WiFi Basics

Yogesh M Iggalore

WiFi History

- WiFi – Wireless Fidelity
- WiFi is a wireless network protocol based on IEEE 802.11
- Invented by Australian radio-astronomer Jhon o’Sullivan in CSIRO
- More than 800 companies have WiFi certificate
- WiFi alliance is non profit organisation
- As of 2019, more than 3.05 billion WiFi enabled shipped globally.

WiFi versions

Year	IEEE	Name	Frequency(GHz)	Link rate(Mbit/s)
1997	802.11		2.4	1 to 2
1999	802.11b	WiFi1	2.4	1 to 11
1999	802.11a	WiFi2	5	6 to 54
2003	802.11g	WiFi3	2.4	6 to 54
2008	802.11n	WiFi4	2.4/5	72 to 600
2014	802.11ac	WiFi5	2.4/5	433 to 6933
2019	802.11ax	WiFi6	2.4/5	600 to 9608
2019	802.11ax	WiFi6E	6	600 to 9608

802.11a WiFi-2

- Introduced in year 1999
- Radio Frequency band 5GHz
- Maximum data rate 54 Mbps
- Typical data rate 25Mbps
- Typical range 30 meters
- Number of stream 1
- Modulation OFDM : Orthogonal frequency division multiplexing
- Channel width 20Mhz

802.11b WiFi-1

- Introduced in year 1999
- Radio Frequency band 2.4GHz
- Maximum data rate 11Mbps
- Typical data rate 5Mbps
- Typical range 30 meters
- Modulation CCK(DSSS) : complementary code keying (direct sequence spread spectrum)
- 12 non overlapping channels
- Channel width 20Mhz
- Number of stream 1

802.11g WiFi-3

- Introduced in year 2003
- Radio Frequency band 2.4GHz
- Maximum data rate 54Mbps
- Typical data rate 25Mbps
- Typical range 30 meters
- Modulation CCK(DSSS) or OFDM
- Channel width 20Mhz
- Number of stream 2

802.11n WiFi-4

- Introduced in year 2008
- Radio Frequency band 2.4GHz and 5GHz
- Maximum data rate 600Mbps
- Typical range 100 meters
- Modulation CCK(DSSS) or OFDM
- Number of streams 1,2,3 or 4
- Channel width 20MHz or 40MHz
- Backward compatibility to 802.11a, 802.11b and 802.11g
- Beam forming technique
- MIMO channels

MIMO : Multiple-Input Multiple-Output

- MIMO is a wireless technology that uses multiple transmitters and receivers to transfer more data at the same time.
- All wireless products with 802.11n support MIMO.
- The technology helps allow 802.11n to reach higher speeds.
- MIMO technology uses a natural radio-wave phenomenon called multipath.
- With multipath, transmitted information bounces off walls, ceilings, and other objects, reaching the receiving antenna multiple times at different angles and slightly different times
- An adapter with two antennas has a speed of 300 Mbps.
- A adapter with three antennas can have a speed of 600 Mbps

