IEEE 802.11 Family of Standards

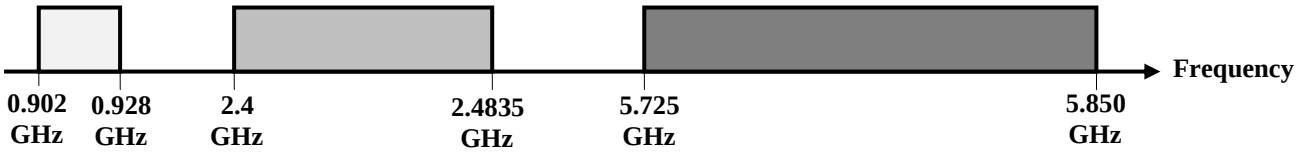
There is no single 802.11x standard. The term IEEE 802.11 is also used to refer to the original 802.11, which is now sometimes called "802.11 legacy". The followings are the most important IEEE 802.11 standards.

1- IEEE 802.11 legacy:

The original version of the standard IEEE 802.11 released in 1997 specifies two raw data rates of 1 and 2 Mbps to be transmitted via IR (using a wavelength range from 850 to 950 nm) or by either FHSS or DSSS at 2.4GHz of the Industrial Scientific Medical (ISM) bands. Legacy 802.11 was rapidly supplemented (and popularized) by IEEE 802.11b.

Note: In 1985, the Federal Communications Commission (FCC) in the United States defines the ISM bands to be used by unlicensed devices.

ISM Frequency bands



The 2.4 GHz band is available globally while the other two bands are unlicensed only in USA.

2- IEEE 802.11a

The 802.11a amendment to the original standard was ratified in 1999. The 802.11a standard uses the same core protocol as the original standard, operates in 5.725 GHz band, OFDM with a maximum data rate of 54 Mbps.

Since the 2.4 GHz band is heavily used, using the 5.725 GHz band gives 802.11a the advantage of less interference. However, this high carrier frequency also brings disadvantages. It restricts the use of 802.11a to almost line of sight, necessitating the use of more access points; it also means that 802.11a cannot penetrate as far as 802.11b since it is absorbed more readily.

Because IEEE 802.11b (released on the same year) was already widely adopted. And due its disadvantages including the restrictions of range and regulations, IEEE 802.11a was not widely adopted.

3- IEEE 802.11b

The 802.11b amendment to the original standard was ratified in 1999. IEEE 802.11b has a maximum data rate of 11 Mbps.

802.11b products appeared on the market very quickly, since 802.11b is a direct extension of the DSSS defined in the original standard.

802.11b cards can operate at 11 Mbps, but they can also operate at 5.5, 2, and 1 Mbps.

4- IEEE 802.11g

In June 2003, a third modulation standard was ratified: 802.11g. This standard works in the 2.4 GHz band (like 802.11b) but operates at a maximum raw data rate of 54 Mbps. 802.11g hardware work with 802.11b hardware.

The modulation scheme used in 802.11g is OFDM for the data rates of 6, 9, 12, 18, 24, 36, 48, and 54 Mbps, and DSSS for 11, 5.5, 2, and 1Mbit/s

Note: IEEE 802.11b, IEEE 802.11g use the 2.4 GHz range of the (ISM) band. Because of this choice, 802.11b and 802.11g equipment can incur interference from microwave ovens, cordless telephones, Bluetooth devices, and other appliances using this same band. The 802.11a standard uses the 5 GHz band, and is therefore not affected by products operating on the 2.4 GHz band.

5- IEEE 802.11n

IEEE 802.11n ratified in 2009 is a huge step forward for the standard and is a major improvement in almost every aspect of Wi-Fi. The current 802.11n products that are available today offer a variety of data rates up to 300 Mbps and ultimately will support up to 600 Mbps. In addition, 802.11n offers excellent backwards compatibility with previous versions of the standard. Higher SNR is offered by 802.11n devices and better coverage as compared to the previous versions of the standard. IEEE 802.11n achieves these enhancements mainly due to one or more of the followings:-

1. Transmit beamforming: IEEE 802.11n depends MIMO (Multiple Input Multiple Output), the utilization of this technology allows 802.11n to make use of transmit beamforming by which the signal sent by each

transmitting antenna can be coordinated so that the signal at the receiver is dramatically improved. This adjustment can be achieved via a feedback signal from the receiver to the transmitter. So, it is clear that transmit beamforming is not useful in multicast or broadcast situations.

