6.3 *Video Conference*

*Video conference* merupakan komunikasi visual yang dapat mengirimkan *audio video* agar dapat dilihat dan didengar secara bersamaan pada waktu yang sama dengan menggunakan jaringan internet atau fasilitas yang digunakan untuk melakukan pertemuan dengan dua pihak atau lebih dalam waktu yang bersamaan dan pada tempat yang berbeda dengan memanfaatkan jaringan internet. Komunikasi visual ini merupakan alternatif yang sangat efektif jika kondisi yang tidak memungkinkan untuk melakukan pertemuan pada satu lokasi dan waktu yang diinginkan. Dengan adanya *video conference* maka komunikasi visual dapat berjalan dengan baik pada lokasi yang berbeda. Salah satu implementasi *video conference* yaitu digunakan untuk melaksanakan kuliah jarak jauh [9].

## 2.7 **PARAMETER *QUALITY OF SERVICE***

### 2.7.1 *Throughput*

*Throughput* merupakan kecepatan transfer data efektif, yang diukur dalam bits/sec [11]. Pengukuran *throughput* bertujuan untuk mengetahui kehandalan jaringan dalam meneruskan data dalam rentang waktu tertentu. Nilai *throughput* dihitung dari total ukuran dari paket yang sampai pada sisi klien dibagi dengan rentang

waktu kedatangan paket pertama dan paket terakhir di sisi klien [11].

### 2.7.2 *Delay*

*Delay* merupakan waktu yang dibutuhkan sebuah paket untuk sampai ke titik akhir (*user*) setelah ditransmisikan dari titik akhir pengiriman (*server*). Kategori *delay* dapat dilihat pada tabel 2.1 seperti berikut ini:

Tabel 2.1 Kategori *Delay* [11]

Kategori	Besar <i>Delay</i>
Sangat Bagus	<150 ms
Bagus	150 ms-300ms
Sedang	300 ms-450ms
Jelek	> 450 ms

### 2.7.3 *Packet Loss*

*Packet loss* adalah banyaknya paket yang hilang selama proses transmisi ke tujuan. Paket hilang terjadi ketika satu atau lebih paket data yang melewati suatu jaringan gagal mencapai tujuannya.[5] *Packet Loss* dapat dicari dengan menggunakan persamaan matematika 2.2 dan



kategori *packet loss* dapat dilihat pada tabel 2.2 seperti berikut ini:

$$\text{Packet loss} = \frac{\text{Traffic Sent} - \text{Traffic Received}}{\text{Traffic Sent}} \times 100\% \dots\dots(1)$$

Tabel 2.2 Kategori *Packet Loss* [11]

Kategori	<i>Packet Loss</i>
Sangat Bagus	0 %
Bagus	3 %
Sedang	15 %
Jelek	25 %

## 2.8 *DIFFERENTIATED SERVICE CODE POINT (DSCP)*

DSCP merupakan pengembangan dari *Field Type of Service (ToS)*. Pada mulanya *field ToS* banyak digunakan untuk menyediakan QoS pada jaringan IP. QoS yang dimaksud adalah dengan membagi-bagi prioritas masing-masing layanan. *Field ToS* menggunakan 3 bit untuk membagi layanan yang disebut dengan nilai IP *Precedence*. Pada *field ToS*, nilai IP *Precedence* inilah yang menentukan prioritas suatu layanan. Nilai IP *Precedence* yang paling penting adalah *Critical*, *Flash override*, dan *Flash*. Pada umumnya *Critical* (5) digunakan untuk trafik VoIP atau

trafik *realtime (time sensitive)*, *Flash override* (4) untuk trafik video, dan *Flash* (3) untuk *multimedia streaming*. Pada umumnya, trafik lainnya dipetakan ke trafik *best effort* atau *Routine* (0) [6]. DSCP merupakan perluasan dari IP *Precedence* dan masih bisa dikodekan sebagai nilai ToS. Nilai DSCP adalah IP *Precedence* ditambah dengan variabel *delay*, *throughput*, dan *reliable*. Pada implementasi DSCP, variabel *delay* dan *throughput* disebut *drop probability*. Nilai-nilai DSCP yang sering digunakan adalah kelas-kelas *expedited forwarding* (EF) dan *assured forwarding* (AF) [6]

Tabel 2.3 DSCP dan Kelas Layanan

<b>Nama</b>	<b>Biner</b>	<b>IP Prec</b>	<b>Drop Pecedence</b>	<b>Layanan</b>
CS0	000 000	0		Standar (DNS, DHCP)
CS1	001 000	1		<i>Low Priority Data</i> (Semua trafik yang tidak mendapat jaminan <i>bandwidth</i> )
AF11	001 010	1	<i>Low</i>	<i>High-Throughput Data</i>
AF12	001 100	1	<i>Medium</i>	

AF13	001 110	1	<i>High</i>	<i>(Transfer File, Store and forward application)</i>
<b>Nama</b>	<b>Biner</b>	<b>IP Prec</b>	<b>Drop Pecedence</b>	<b>Layanan</b>
CS2	010 000	2		OAM (OAM&O)
AF21	010 010	2	<i>Low</i>	Data latency rendah (Transaksi web, transfer keuangan)
AF22	010 100	2	<i>Medium</i>	
AF23	010 110	2	<i>High</i>	
CS3	011 000	3		<i>Broadcast Video (broadcast TV &amp; live events, video surveillance, video on demand)</i>
AF31	011 010	3	<i>Low</i>	<i>Multimedia Streaming (Buffered Streaming Audio, Webcast)</i>
AF32	011 100	3	<i>Medium</i>	

<b>Nama</b>	<b>Biner</b>	<b>IP Prec</b>	<b>Drop Pecedence</b>	<b>Layanan</b>
CS4	100 000	4		<i>Real-time interactive (video conference,)</i>
AF41	100 010	4	<i>Low</i>	<i>Multimedia Conferencing (H323/v2 video conferencing)</i>
AF42	100 100	4	<i>Medium</i>	
AF43	100 110	4	<i>High</i>	
CS5	101 000	5		<i>Signaling (Perr-to-peer IP, IP telephony)</i>
EF	101 110	5		<i>Telephony (VoIP, Voice)</i>
CS6	110 000	6	<i>Routing</i>	<i>Network Control (Network Routing)</i>
CS7	111 000	7	<i>Network</i>	