Wireless
IEEE 802.11

- WLAN Standards
- Performance
- Architecture
- Security

IEEE 802.11 Standard

- IEEE 802.11b
- IEEE 802.11a
- IEEE 802.11g
- IEEE 802.11i
- IEEE 802.11n
- IEEE 802.11ac

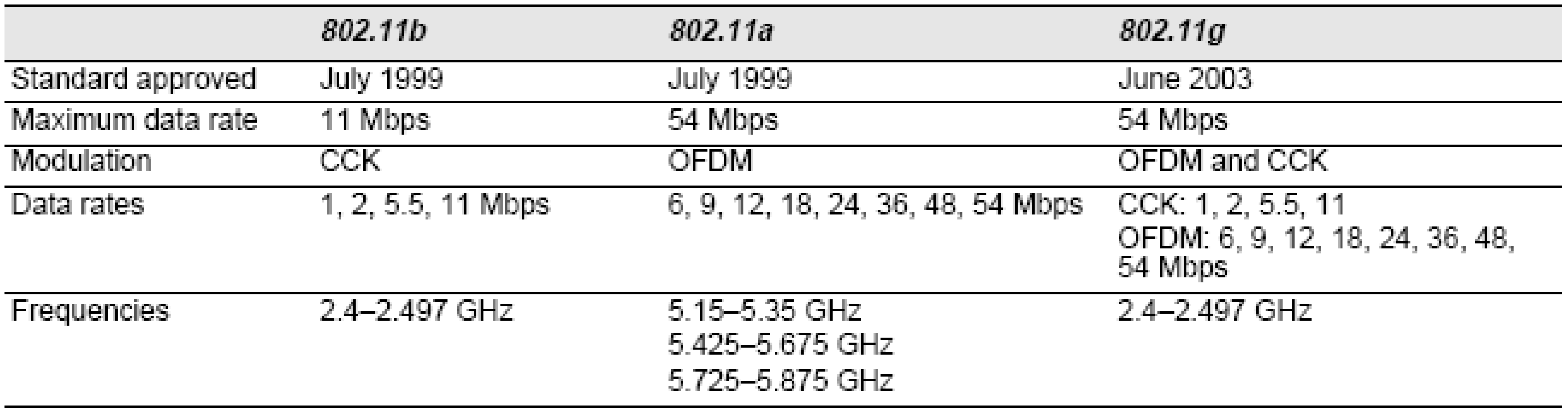


Table 1: IEEE 802.11 Specifications

	802.11b	*802.11a*	*802.11g*
Standard approved	July 1999	July 1999	June 2003
Maximum data rate	11 Mbps	54 Mbps	54 Mbps
Modulation	CCK	OFDM	OFDM and CCK
Data rates	1, 2, 5.5, 11 Mbps	6, 9, 12, 18, 24, 36, 48, 54 Mbps	CCK: 1, 2, 5.5, 11 OFDM: 6, 9, 12, 18, 24, 36, 48, 54 Mbps
Frequencies	2.4–2.497 GHz	5.15–5.35 GHz 5.425–5.675 GHz 5.725–5.875 GHz	2.4–2.497 GHz

802.11b

- CCK (Complimentary Code Keying)
- DSSS (Direct Sequence Spread Spectrum)
- 11 Mbps / 2.4 GHz
- 4 Data Rates (1, 2, 5,5 11 Mbps)
- Up to 3 non overlapping channels in the same area
- Up to 13 overlapping channels

802.11a

- 5 GHz
- The 802.11a standard was designed for higher bandwidth applications than 802.11b
- data rates of 6, 9, 12, 18, 24, 36, 48, 54 Mbps
- using (OFDM) orthogonal frequency division multiplexing
- modulation on up to 12 discrete channels.
- ประเทศไทยไม่อนุญาตให้มีการใช้งานอุปกรณ์ IEEE 802.11a เนื่องจากความถี่ย่าน 5 GHz ได้ถูกจัดสรรสำหรับกิจการอื่นอยู่ก่อนแล้ว

802.11g

- 2.4-GHz unlicensed spectrum
- 54 Mbps
- OFDM (the same technology used in 802.11a) and CCK as the mandatory modulation schemes with 24 Mbps
- Backward compatibility with 802.11b
- Possible range of both OFDM data rates of 54, 48, 36,24, 18, 12, 9, and 6 Mbps, and the CCK rates of 11, 5.5, 2, and 1 Mbps.

IEEE 802.11i

- security improvements for the 802.11 family (2004)

IEEE 802.11n

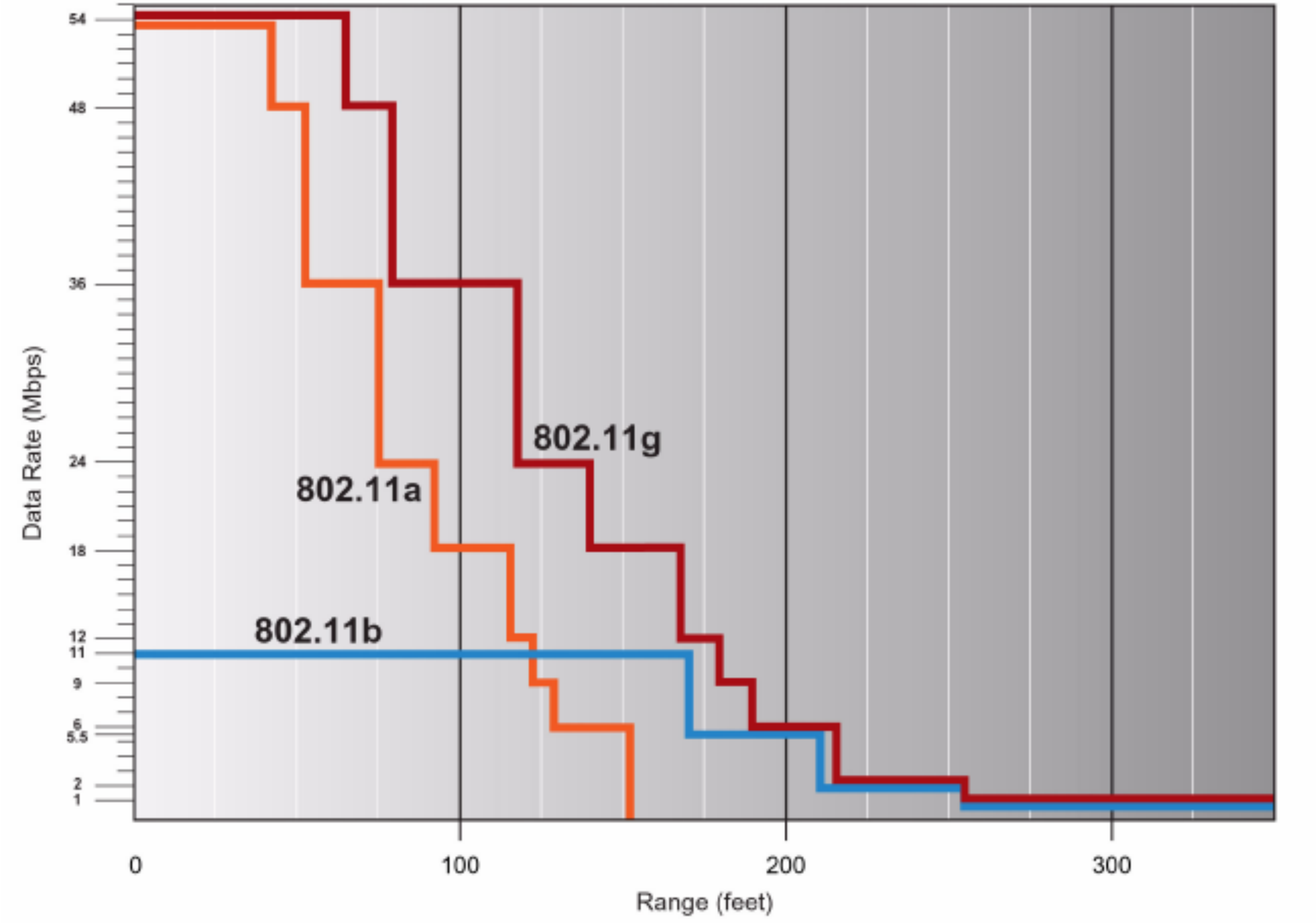
- *802.11n* (also sometimes known as "Wireless N") was designed to improve on 802.11g in the amount of bandwidth supported by utilizing multiple wireless signals and antennas (called *MIMO*technology) instead of one.
- Industry standards groups ratified 802.11n in 2009 with specifications providing for up to 300 Mbpsof network bandwidth. 802.11n also offers somewhat better range over earlier Wi-Fi standards due to its increased signal intensity, and it is backward-compatible with 802.11b/g gear.

- **Pros of 802.11n** - Fastest maximum speed and best signal range; more resistant to signal interference from outside sources.
- **Cons of 802.11n** - Standard is not yet finalized; costs more than 802.11g; the use of multiple signals may greatly interfere with nearby 802.11b/g based networks.

802.11ac

- The newest generation of Wi-Fi signaling in popular use, 802.11ac utilizes dual-band wirelesstechnology, supporting simultaneous connections on both the 2.4 GHz and 5 GHz Wi-Fi bands. 802.11ac offers backward compatibility to 802.11b/g/n and bandwidth rated up to 1300 Mbps on the 5 GHz band plus up to 450 Mbps on 2.4 GHz.