2. MRC (Maximum Ratio combining): Again due to MIMO; 802.11n devices can make use of multipath by using MRC technique. MRC enables the receiver to correlate the signal reception from multiple antennas so that the aggregated signal is strongest and most consistent than any of the signals at each receiving antenna.
3. Channel bonding: The bandwidth of a radio channel is an important factor to decide the radio efficiency. Radio efficiency is usually expressed by the spectral efficiency which is a measurement of how many bits the radio can transmit per Hertz. Old IEEE 802.11 standards utilize a 20MHz bandwidth for each channel (as an example this channel Bandwidth gives a spectral efficiency of 0.55 bits per Hz at 11Mbps). While the new 802.11n can still use the same 20MHz channels, it can use two adjacent 20 MHz channels at the same time. This called channel bonding which gives a simple way to approximately double the data rate.
4. Overhead reduction: Overhead consumes time in the transmission of headers, footers, interframe spaces and control and management frames. IEEE 802.11n can reduce overhead via one or more of the followings:
    a) Frame aggregation: 802.11n introduces frame aggregation by which two or more frames are put together into a single transmission.
    b) Block acknowledgement: here a single ACK frame can be returned by the recipient to confirm the reception of number of individual constituting frames instead of using an ACK frame for each received frame.
    c) Reducing inter frame spaces: this cuts down the dead time between frames which increasing the amount of time in transmit opportunity that is occupied by sending frames.

Standard	Release Date	Op. Freq. band (GHz)	Channel bandwidth (MHz)	Allowed MIMO Streams	Transfer rates (Mbps)	Digital Bandwidth (Mbps)	Signaling Scheme
IEEE 802.11	1997	2.4	20	1	1,2	2	FHSS
							DSSS
		Infrared	20	1	1,2	2	
IEEE 802.11a	1999	5.725	20	1	6,9,12,18, 24,36,48,54	54	OFDM
IEEE 802.11b	1999	2.4	20	1	1,2,5.5,11	11	DSSS
IEEE 802.11g	2003	2.4	20	1	1,2,5.5,11	54	DSSS
					6,9,12,18, 24,36,48,54		OFDM
IEEE 802.11n	2009	2.4 , 5.725	20	4	7.2,14.4,21.7,28.9, 43.3,57.8,65,72.2	300	OFDM
			40	4	15,30,45,60,90,120, 135,150	600	

Frame Format

IEEE 802.11 standards define three types of frames. These types are:

1. Data.
2. Management.
3. Control.

The format of data frame used in the IEEE 802.11 standards is

2 B	2 B	6 B	6 B	6 B	2B	6 B	0-2312 B	4 B
Frame Control	Duration	Address 1	Address 2	Address 3	Seq	Address 4	Frame body	FCS

- **Frame control:** it is one of the most important fields in the IEEE 802.11 frame, it consists of several subfields as illustrated bellow:

2b	2b	4b	1b	1b	1b	1b	1b	1b	1b	1b
Version	Type	subtype	To DS	From DS	More Frag	Retry	Pwr Mgt	More data	WEP	Rsvd

Field	*Explanation*
Version	**Current version is 0**
Type	**Type of information: management (00), control (01), or data (10)**
Subtype	**Subtype of each type**
To DS	**Regarded to addressing (Defined later in this lecture)**
From DS	**Regarded to addressing (Defined later in this lecture)**
More Frag	**Set to "1" for more fragments**
Retry	**Set to "1" in retransmitted frames**
Pwr mgt	**Set to "1" when station in power management mode**
More data	**Set to "1" where the station has other frames to send**
WEP	**Wired Equivalent Privacy (for encryption)**
Rsvd	**Reserved for future use**

- **Duration:** indicate the time (in microseconds) the channel will be allocated for successful transmission of layer2 PDU.
- **Address fields (1-4)**: contains up to four 6-byte addresses. The usage of each address field is dependant on the "To DS" and "From DS" subfields in the frame control field.
- **Sequence Control:** consists of fragment number and sequence number. It is used to represent the order of different fragments belonging to the same frame.
- **Frame body:** depending on the frame type and subtype, this field contains data or management information.
- **FCS (Frame Check Sequence)**: contains a 32-bit Cyclic Redundancy Check (utilizes CRC-32).

MAC Mechanism (CSMA/CA)

Like all of the protocols developed by the IEEE 802 working groups, IEEE 802.11 splits the data-link layer into two sublayers, LLC and MAC.

IEEE 802.11 uses a MAC mechanism called Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA).

Carrier Sense

CSMA/CA is similar to CSMA/CD in that computers listen to the network to see if it is in use before they send their data, and if the network is free, the transmission proceeds.