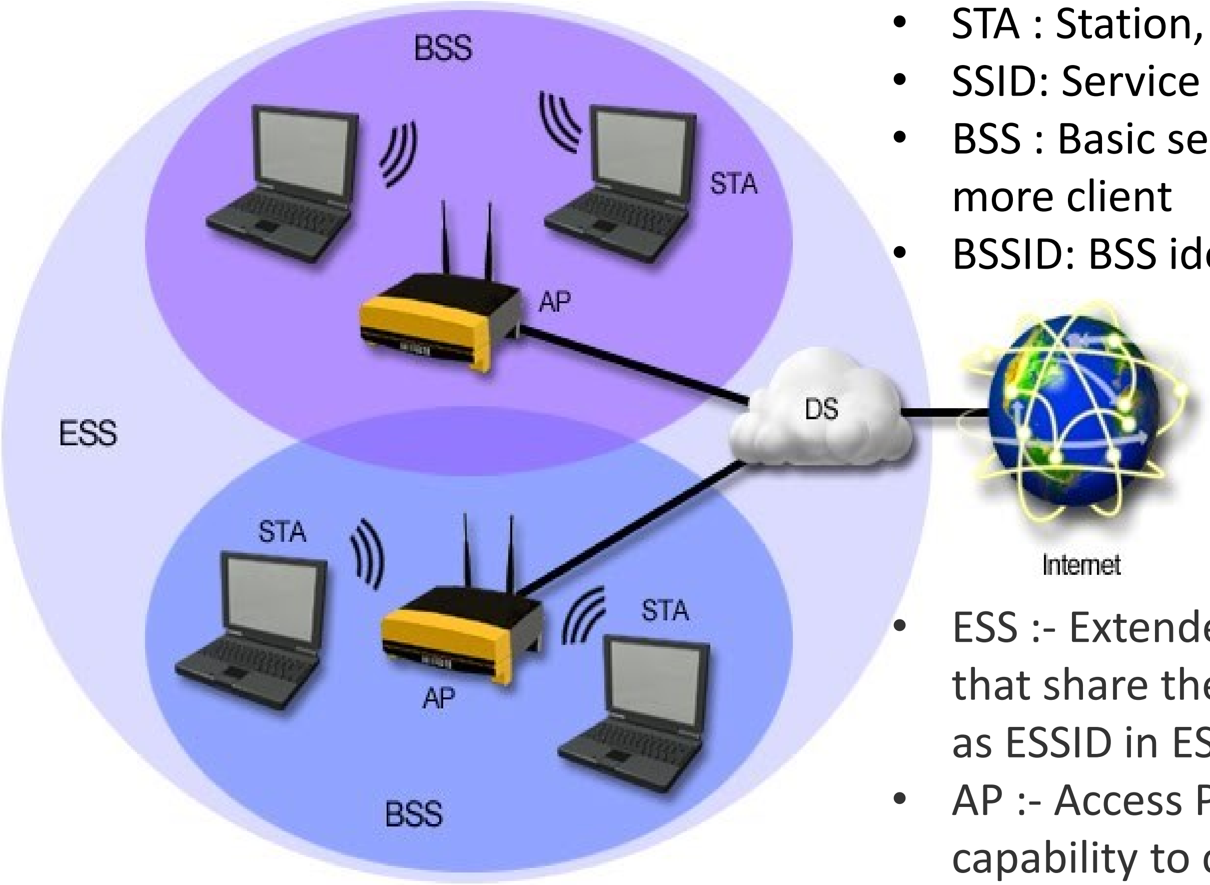
802.11ac WiFi-5

- Introduced in year 2014
- Radio Frequency band 2.4GHz and 5GHz
- Maximum data rate 6.93Gbps
- Modulation BPSK, QPSK, 16-QAM, 64-QAM and 256-QAM
- Number of streams 8
- Channel width 20,40 and 80MHz
- Backward compatibility to 802.11n
- Beam forming

802.11ax WiFi-6

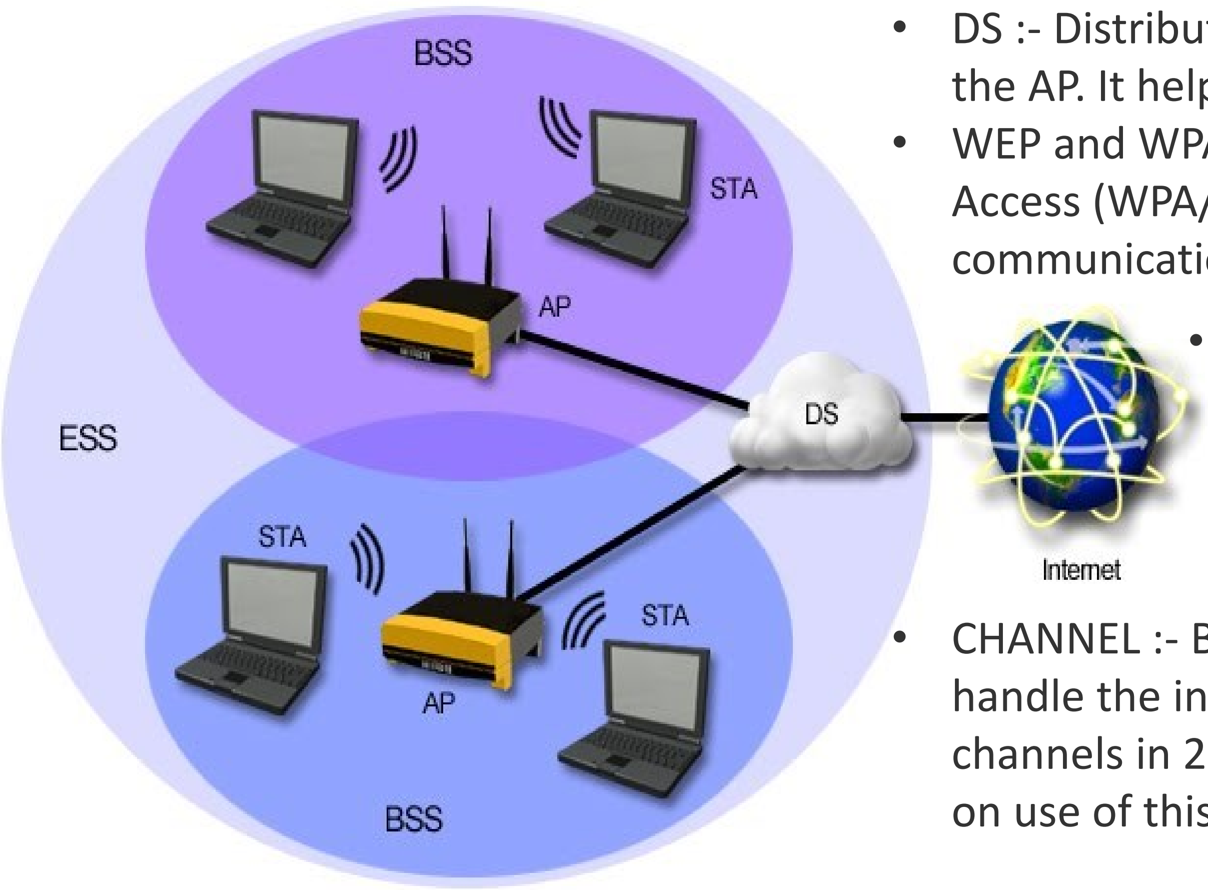
- Introduced in year 2019
- Radio Frequency band 2.4GHz and 5GHz
- Maximum data rate 14Gbps
- Modulation OFDM
- Number of streams 8
- Channel width 20,40 and 80MHz
- Backward compatibility to 802.11ac
- Beam forming
- Target wakeup time

Basic components of wireless network



- STA : Station, any device in a network is called STA or station
- SSID: Service set identifier is wireless network name, configured in AP
- BSS : Basic service set is a wireless network consist of AP supporting one or more client
- BSSID: BSS identifier unique identity each BSS in network. MAC address of AP
- IBSS :- An Independent BSS is a wireless network, consisting of at least two STAs, used where no access to a DS is available. An IBSS is also sometimes referred to as an ad hoc wireless network.
- ESS :- Extended Service Set (ESS) is two or more group of interconnected BSS that share the Same SSID. Because all BSS use the same name SSID is called as ESSID in ESS.
- AP :- Access Point (AP) is base the base station in the network. It provide the capability to connect the physical network to wireless network.