Range and Data Rate



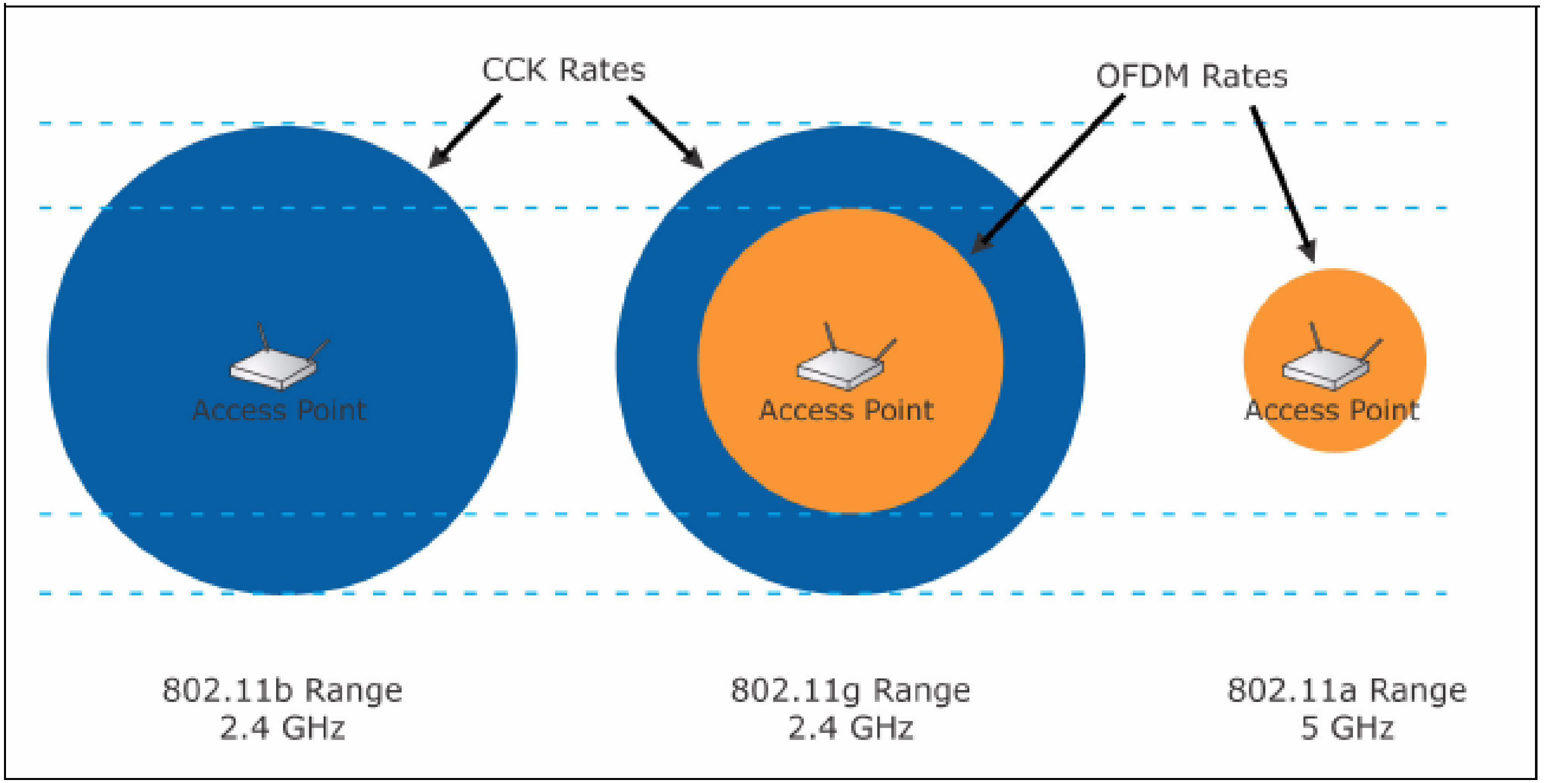


Figure 3: Relative Range of 802.11b, 802.11g, and 802.11a Devices

802.11g throughput

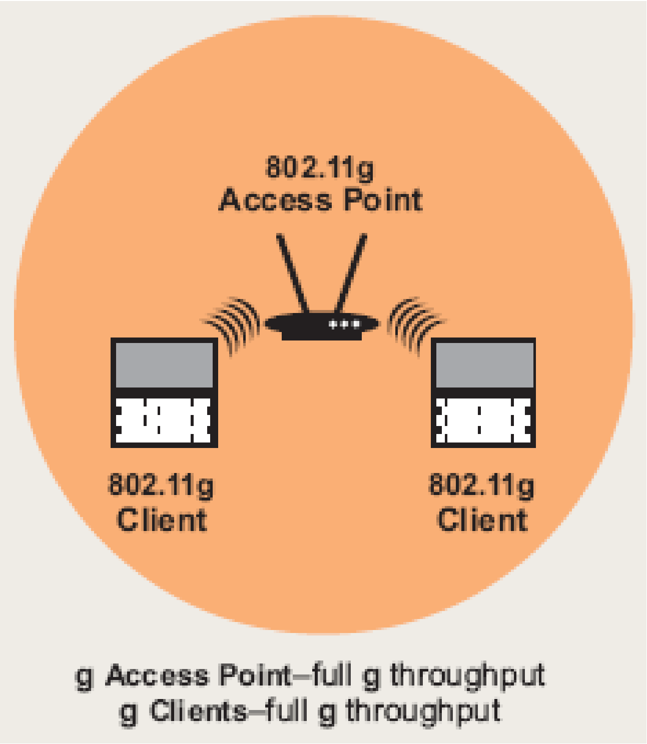
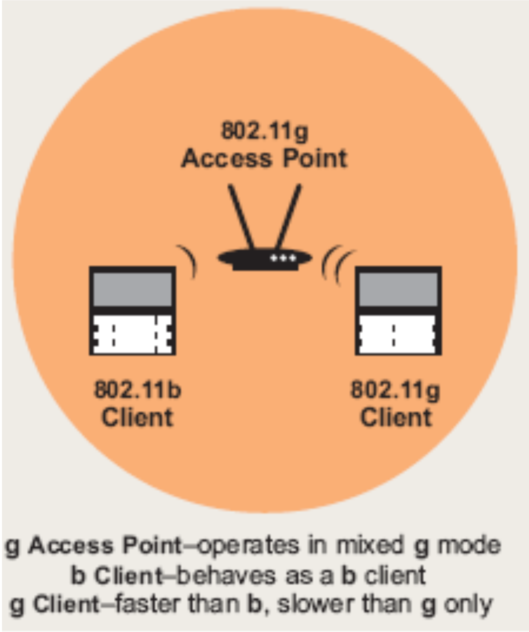


Figure 4: 802.11g-Only Environment

802.11g throughput



g Access Point–operates in mixed g mode
b Client–behaves as a b client
g Client–faster than b, slower than g only

Figure 5: 802.11g AP, Mixed Client Environment

802.11g throughput

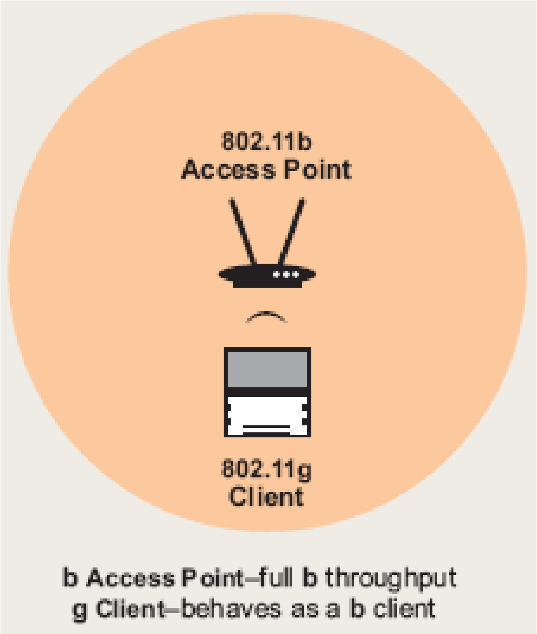
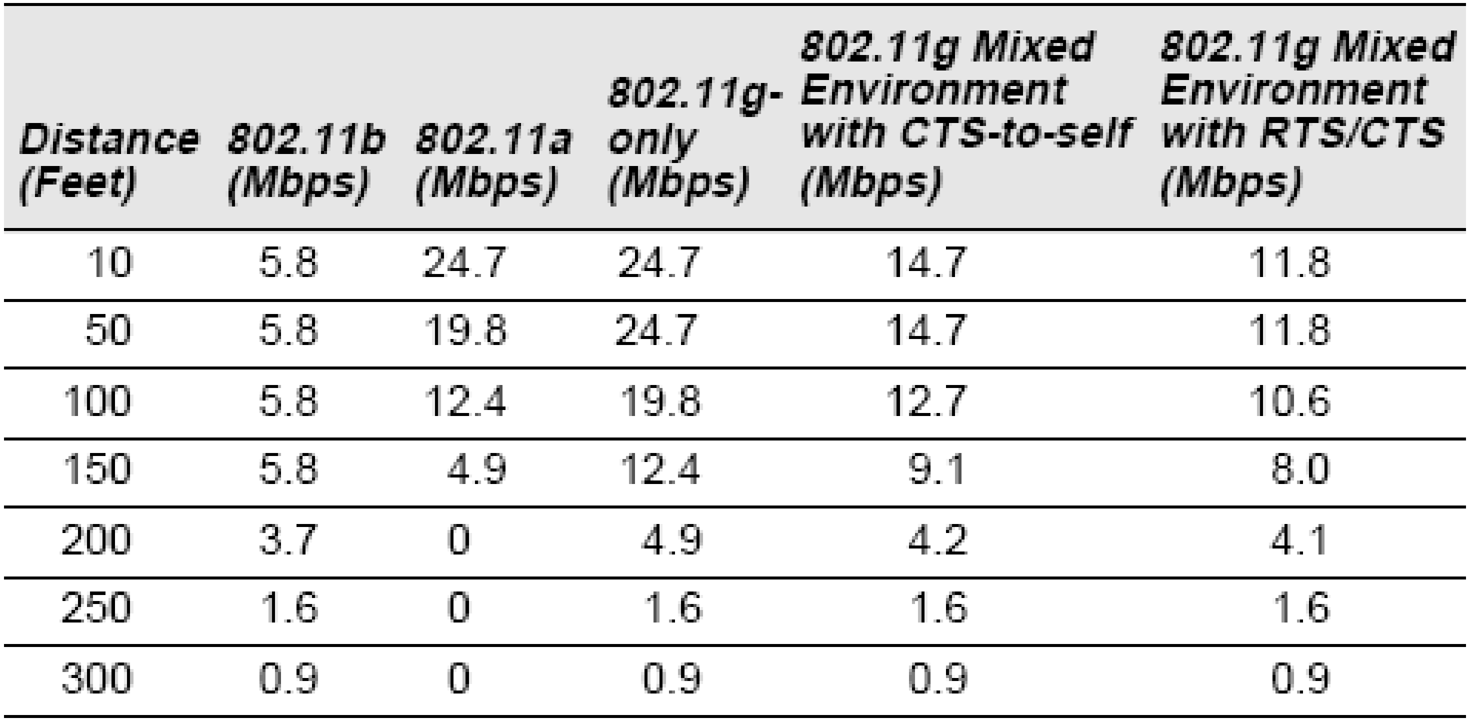

802.11b
Access Point
802.11g
Client
b Access Point–full b throughput
g Client–behaves as a b client

Figure 6: 802.11b AP, 802.11g
Client Environment

802.11g TCP throughput

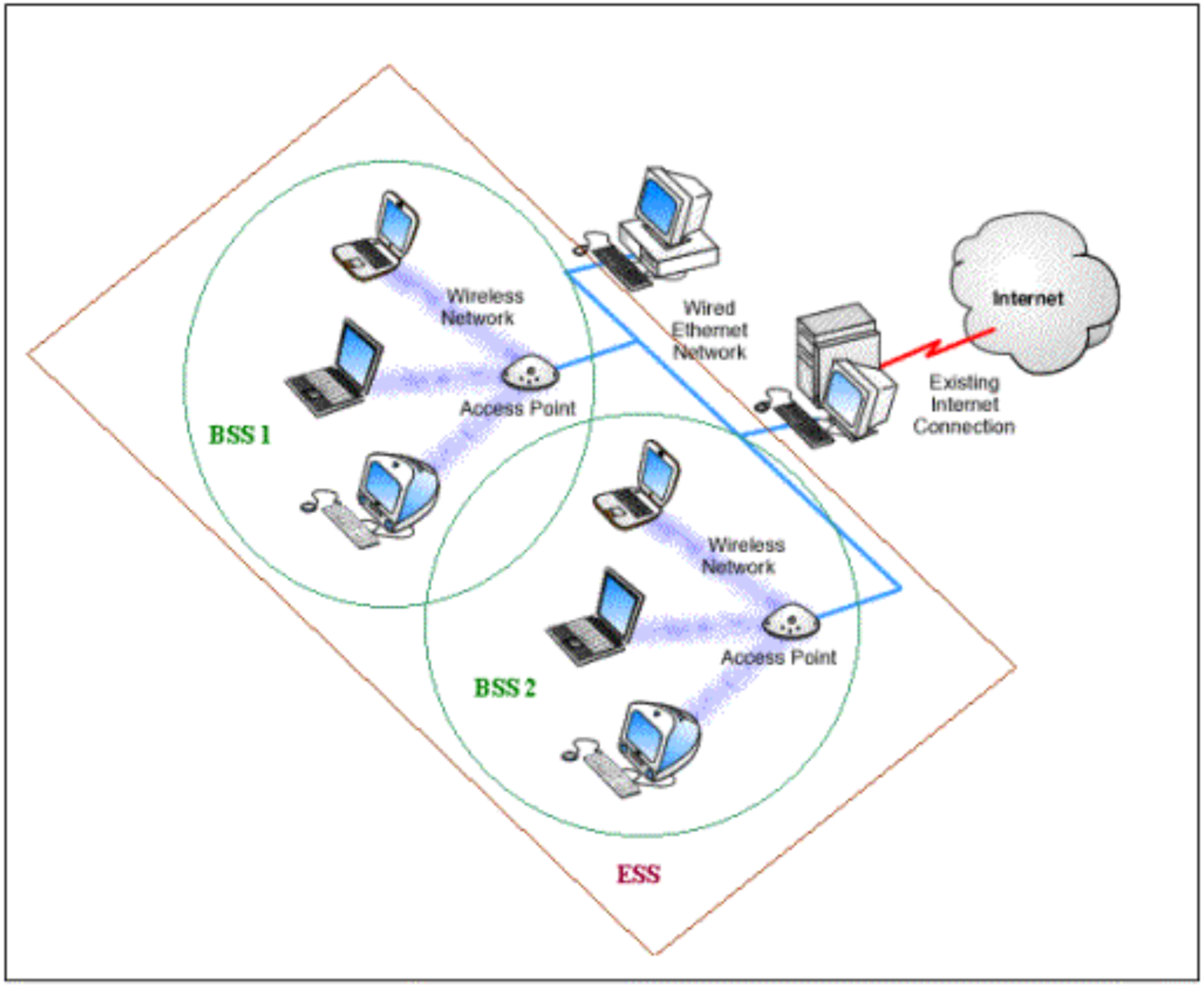


Distance (Feet)	802.11b (Mbps)	802.11a (Mbps)	802.11g-only (Mbps)	802.11g Mixed Environment with CTS-to-self (Mbps)	802.11g Mixed Environment with RTS/CTS (Mbps)
10	5.8	24.7	24.7	14.7	11.8
50	5.8	19.8	24.7	14.7	11.8
100	5.8	12.4	19.8	12.7	10.6
150	5.8	4.9	12.4	9.1	8.0
200	3.7	0	4.9	4.2	4.1
250	1.6	0	1.6	1.6	1.6
300	0.9	0	0.9	0.9	0.9