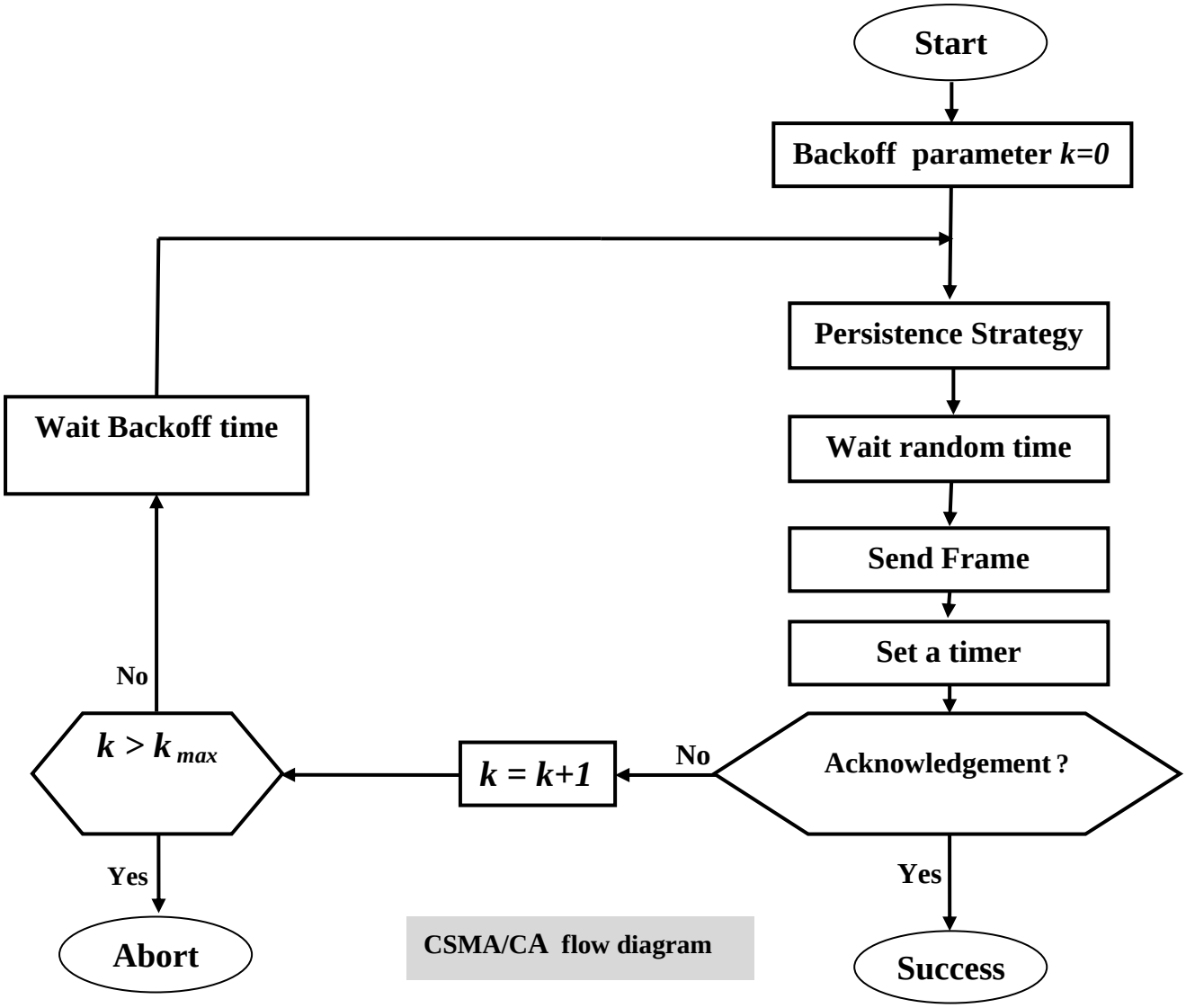
Multiple Access

like CSMA/CD, because all of the stations on the network are contending for access to the same network medium, this phase is called the multiple access phase.

Collision Avoidance:

Also like CSMA/CD, two computers can transmit at the same time on a CSMA/CA network, causing a collision. The difference between the two MAC mechanisms is that in a wireless environment, the CSMA/CD collision detection mechanism would be impractical, because it would require full-duplex communications. A computer on a twisted-pair Ethernet network assumes that a collision has occurred when an incoming signal arrives over its receive wire pair while it's sending data over the transmit wire pair.

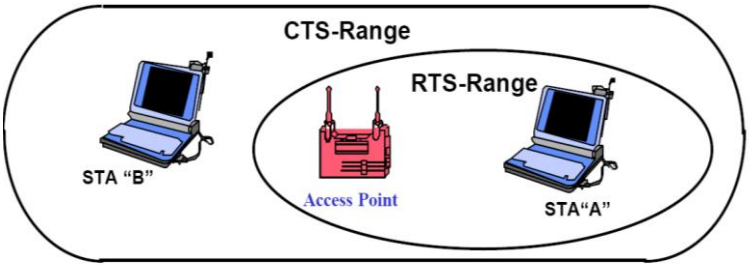
Instead of detecting collisions as they occur, the receiving computer on a CSMA/CA network performs a CRC check on the incoming packets and, if no errors are detected, transmits an acknowledgment message to the sender. This acknowledgment serves as an indication that no collision has occurred. If the sender does not receive an acknowledgment for a particular packet, it automatically retransmits it until it either receives an acknowledgment or times out. If the sender still doesn't receive an acknowledgment after a specific number of retransmissions, it overcomes that effort and leaves the error correction process to the protocols at the upper layers of the networking stack.