Basic components of wireless network

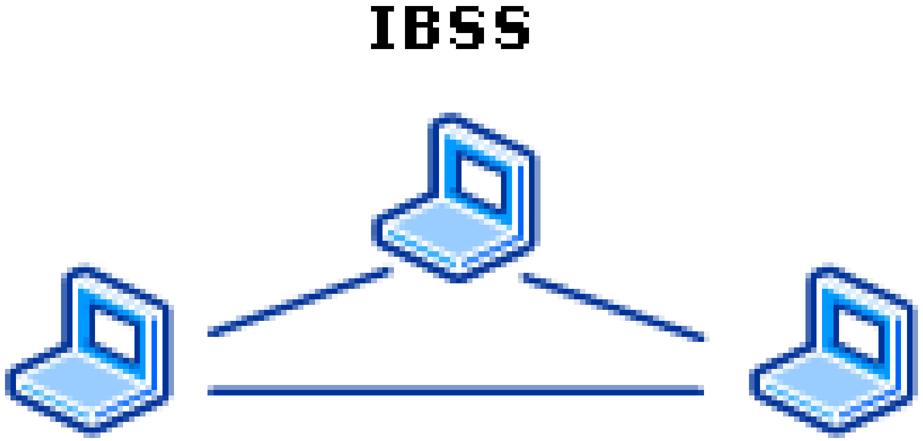


- DS :- Distribution System (DS) is the logical component used to interconnect the AP. It helps the STA to roam from one BSS to other BSS.
- WEP and WPA/WPA2 :- Wired equivalence privacy(WEP)and WiFi Protected Access (WPA/WPA2) are the security mechanism used to provide the secured communication between STA and AP
- BAND :- wireless network basically works in between 2 Band frequency that in 2.4GHZ and 5GHZ. So band is frequency in which WiFi Devices can work, it's all depend on the hardware capability of device
- CHANNEL :- Band is further divided in sub group called channel. This is used to handle the interference between the 2 wireless devices. There is around 13 channels in 2.4GHz band and 42 channels 5GHz band. There is some restriction on use of this channels which differ from country to country

Operating modes

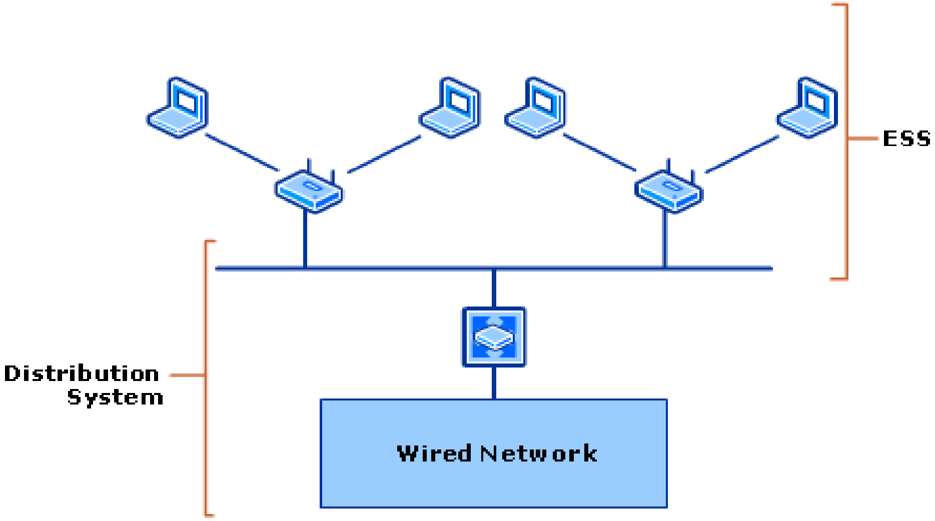
Ad-Hoc

In Ad-hoc wireless client or STA communicate with each other without any wireless AP. Ad hoc mode is also called as peer to peer mode. Wireless client in Ad hoc mode IBSS. In Ad hoc first wireless client takes some responsibility AP. This responsibility include periodic beacon and authenticating the other STA or client. But this client dose not relay the communication between 2 other clients.



Infrastructure

In infrastructure mode there is at least one AP and one wireless client present. Wireless client use the wireless AP to access the resource on traditional wired network.