Architecture

1. โหมด Infrastructure
2. โหมด Ad-Hoc หรือ Peer-to-Peer

Infrastructure Mode

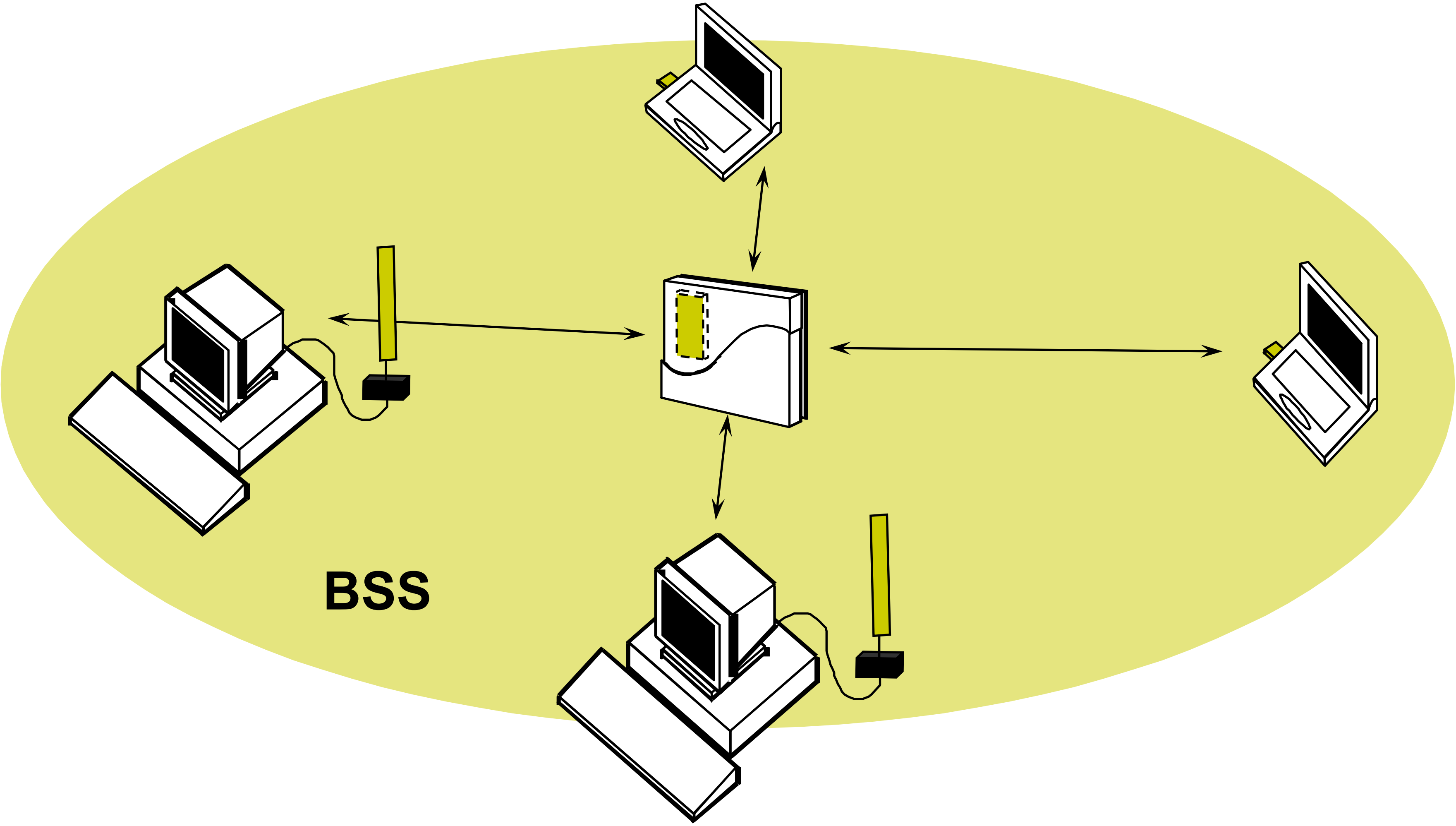


- **Basic Service Set (BSS)**
  - A set of stations controlled by a single “Coordination Function”
- **Extended Service Set (ESS)**
- A set of one or more Basic Service Sets interconnected by a Distribution System (DS)

Ad-Hoc or Peer to Peer

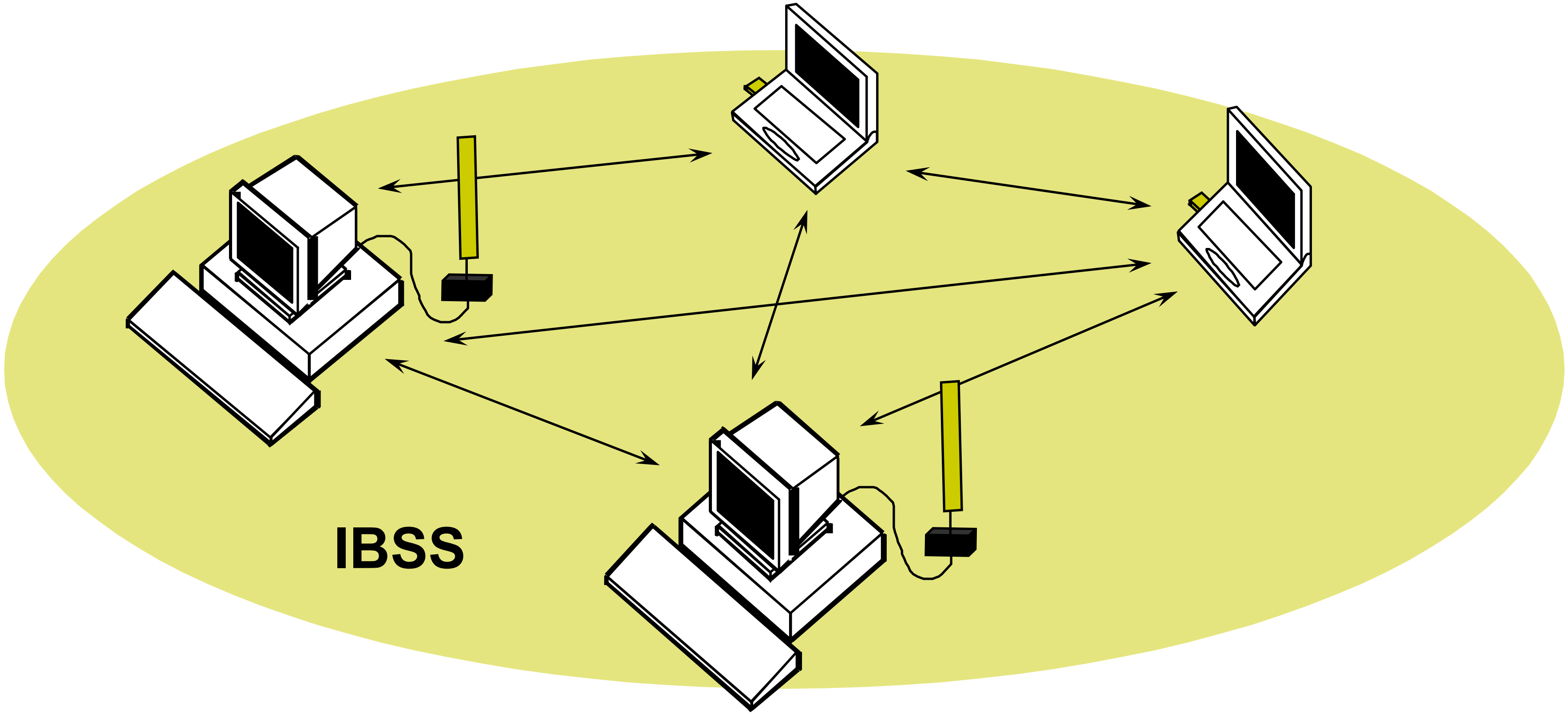
- May called ***Independent Basic Service Set***
- (IBSS)

Basic Service Set (BSS)



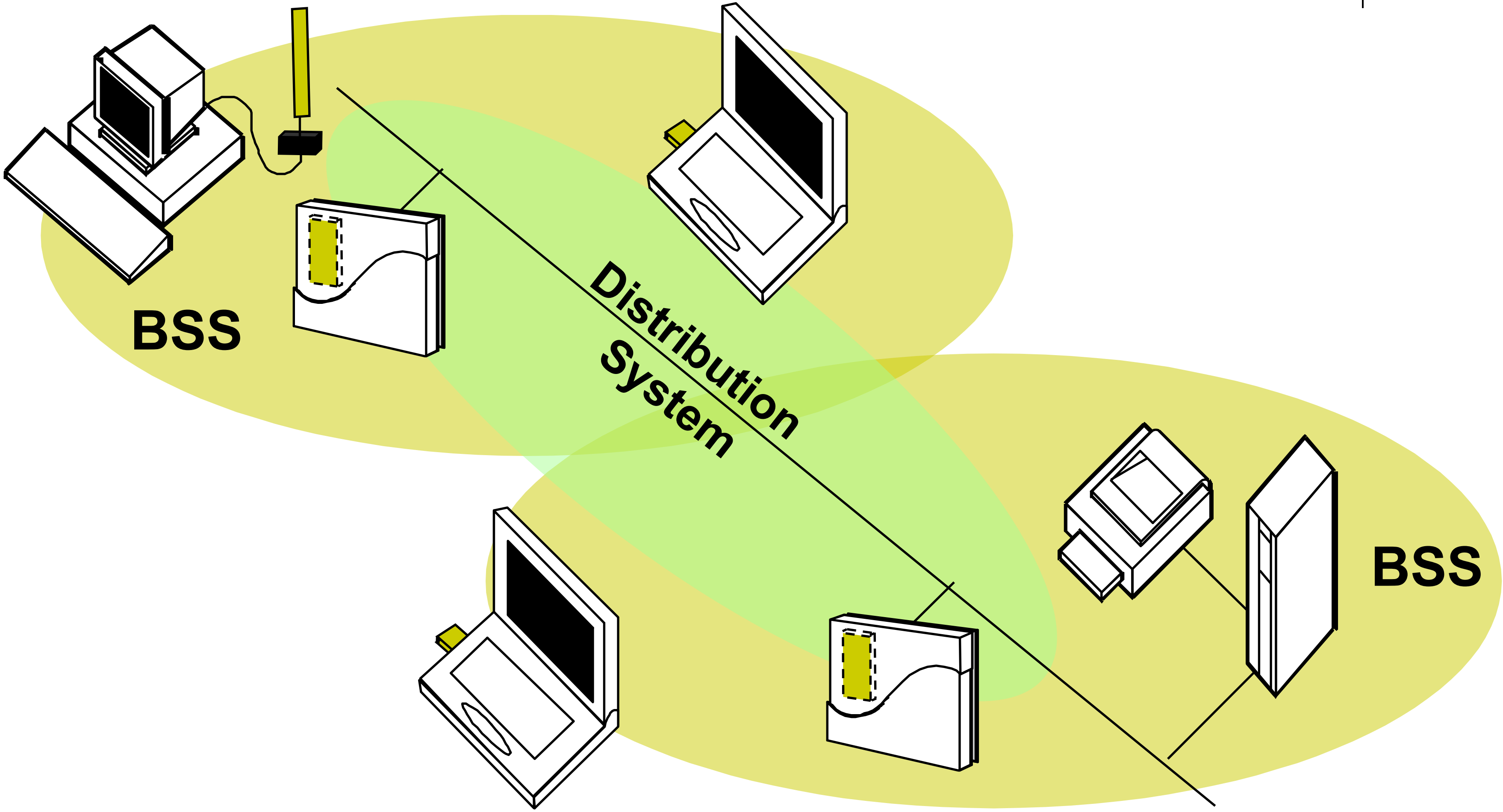
Independent Basic Service Set

(IBSS) or also called peer to peer



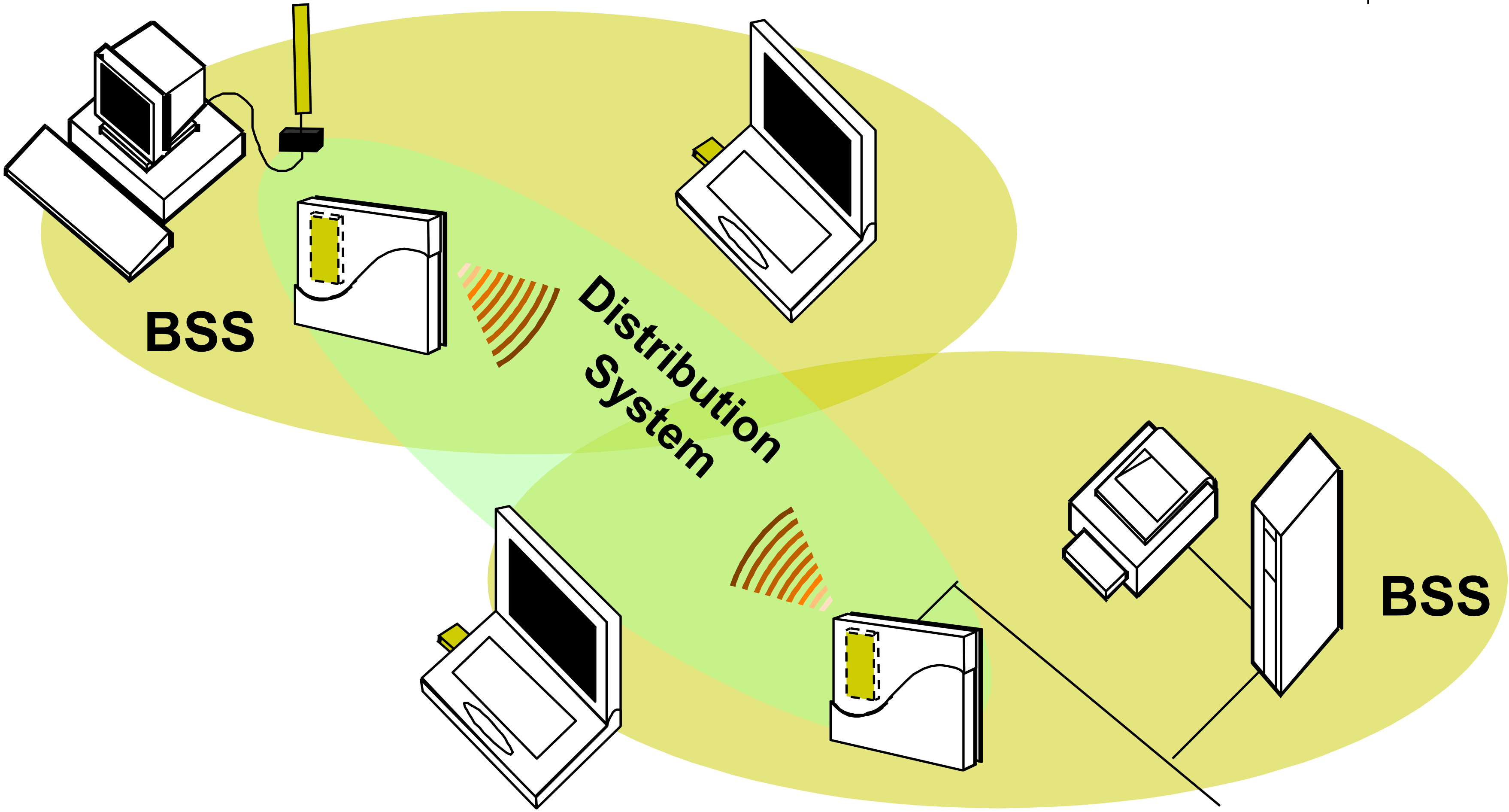
Extended Service Set (ESS)

BSS's with wired Distribution System (DS)



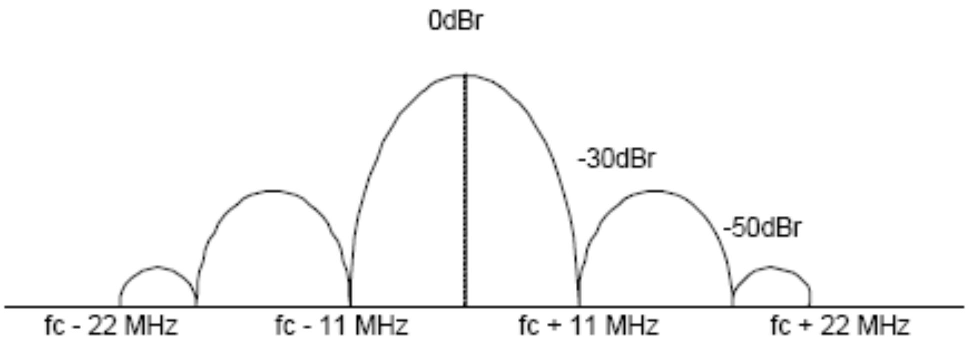
Extended Service Set (ESS)

BSS's and wireless Distribution System (DS)

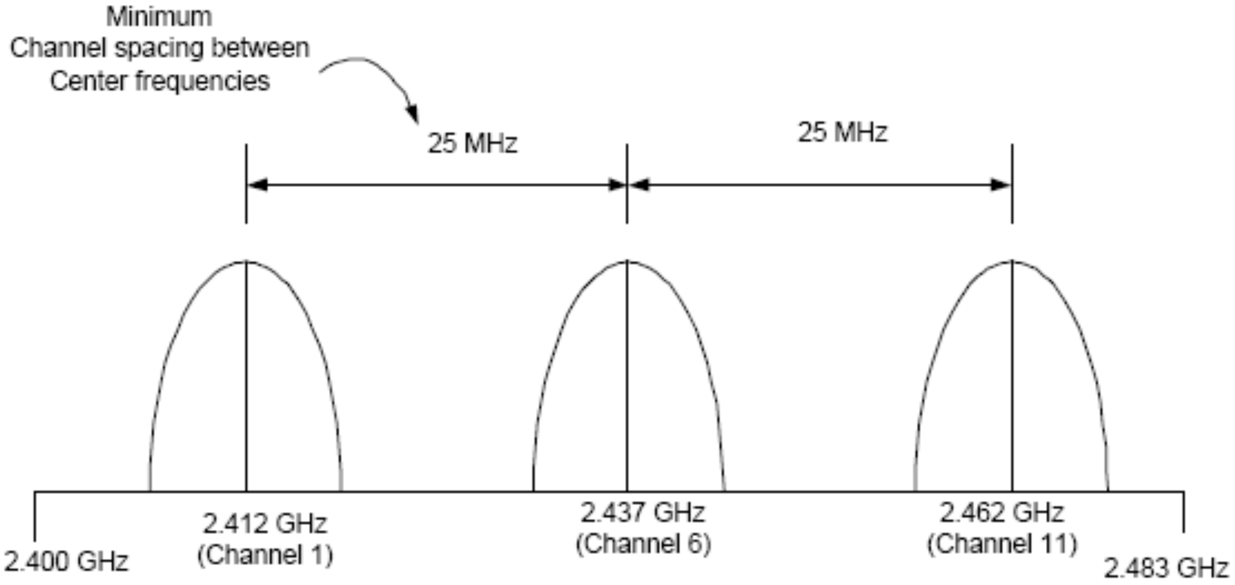


Operation Channel

- Noninterference channel min is 25 MHz apart in 2.4 GHz



Transmit Channel Shape



Architecture

Service Set Identifier (SSID):

- “Network name”
- 32 octets long
- Similar to “Domain-ID” in the pre-IEEE WaveLAN systems
- One network (ESS or IBSS) has one SSID
- also known as a WLAN ServiceArea ID

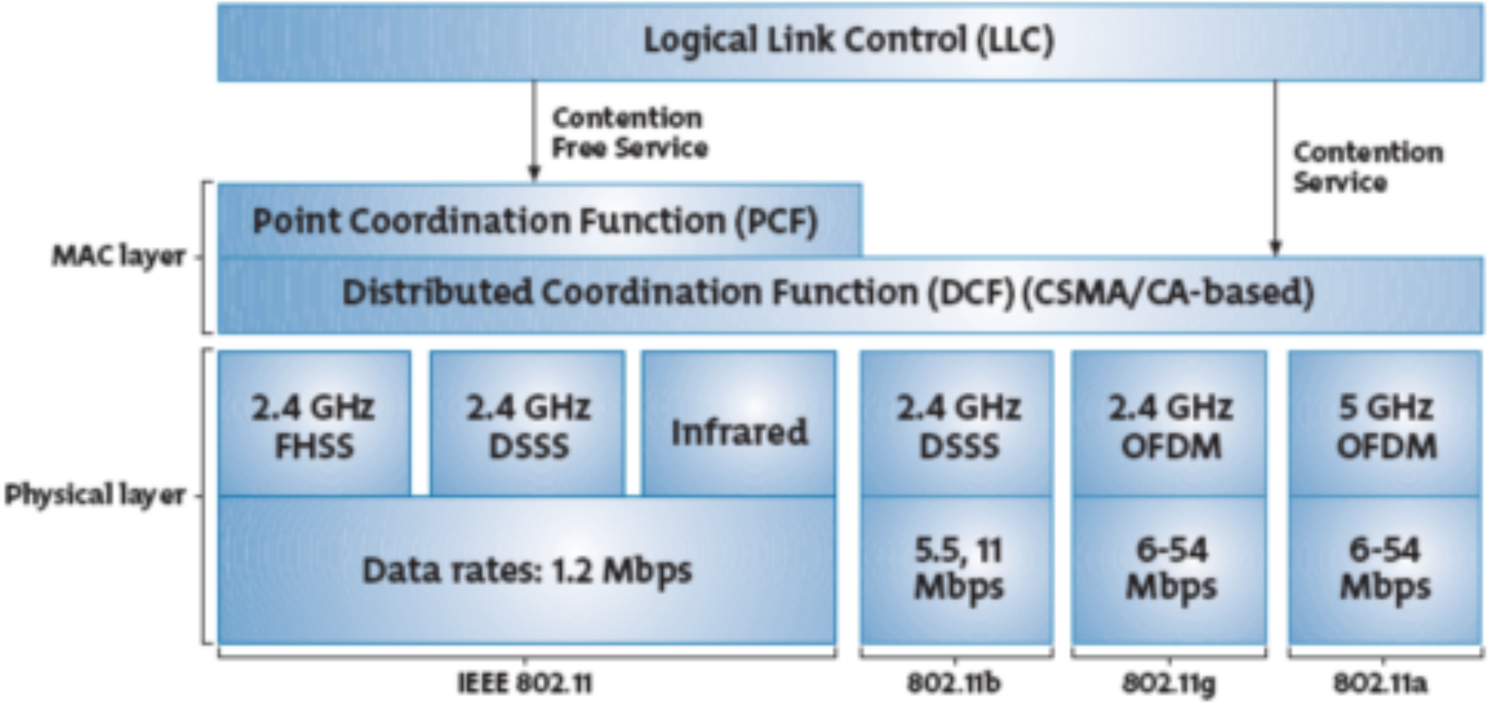
Basic Service Set Identifier (BSSID)

- “cell identifier”
- 6 octets long (MAC address format)
- Similar to NWID in pre-IEEE WaveLAN systems
- One BSS has one SSID
- Value of BSSID is the same as the MAC address of the radio in the Access-Point

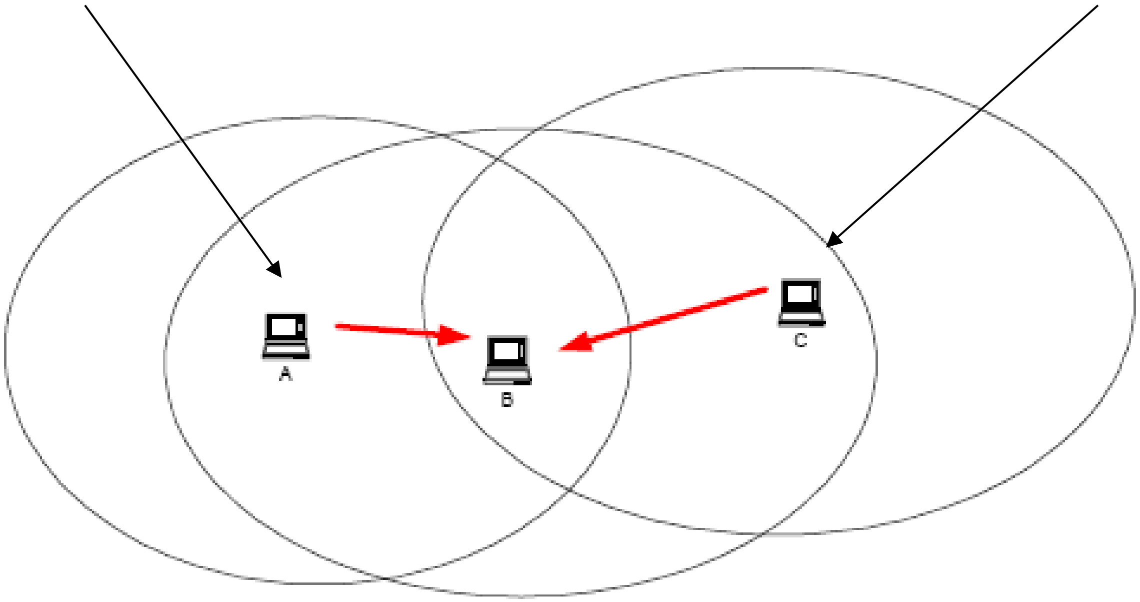
Architecture

- 802.11 Layer
- MAC (Media Access Control)
    - Basic processes in IEEE 802.11 networks (CSMA/CA)