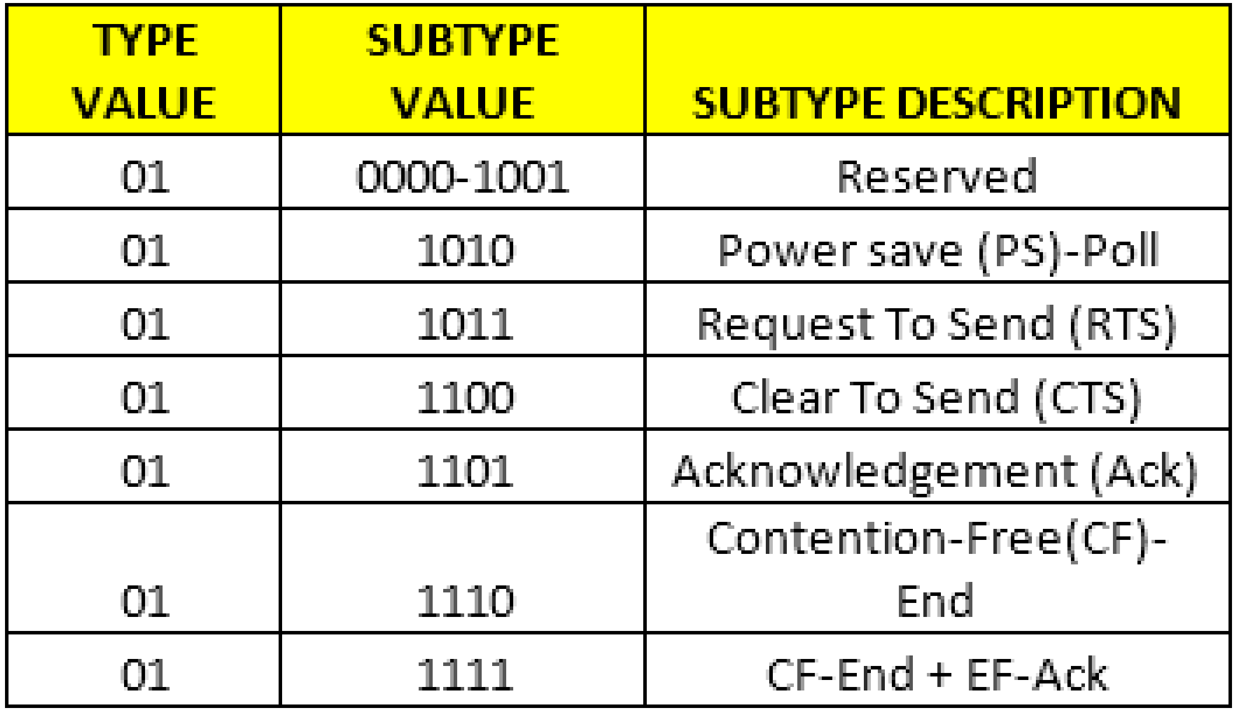


Protocol

- 802.11 uses data link and physical layer of OSI model
- 802.11 works at 2.4GHz, 5GHz, 6GHz, 900MHz(802.11ah) and 60GHz(802.11ai)
- 14 channel with 20MHz bandwidth
- 5MHz channel spacing

WiFi MAC Frame

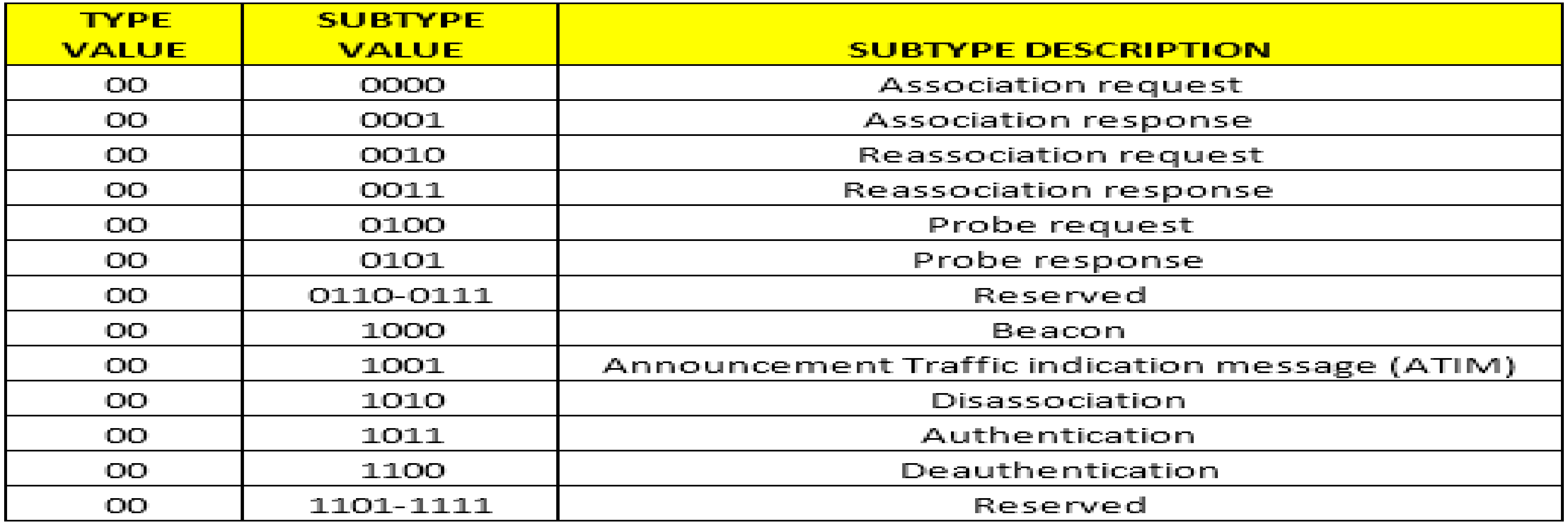
Control :- Control frame is basically used for RTS(Request to send), CTS(Clear to send),PS (Power save Poll), ACK (Acknowledgement) control frame assist the reliability of data.