IEEE 802.11 Layer



Hidden Node Problem

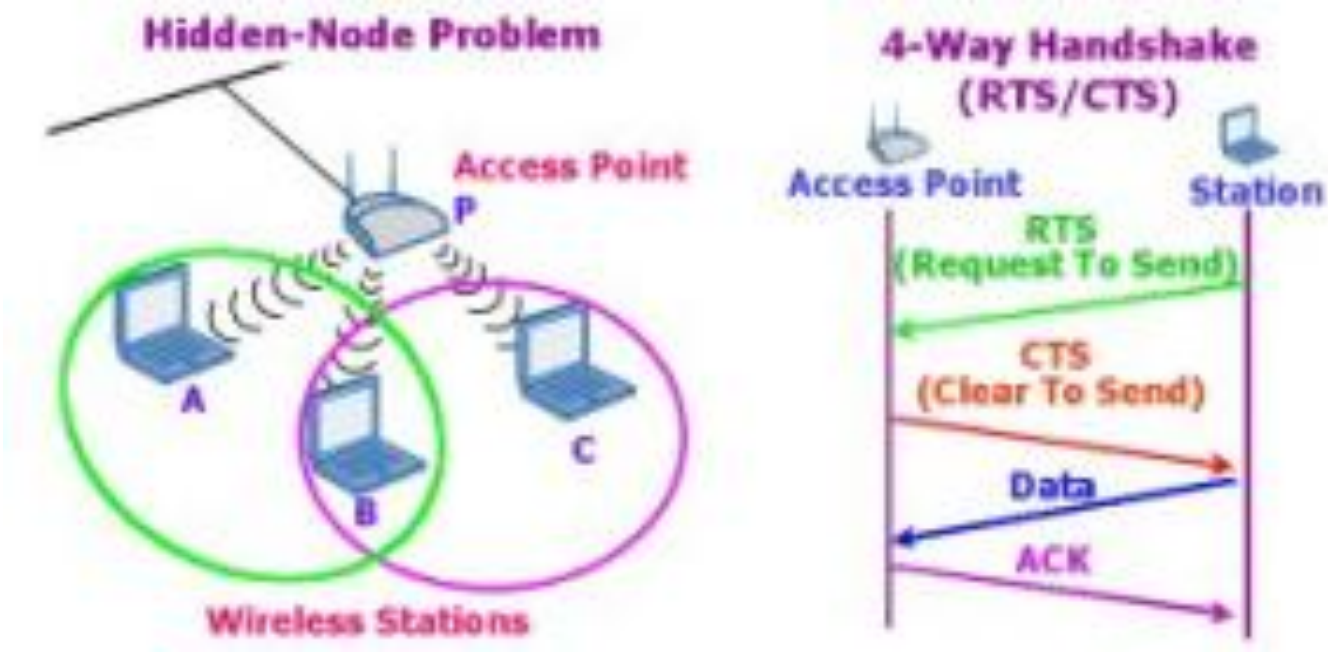


- On the wireless environment, we can not assume that all stations will here each other (Basic assumption for Collision Detect)

CSMA/CA

- Thus, IEEE 802.11 use *Collision Avoidance* rather than CA (collision detect) with Positive Acknowledgement Scheme (RTS/CTS Concept)

Virtual Carrier Sense (RTS and CTS) Concept



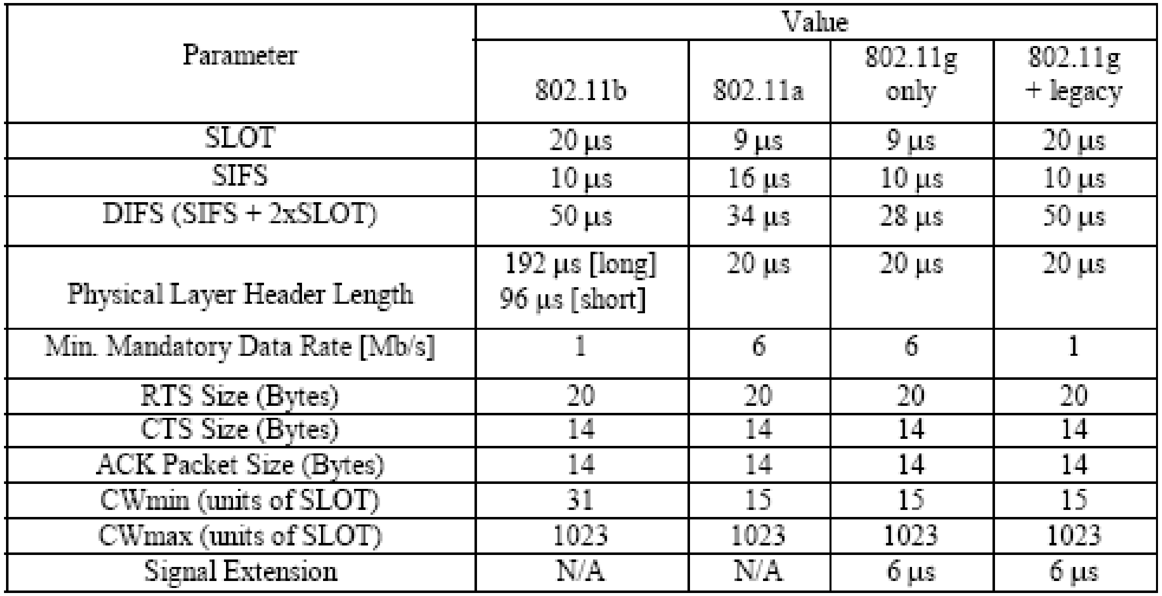
A station willing to transmit a packet, if the medium is free for a specified time Called DIFS, Distributed Inter Frame Space), then the station is allow to send Request To Send (RTS) which will include “Source, Destination and duration of the transmission time.

The destination will response (if the medium is free) with Clear To Send (CTS)

- *All station receiving either RTS and/or CTS, will set their* ***Virtual Carrier Sense*** indicator called ***NAV (Network Allocation Vector)***
- They will use this duration information with Physical Carrier Sense when sensing medium

- Time Intervals (ช่วงเวลาใน MAC)
  - PHY Determines: SIFS (Shot Inter Frame Space)
  - PHY Determines: Slot Time
  - PIFS (Priority Inter Frame Space) = SIFS + 1 Slot
  - DIFS (Distributed Inter Frame Space) = SIFS +

Table 1 Summary of important constants in 802.11b, 802.11a and 802.11g



Parameter	Value			
	802.11b	802.11a	802.11g only	802.11g + legacy
SLOT	20 µs	9 µs	9 µs	20 µs
SIFS	10 µs	16 µs	10 µs	10 µs
DIFS (SIFS + 2xSLOT)	50 µs	34 µs	28 µs	50 µs
Physical Layer Header Length	192 µs [long] 96 µs [short]	20 µs	20 µs	20 µs
Min. Mandatory Data Rate [Mb/s]	1	6	6	1
RTS Size (Bytes)	20	20	20	20
CTS Size (Bytes)	14	14	14	14
ACK Packet Size (Bytes)	14	14	14	14
CWmin (units of SLOT)	31	15	15	15
CWmax (units of SLOT)	1023	1023	1023	1023
Signal Extension	N/A	N/A	6 µs	6 µs

- **DCF**
  - The basic 802.11 MAC layer uses the Distributed Coordination Function (DCF) to share the medium between multiple stations. DCF relies on CSMA/CA and optional 802.11 RTS/CTS to share the medium between stations. This has several limitations:
  - if many stations communicate at the same time, many collisions will occur, which will lower the available bandwidth (just like in Ethernet, which uses CSMA/CD)
  - there is no notion of high or low priority traffic
  - once a station "wins" access to the medium, it may keep the medium for as long as it chooses. If a station has a low bit rate (1 Mbit/s, for example), then it will take a long time to send its packet, and all other stations will suffer from that.
  - more generally, there are no Quality of Service (QoS) guarantees.

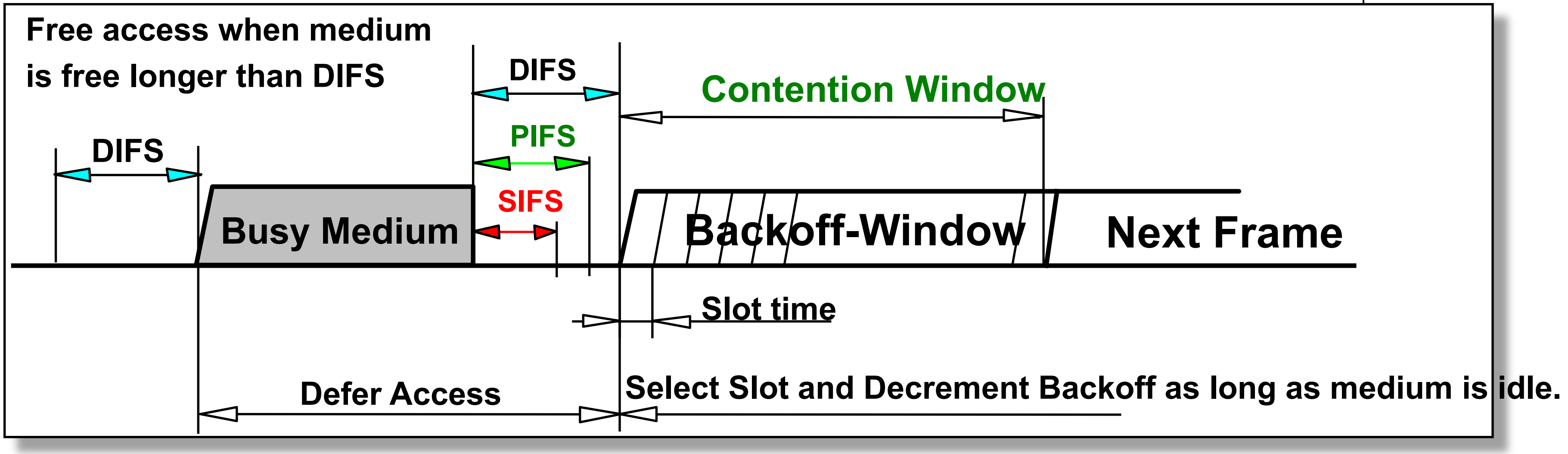
- **PCF**
  - The original 802.11 MAC defines another coordination function called the Point Coordination Function (PCF): this is available only in "infrastructure" mode, where stations are connected to the network through an Access Point (AP). This mode is optional, and only very few APs or Wi-Fi adapters actually implement it. APs send "beacon" frames at regular intervals (usually every 0.1 second). Between these beacon frames, PCF defines two periods: the Contention Free Period (CFP) and the Contention Period (CP). In CP, the DCF is simply used. In CFP, the AP sends Contention Free-Poll (CF-Poll) packets to each station, one at a time, to give them the right to send a packet. The AP is the coordinator. This allows for a better management of the QoS. Unfortunately, the PCF has limited support and a number of limitations (for example, it does not define classes of traffic).

CSMA/CA with Acknowledgement (DCF Operation)

IN CSMA/CA a Wireless node that wants to transmit performs the following sequence:

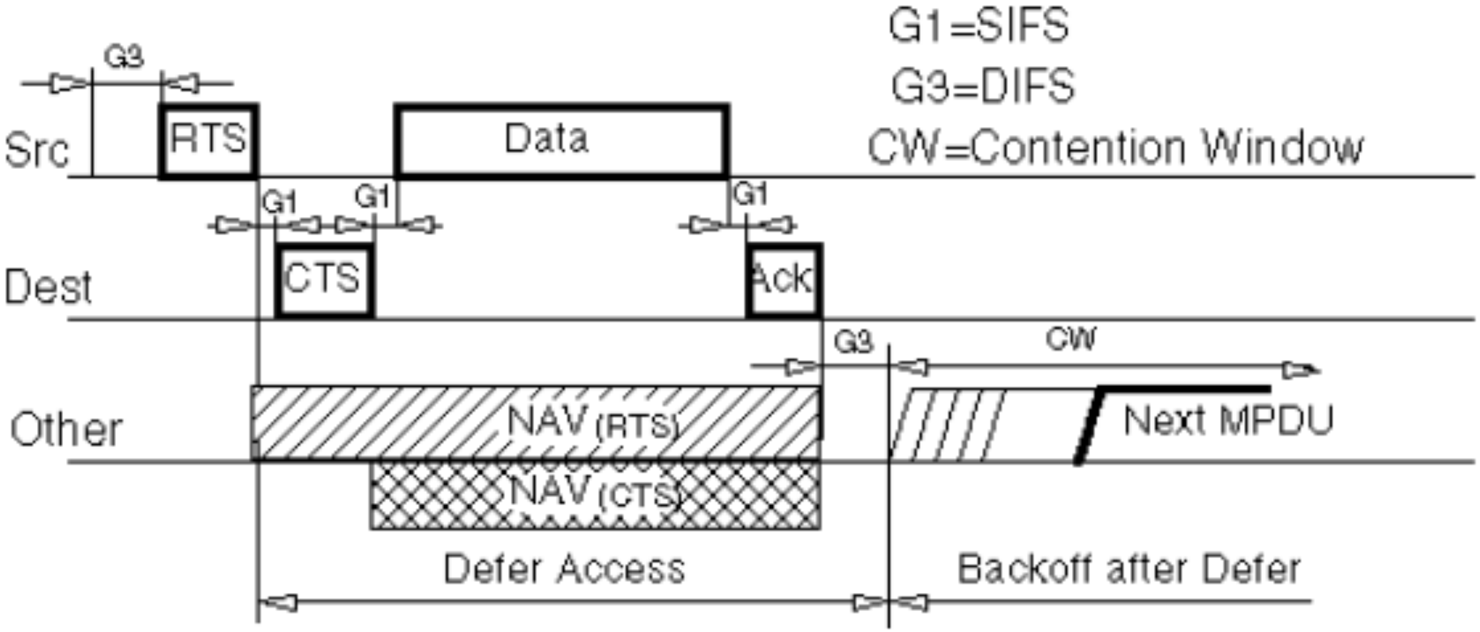
1. Listen on the desired channel.
2. If channel is idle for SIFS (no active transmitters) it sends a packet (RTS).
3. If channel is busy (an active transmitter) node waits until transmission stops then a further **CONTENTION** period. (The Contention period is a random period after every transmit on every node and statistically allows every node equal access to the media. To allow tx to rx turn around the contention time is **slotted** 50 micro sec for FH and 20 micro sec for DS systems).
4. If the channel is still idle at the end of the **CONTENTION** period the node transmits its packet otherwise it repeats the process defined in 3 above until it gets a free channel.

Access to the medium



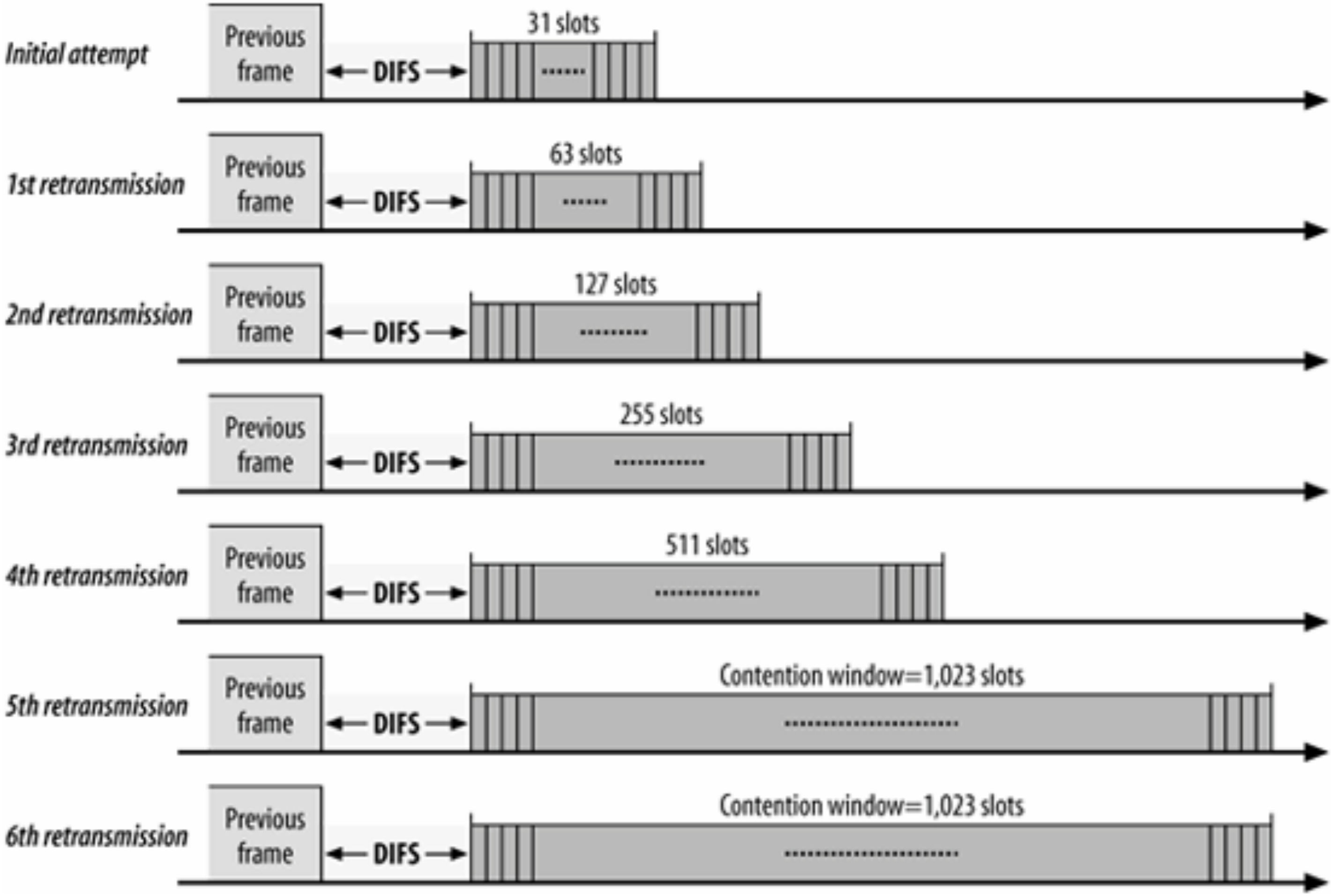
- Inter frame spacing required for MAC protocol traffic
  - SIFS = Short interframe space
  - PIFS = Priority interframe space
  - DIFS = Distributed interframe space
- Back-off timer expressed in terms of number of time slots

Data transmission

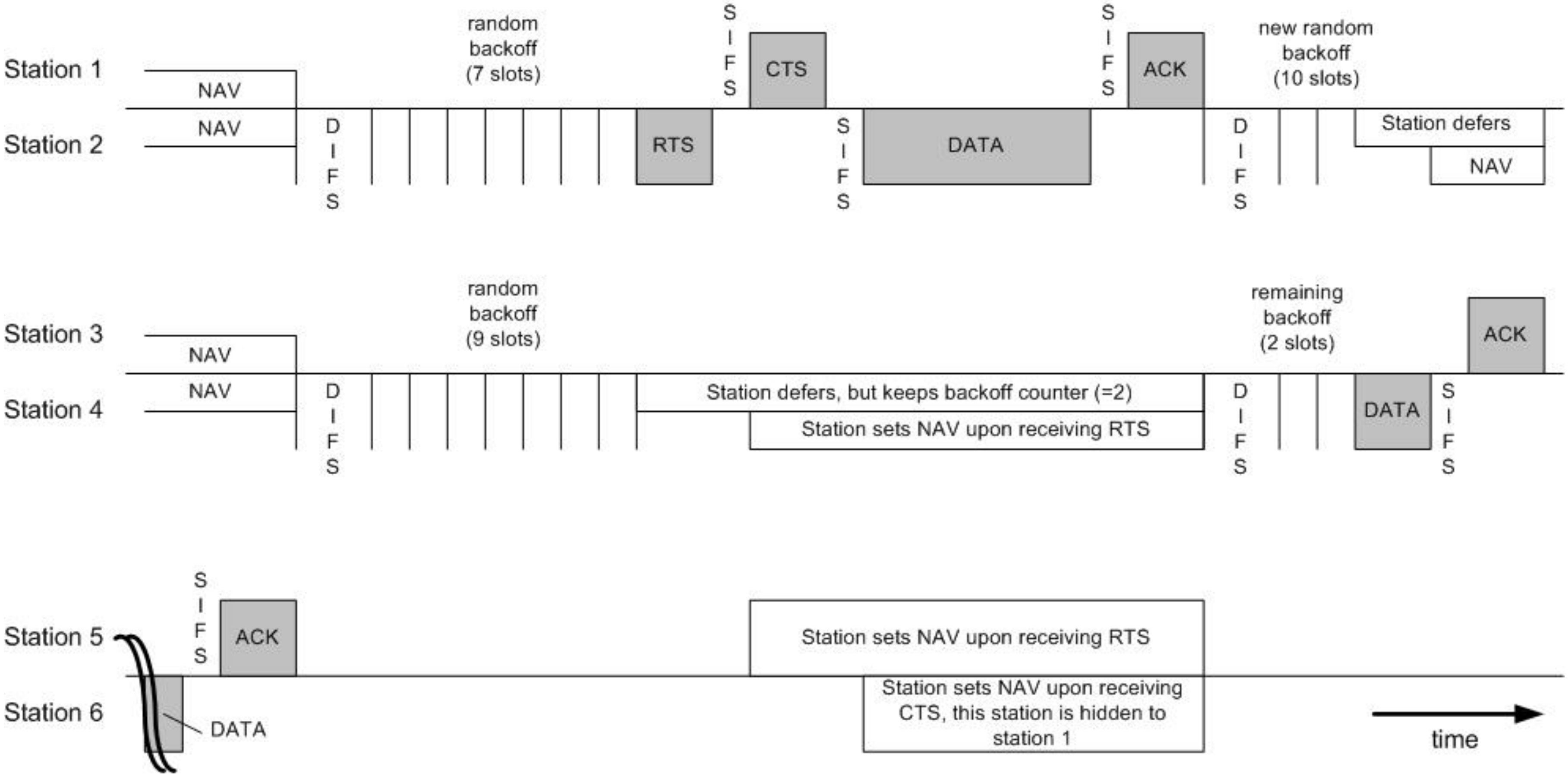


- Acknowledgment are to arrive at within the SIFS

Backoff


Initial attempt
Previous frame
DIFS
31 slots
1st retransmission
Previous frame
DIFS
63 slots
2nd retransmission
Previous frame
DIFS
127 slots
3rd retransmission
Previous frame
DIFS
255 slots
4th retransmission
Previous frame
DIFS
511 slots
5th retransmission
Previous frame
DIFS
Contention window=1,023 slots
6th retransmission
Previous frame
DIFS
Contention window=1,023 slots

DCF Operation


Station 1
Station 2
Station 3
Station 4
Station 5
Station 6
NAV
NAV
DIFS
random backoff (7 slots)
RTS
SIFS
CTS
SIFS
DATA
SIFS
ACK
DIFS
new random backoff (10 slots)
Station defers
NAV
NAV
NAV
DIFS
random backoff (9 slots)
Station defers, but keeps backoff counter (=2)
Station sets NAV upon receiving RTS
remaining backoff (2 slots)
DIFS
DATA
SIFS
ACK
SIFS
ACK
DATA
Station sets NAV upon receiving RTS
Station sets NAV upon receiving CTS, this station is hidden to station 1
time

PCF Operation

- Poll – eliminates contention
- PC – Point Coordinator
  - Polling List
  - Over DCF
  - PIFS
- CFP – Contention Free Period
  - Alternate with DCF
- Periodic Beacon – contains length of CFP
- CF-Poll – Contention Free Poll
- NAV prevents during CFP
- CF-End – resets NAV