TYPE VALUE	SUBTYPE VALUE	SUBTYPE DESCRIPTION
01	0000-1001	Reserved
01	1010	Power save (PS)-Poll
01	1011	Request To Send (RTS)
01	1100	Clear To Send (CTS)
01	1101	Acknowledgement (Ack)
01	1110	Contention-Free(CF)-End
01	1111	CF-End + EF-Ack

WiFi MAC Frame

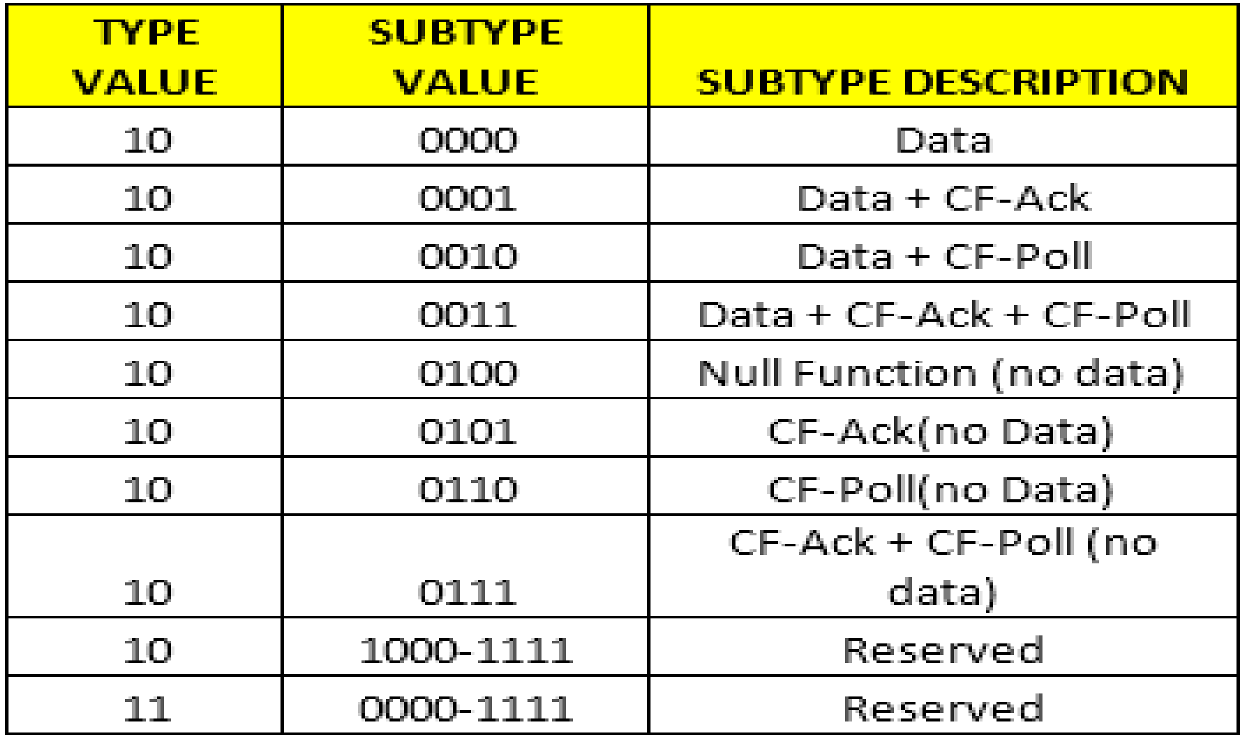
Management :- Actual work of management frame is for transmitting the Beacon, probe for request and response, authentication and De-authentication, Association request and response, disassociation, Re-association request and response .



TYPE VALUE	SUBTYPE VALUE	SUBTYPE DESCRIPTION
00	0000	Association request
00	0001	Association response
00	0010	Reassociation request
00	0011	Reassociation response
00	0100	Probe request
00	0101	Probe response
00	0110-0111	Reserved
00	1000	Beacon
00	1001	Announcement Traffic indication message (ATIM)
00	1010	Disassociation
00	1011	Authentication
00	1100	Deauthentication
00	1101-1111	Reserved