Frame Format

Preamble	PLCP	MAC Data	CRC

<u>Preamble</u>

- **Sync: 80 bits**

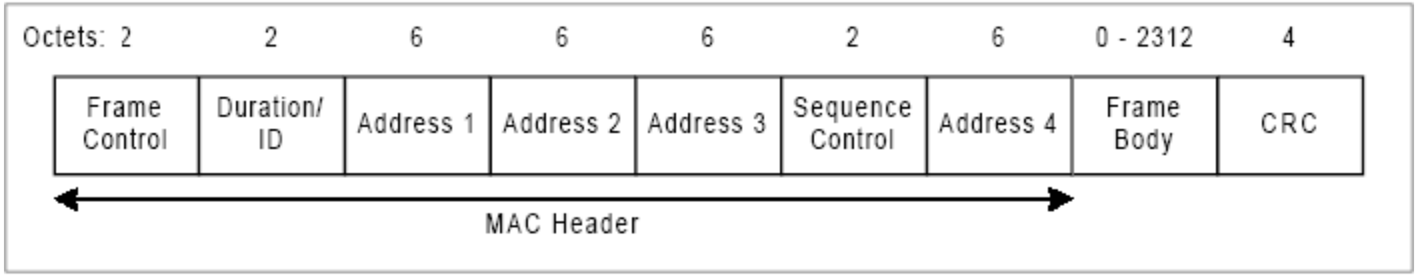
•SDF: Start of Fame Delimiter

<u>PLCP Physical Layer Convergence Procedure</u>

<u>MAC Data (Data transmits from MAC Layer – See the following)</u>

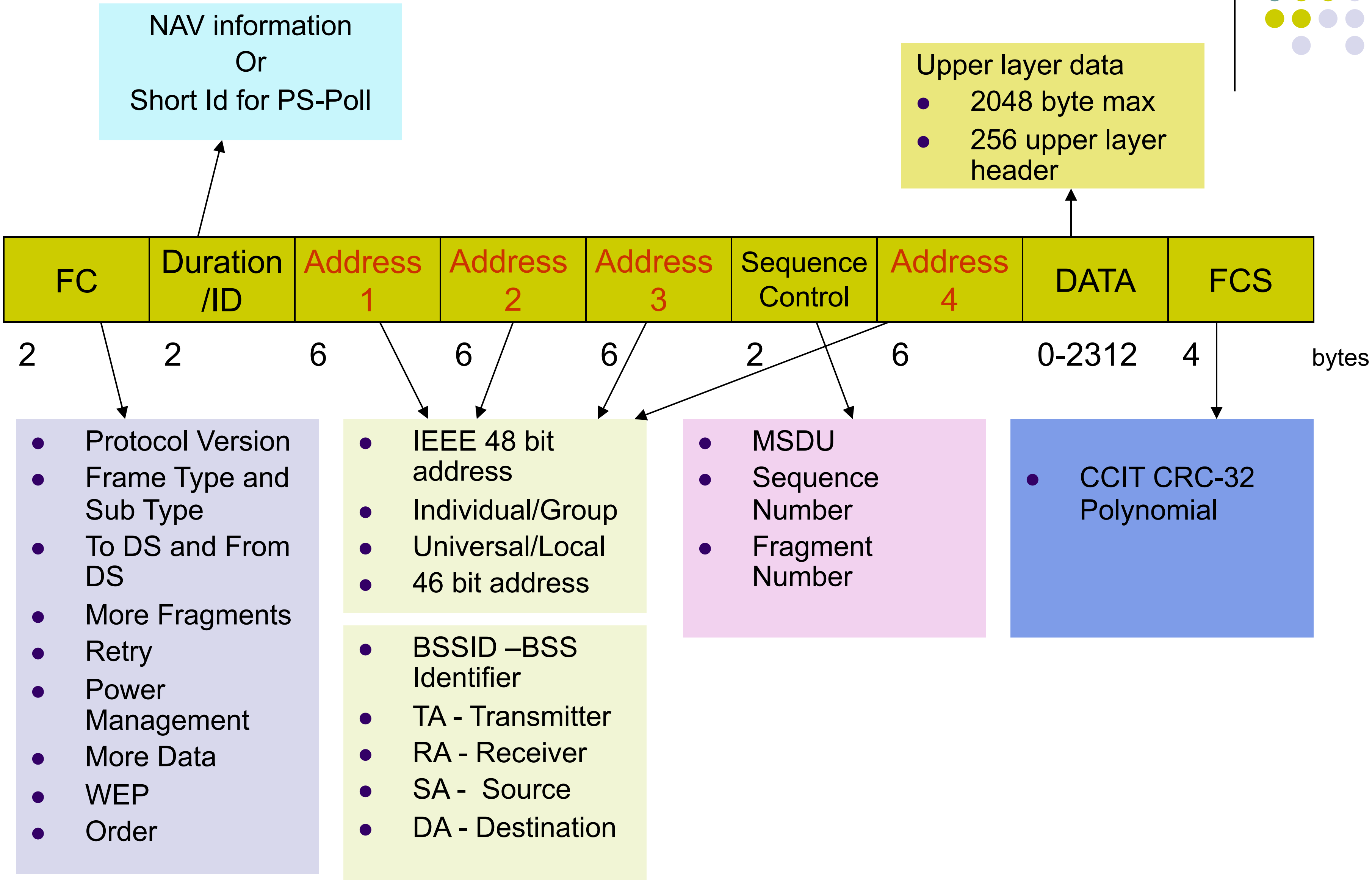
<u>CRC Error Checking</u>

MAC Data



Octets: 2	2	6	6	6	2	6	0 - 2312	4
Frame Control	Duration/ ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Frame Body	CRC

Frame Types



NAV information
Or
Short Id for PS-Poll

Upper layer data
- 2048 byte max
- 256 upper layer header

FC	Duration /ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	DATA	FCS	
2	2	6	6	6	2	6	0-2312	4	bytes

- Protocol Version
- Frame Type and Sub Type
- To DS and From DS
- More Fragments
- Retry
- Power Management
- More Data
- WEP
- Order

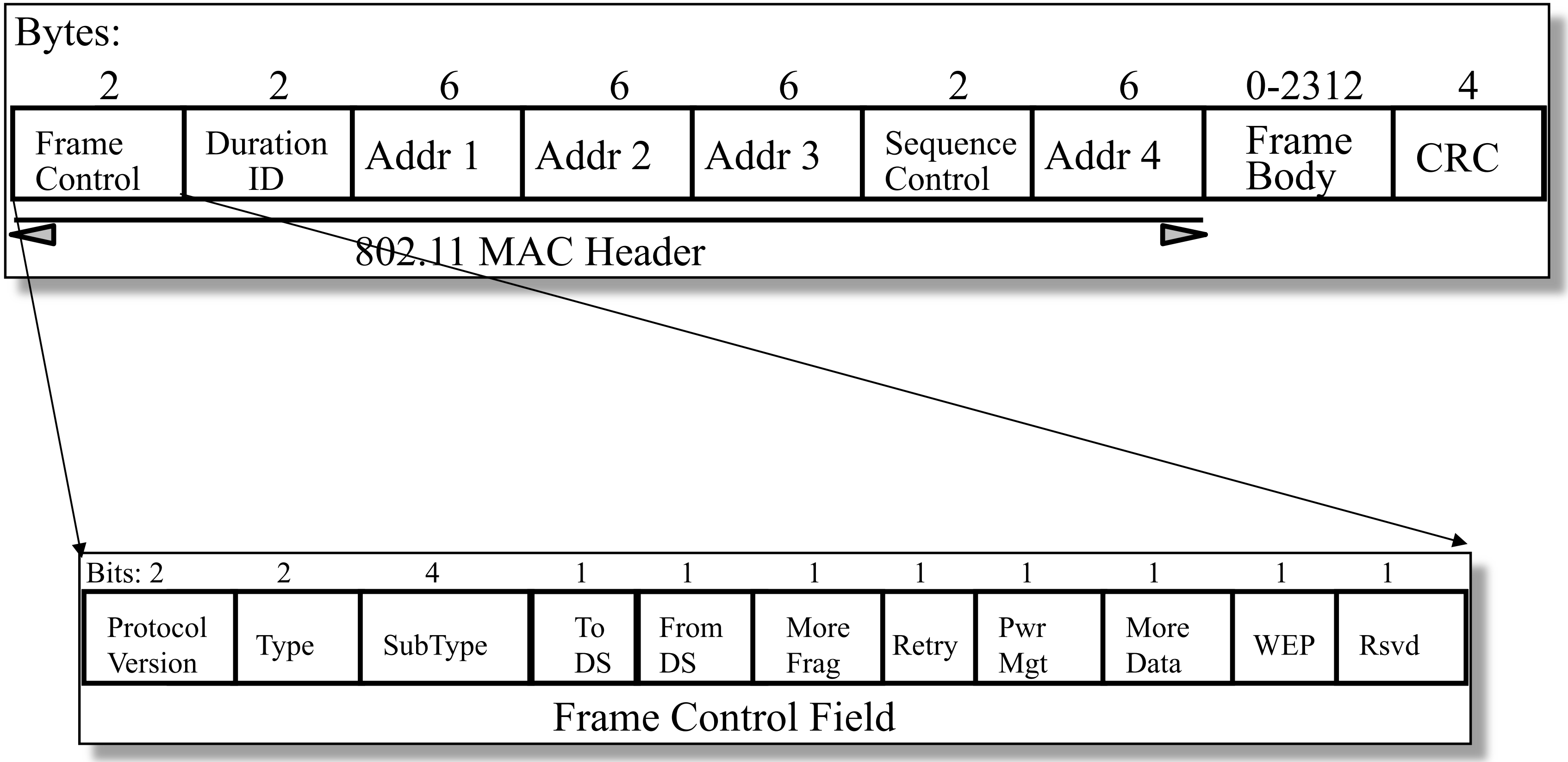
- IEEE 48 bit address
- Individual/Group
- Universal/Local
- 46 bit address

- BSSID –BSS Identifier
- TA - Transmitter
- RA - Receiver
- SA - Source
- DA - Destination

- MSDU
- Sequence Number
- Fragment Number

- CCIT CRC-32 Polynomial

Frame Formats
- Frame Control Filed



Bytes: 2	2	6	6	6	2	6	0-2312	4
Frame Control	Duration ID	Addr 1	Addr 2	Addr 3	Sequence Control	Addr 4	Frame Body	CRC

802.11 MAC Header

Bits: 2	2	4	1	1	1	1	1	1	1	1
Protocol Version	Type	SubType	To DS	From DS	More Frag	Retry	Pwr Mgt	More Data	WEP	Rsvd

Frame Control Field

Frame Control

- 2 bits Version
- 2 bits type + 4 bit subtype

  MAC Header format differs per Type:

  - Control Frames (several fields are omitted)
  - Management Frames
  - Data Frames

Type field descriptions

Bits: 2	2	4	1	1	1	1	1	1	1	1
Protocol Version	Type	SubType	To DS	From DS	More Frag	Retry	Pwr Mgt	More Data	WEP	Rsvd

Frame Control Field

Type and subtype identify the function of the frame:

- Type=00 Management Frame

  Beacon

  Probe

  Power Management

  (Re)Association

  (De)Authentication

- Type=01 Control Frame

  RTS/CTS ACK

- Type=10 Data Frame

Frame Subtypes

MANAGEMENT

- Beacon
- Probe Request & Response
- Authentication
- Deauthentication
- Association Request & Response
- Reassociation Request & Response
- Disassociation
- Announcement Traffic Indication Message (ATIM)

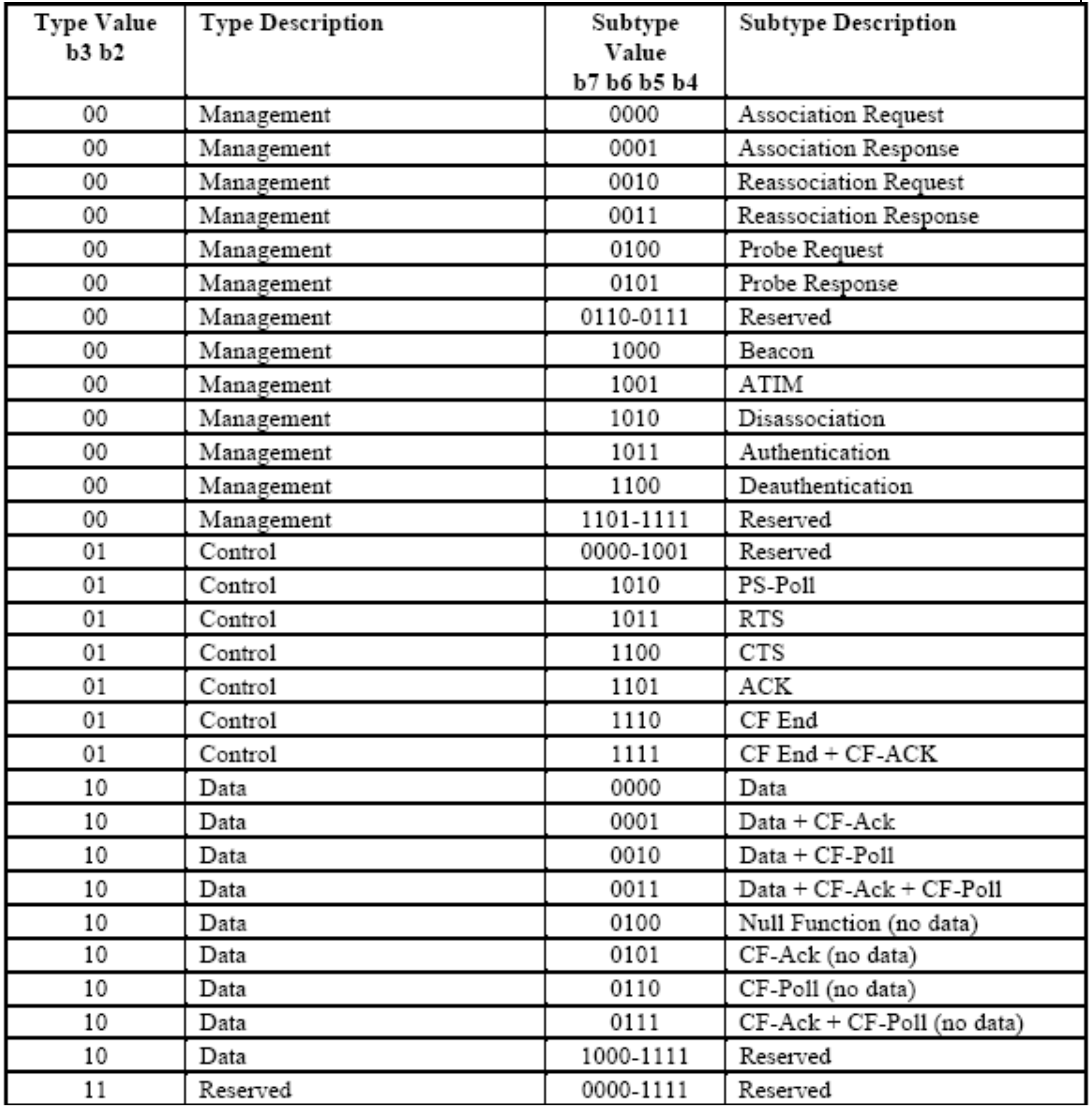
CONTROL

- RTS
- CTS
- ACK
- PS-Poll
- CF-End & CF-End ACK

DATA

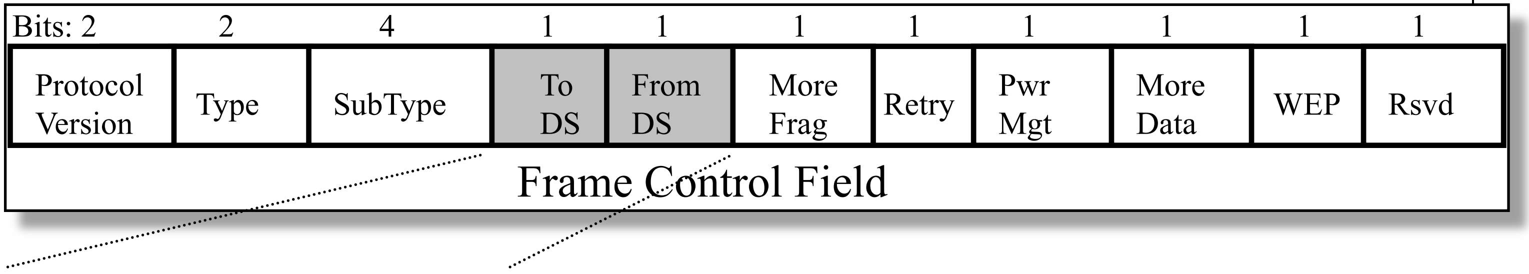
- Data
- Data+CF-ACK
- Data+CF-Poll
- Data+CF-ACK+CF-Poll
- Null Function
- CF-ACK (nodata)
- CF-Poll (nodata)
- CF-ACK+CF+Poll

Type and Subtype



Type Value b3 b2	Type Description	Subtype Value b7 b6 b5 b4	Subtype Description
00	Management	0000	Association Request
00	Management	0001	Association Response
00	Management	0010	Reassociation Request
00	Management	0011	Reassociation Response
00	Management	0100	Probe Request
00	Management	0101	Probe Response
00	Management	0110-0111	Reserved
00	Management	1000	Beacon
00	Management	1001	ATIM
00	Management	1010	Disassociation
00	Management	1011	Authentication
00	Management	1100	Deauthentication
00	Management	1101-1111	Reserved
01	Control	0000-1001	Reserved
01	Control	1010	PS-Poll
01	Control	1011	RTS
01	Control	1100	CTS
01	Control	1101	ACK
01	Control	1110	CF End
01	Control	1111	CF End + CF-ACK
10	Data	0000	Data
10	Data	0001	Data + CF-Ack
10	Data	0010	Data + CF-Poll
10	Data	0011	Data + CF-Ack + CF-Poll
10	Data	0100	Null Function (no data)
10	Data	0101	CF-Ack (no data)
10	Data	0110	CF-Poll (no data)
10	Data	0111	CF-Ack + CF-Poll (no data)
10	Data	1000-1111	Reserved
11	Reserved	0000-1111	Reserved

Address Field Description



Bits: 2	2	4	1	1	1	1	1	1	1	1
Protocol Version	Type	SubType	To DS	From DS	More Frag	Retry	Pwr Mgt	More Data	WEP	Rsvd

Frame Control Field

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	RA=DA	TA=SA	BSSID	N/A
0	1	RA=DA	TA=BSSID	SA	N/A
1	0	RA=BSSID	TA=SA	DA	N/A
1	1	RA	TA	DA	SA

- ToDS
  - = 1 when the frame is addressed to AP for forwarding to Distributed System
  - Including, Destination is in the same BSS and the AP is to relay the frame
  - Otherwise = 0
- FromDS
  - = 1 when the frame is coming from DS

Addr. 1 = All stations filter on this address.

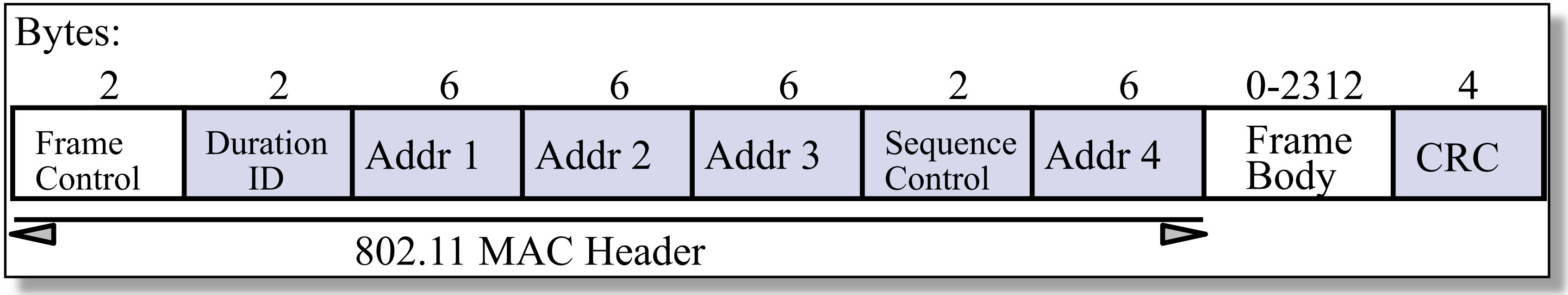
Addr. 2 = Transmitter Address (TA), Identifies transmitter to address the ACK frame to.

Addr. 3 = Dependent on *To* and *From DS* bits.

Addr. 4 = Only needed to identify the original source of WDS (*Wireless Distribution System)* frames

- More Fragments, = 1 ถ้ามี Fragment ที่เป็นข้อมูลชุดเดียวกับ Frame นี่
- Retry, = 1 เมื่อมีการ retransmit ข้อมูล Fragment ในกรณีเมื่อ Ack Packet lost ผู้รับจะทราบได้ว่า Fragment นี้ retransmits มา
- Power Management, = 1 Power management mode for the AP
- More Data, use by the station still have frame buffer in the station (in the power management mode)
- Order, = 1 indicate that the transmission is using strictly order

Frame Format



Bytes:

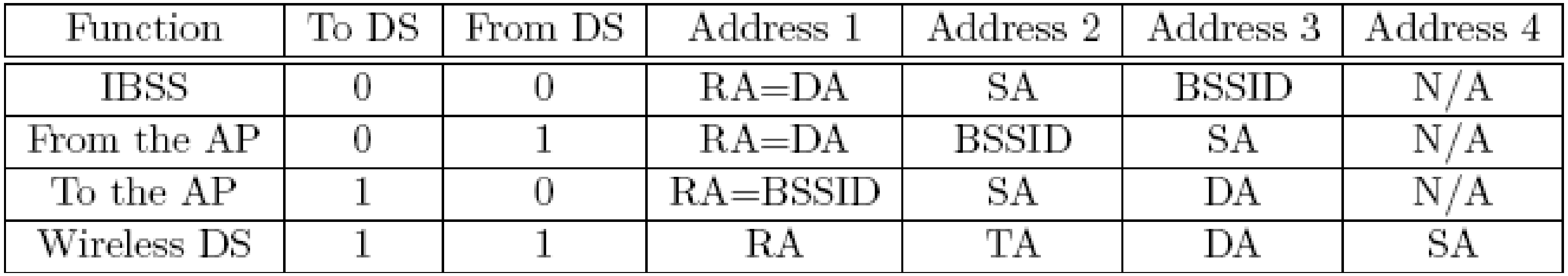
2	2	6	6	6	2	6	0-2312	4
Frame Control	Duration ID	Addr 1	Addr 2	Addr 3	Sequence Control	Addr 4	Frame Body	CRC

802.11 MAC Header

- Duration ID
  - For data frames = duration of frame (NAV Calculation).
  - For Control Frames (Power Saving Pool Message) the associated identity of the transmitting station.
- Sequence Control
  - 16bit: 4bit fragment number and 12bit sequence number. Allow receiving station to eliminate duplicate received frames

Address Fields: 4 address fields: besides 48bit address (IEEE 802.3)

- **BSS Identifier (BSSID):**
  - unique identifier for a particular BSS. In an infrastructure BSSID it is the MAC address of the AP. In IBSS, it is random and locally administered by the starting station.
- **Transmitter Address (TA):**
  - MAC address of the station that transmit the frame to the wireless medium. Always an individual address.
- **Receiver Address (RA):**
  - to which the frame is sent over wireless medium. Individual or Group.
- **Source Address (SA):**
  - MAC address of the station who originated the frame. Always individual address. May not match TA because of the indirection performed by DS of an IEEE 802.11 WLAN. SA field is considered by higher layers.
- **Destination Address (DA):**
  - Final destination . Individual or Group. May not match RA because of the indirection.



Function	To DS	From DS	Address 1	Address 2	Address 3	Address 4
IBSS	0	0	RA=DA	SA	BSSID	N/A
From the AP	0	1	RA=DA	BSSID	SA	N/A
To the AP	1	0	RA=BSSID	SA	DA	N/A
Wireless DS	1	1	RA	TA	DA	SA

- Frame Body Field:
  - contains the information specific to the particular data or management frames. Variable length.
  - As long as 2304bytes and when ecrypted 2312bytes. An application may sent 2048byte with 256 byte upper layer headers.
- Frame Check Sequence Field:
  - 32 bits; CCITT CRC-32 polynomial:
  - $G(x) = x32 + x26 + x23 + x22 + x16 + x12 + x11 + x10 + x8 + x7 + x5 + x4 + x2 + x + 1$