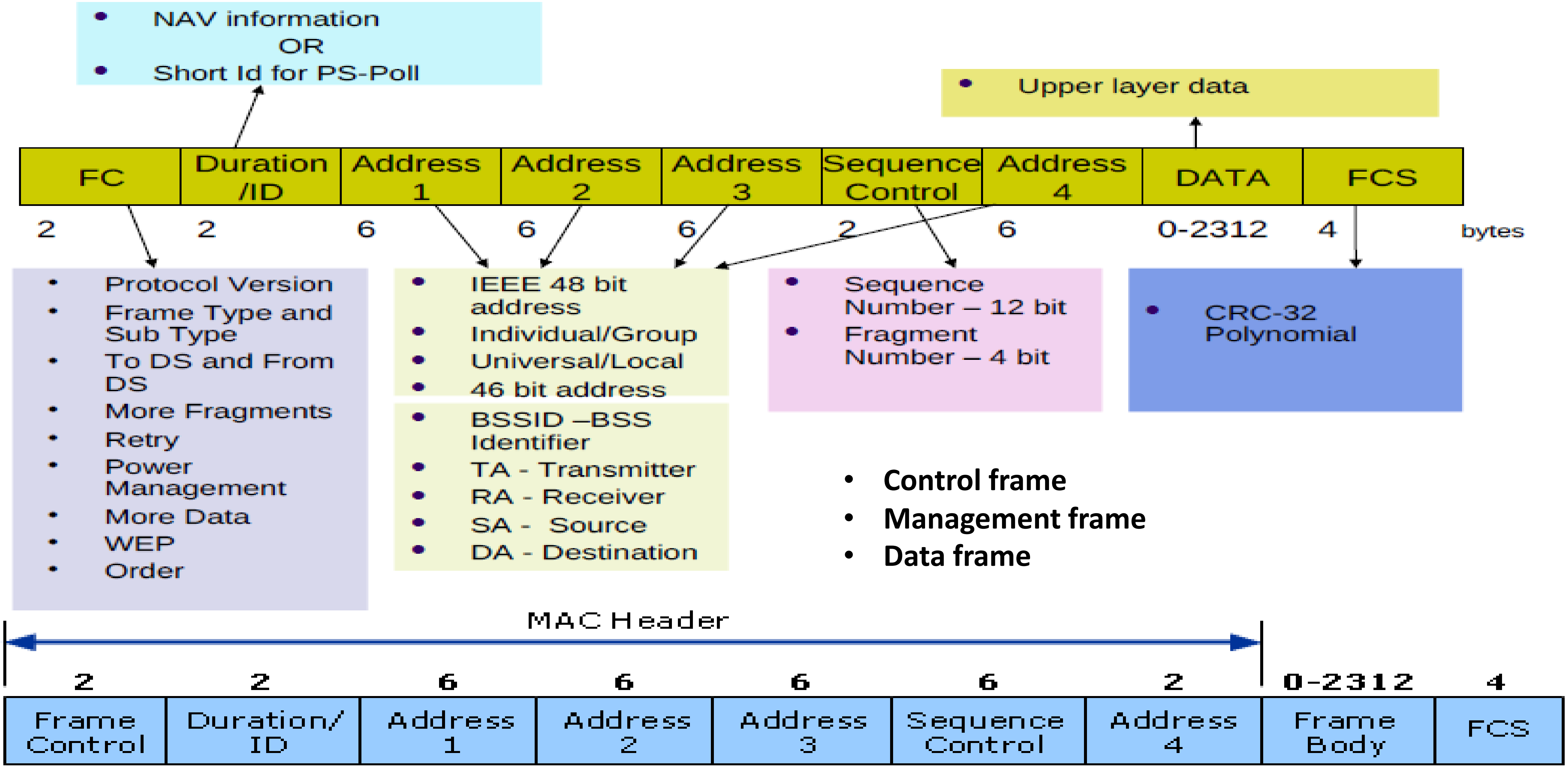
WiFi MAC Frame

Data :- Data frame is used to carry the data.



TYPE VALUE	SUBTYPE VALUE	SUBTYPE DESCRIPTION
10	0000	Data
10	0001	Data + CF-Ack
10	0010	Data + CF-Poll
10	0011	Data + CF-Ack + CF-Poll
10	0100	Null Function (no data)
10	0101	CF-Ack(no Data)
10	0110	CF-Poll(no Data)
10	0111	CF-Ack + CF-Poll (no data)
10	1000-1111	Reserved
11	0000-1111	Reserved

802.11 MAC Frame



- NAV information
  OR
- Short Id for PS-Poll

- Upper layer data

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

- Sequence Number – 12 bit
- Fragment Number – 4 bit

- CRC-32 Polynomial

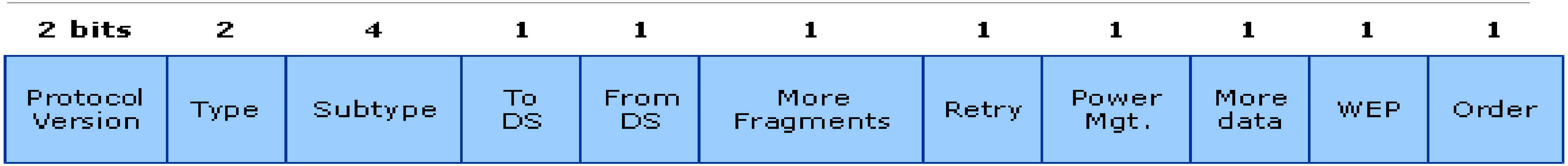
- **Control frame**
- **Management frame**
- **Data frame**

MAC Header

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

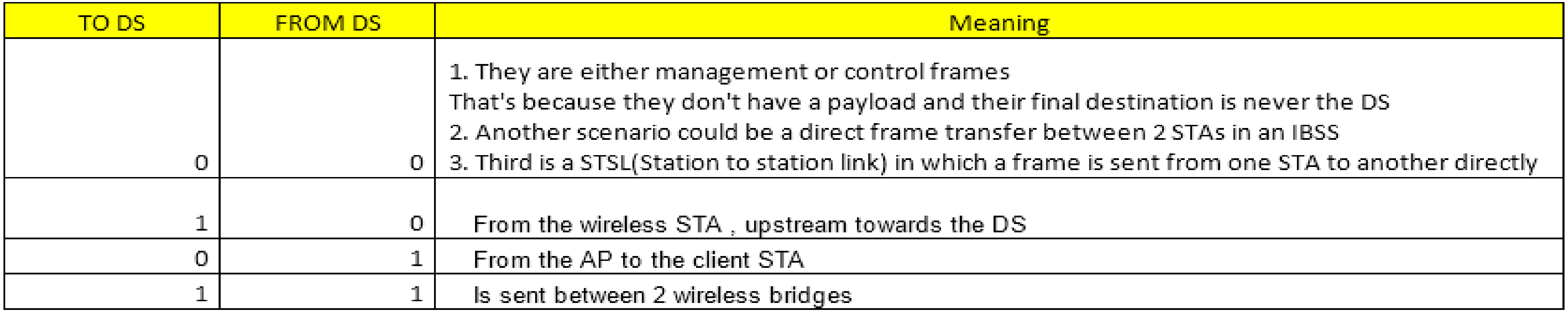
WiFi MAC Frame

Frame Control :- Made up of 2 Bytes, contain following fields.



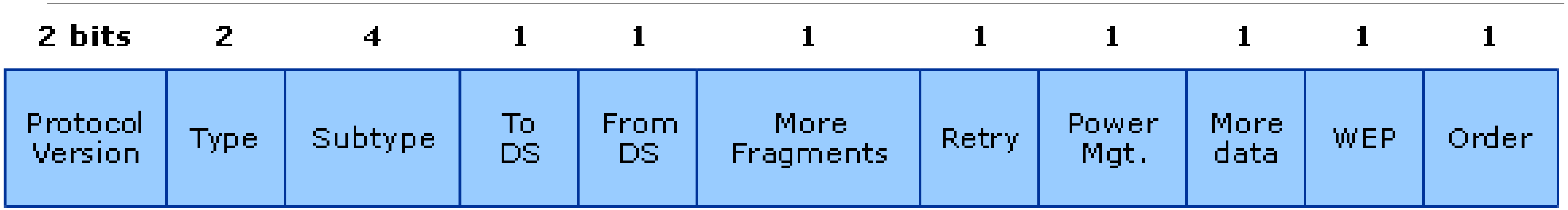
2 bits	2	4	1	1	1	1	1	1	1	1
Protocol Version	Type	Subtype	To DS	From DS	More Fragments	Retry	Power Mgt.	More data	WEP	Order

- Protocol version : – By default value is 0. Used to represent 802.11.
- Type :- used to represent type of frame Control (01), Management (00), Data (10).
- Subtype :- used to represent subtype of frame.
- TO DS and FROM DS :- This Indicates the direction of the flow. There are 4 values.



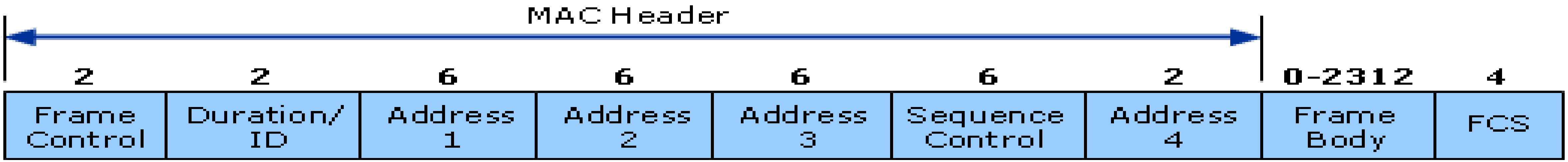
TO DS	FROM DS	Meaning
0	0	1. They are either management or control frames That's because they don't have a payload and their final destination is never the DS 2. Another scenario could be a direct frame transfer between 2 STAs in an IBSS 3. Third is a STSL(Station to station link) in which a frame is sent from one STA to another directly
1	0	From the wireless STA , upstream towards the DS
0	1	From the AP to the client STA
1	1	Is sent between 2 wireless bridges

WiFi MAC Frame



2 bits	2	4	1	1	1	1	1	1	1	1
Protocol Version	Type	Subtype	To DS	From DS	More Fragments	Retry	Power Mgt.	More data	WEP	Order

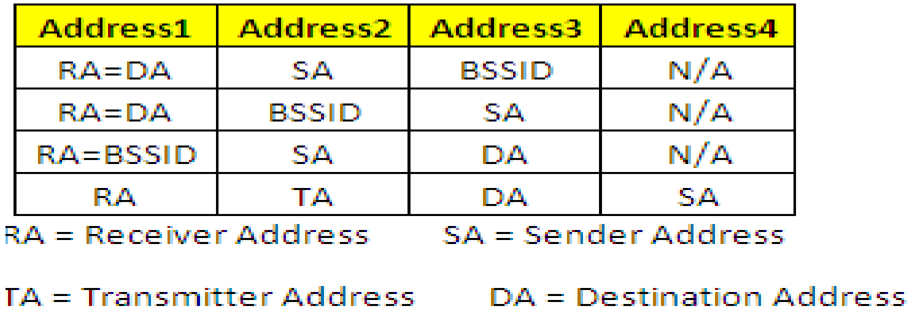
- More Fragments:- Present in management frame. Indicates fragments.
- Retry :- 0 represent original transmission, 1 represent retransmission.
- Power Mgt :- 1 Represent STA is using power save Mode. AP the buffer the data meant to send to STA
- More Data :- When the client receives a frame with the more data field when it’s awake, it knows that it cannot go to sleep and it sends out a PS-POLL message for getting that data
- WEP or protected frame :- indicates whether or not encryption and authentication are used in the frame. It can be set for all data frames and management frames, which have the subtype set to authentication.
- Order :- indicates that all received data frames must be processed in order.



MAC Header

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

- **Duration/ID**:- it used define the transmission time.
- **Address 1, Address 2, Address 3 and Address 4**:- the value of 4 address field is depend on the frame type



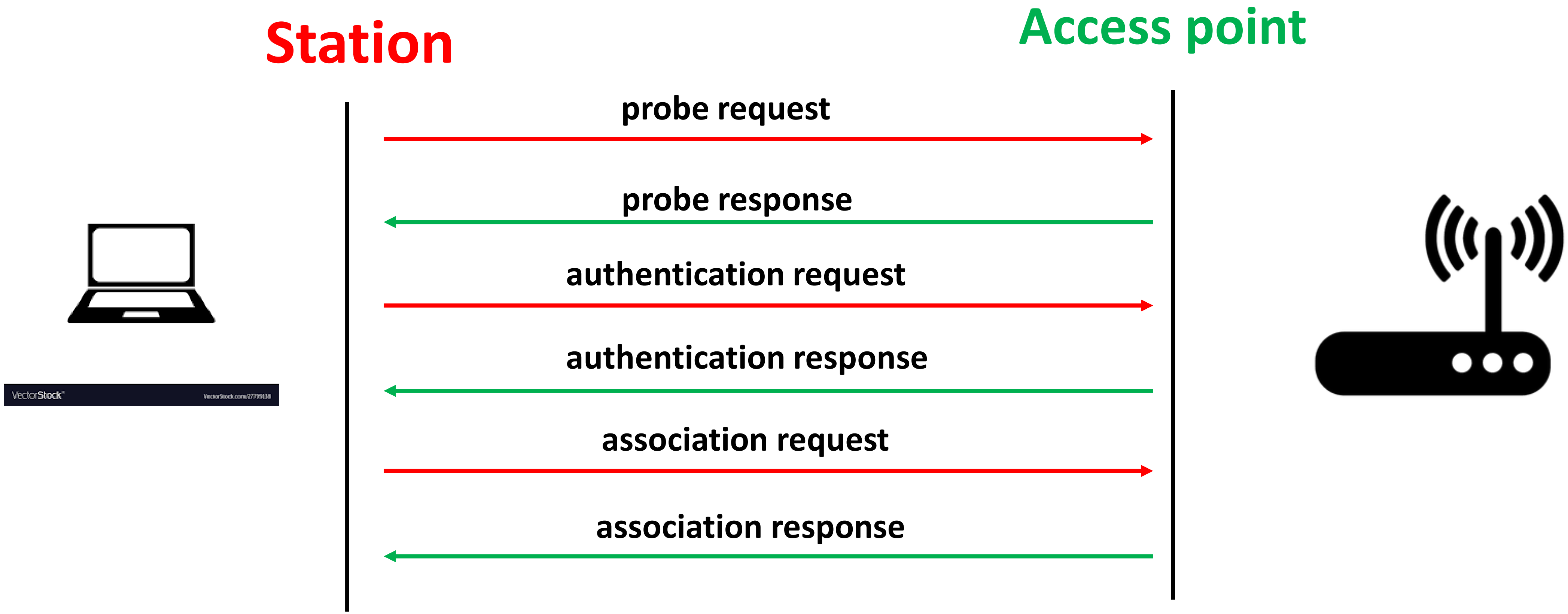
Address1	Address2	Address3	Address4
RA=DA	SA	BSSID	N/A
RA=DA	BSSID	SA	N/A
RA=BSSID	SA	DA	N/A
RA	TA	DA	SA

RA = Receiver Address SA = Sender Address

TA = Transmitter Address DA = Destination Address

- **Sequence Control** :- indicates the sequence number of each frame. The sequence number is the same for each frame sent for a fragmented frame; otherwise, the number is incremented by one until reaching 4095, when it then begins at zero again.
- **Frame Body** :- Actual data
- **FCS** :- 32 bit CRC Check

Packet exchange between Station and Access point



Station

Access point

probe request

probe response

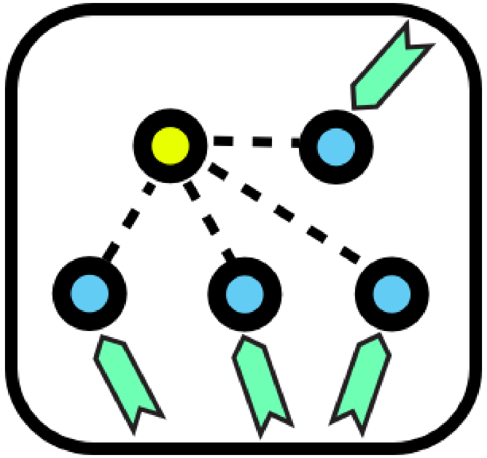
authentication request

authentication response

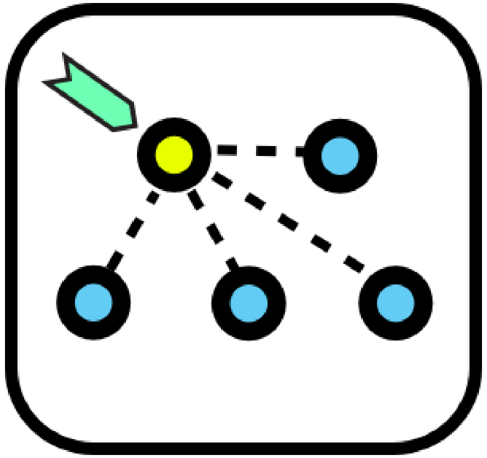
association request

association response

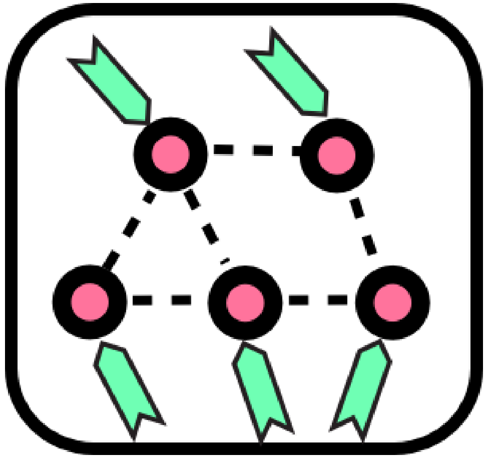
WiFi modes



Station mode



Access point mode



Ad-Hoc mode

WiFi Security

Wired Equivalent Privacy (WEP)

- Most used WiFi security protocol
- Introduced in year 1997, security algorithm to provide data confidentiality for wireless network
- It uses two key Unicast session key and Multicast session key
- In WEP-40, a 40 bit WEP key is concatenated with a 24 bit initialization vector, to generate a 64 bit RC4 key.
- In WEP-104, a 104 bit WEP key is concatenated with the 24 bit initialization vector, to generate a 128 bit RC4 key.
- WEP operates at the data link and physical layer.

Wi-Fi Protected Access(WPA)

- This security introduced in 802.11i
- Uses temporal key integrity protocol (pre packet mixing, integrity checking and extending rekeying)
- Most secured wifi protocol as of now