CSMA/CA flow diagram

Hidden Nodes Problem:

The method described above relies on the Physical Carrier Sense. The underlying assumption is that every station can "hear" all other stations. This is not always the case. Referring to the following figure, the AP is within range of the STA-A, but STA-B is out of range. STA-B would not be able to detect transmissions from STA-A, and the probability of collision is greatly increased. This is known as the Hidden Node.



To overcome this problem, another access methods are used.

- **DCF (Distribution Coordination Function)**
- **PCF (Point Coordination Function)**

DCF

DCF implies a Virtual Carrier Sense instead of the physical carrier sense. DCF is a contention-based access method. It is optional in infrastructure WLANs while it is the only access method in ad hoc WLANs. DCF is based upon the traditional CSMA/CA but with the use of process known "hand shaking".

DCF defines two types of IFS (Inter Frame Space), these are:

- **SIFS (Short Inter Frame Space) used in high priority situations**
- **DIFS(DCF Inter Frame Space) used in other situations.**

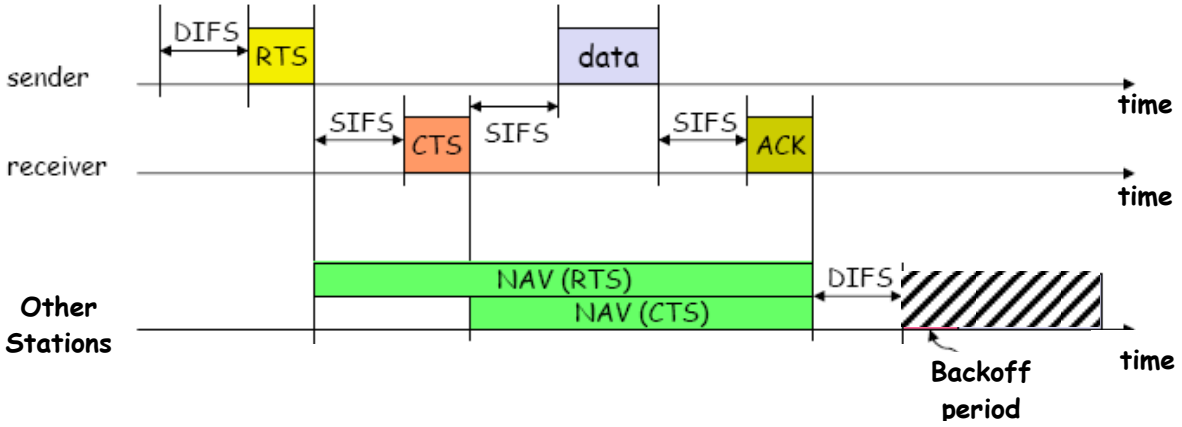
Hand Shaking:

In this process two control frames (RTS and CTS) are exchanged between two communicating wireless nodes before the transmission of data frames. For the previous example where STA-A wants to sends its data to STA-B in an infrastructure WLAN, hand shaking and data transmission process can be explained as follows:-

1. STA-A senses the medium, it waits an idle medium to send, then it waits a DIFS to send an RTS frame to the Access Point. The RTS frame contains a duration field which specifies the period of time for which the medium is reserved for a subsequent transmission. The reservation information is stored in the Network Allocation Vector (NAV) which is reservation parameter that determines amount of time the sender needs the medium.
2. Upon receipt of the RTS, the AP responds with a CTS frame. The CTS gives the green light to STA-A (the requester) to send its data. The CTS frame also contains a duration field specifying the period of time for which the medium is reserved, so when it is received by other stations, they must wait at lest the duration specified in the NAV before trying to sense the medium again. It

should be noticed that, while STA-B did not detect the RTS, it will detect the CTS and update its NAV accordingly. Thus, collision is avoided even though some nodes are hidden from other stations.

3. After receiving the CTS frame, STA-A waits an SIFS to send its data frame(s).
4. To verify that no collision has been occurred, STA-A waits an ACK frame form the Access Point after SIFS.



In the process described above, three subtypes of control frames are used ; Request To Send (RTS), the Clear To Send (CTS), and the Acknowledgment (ACK) frames,

the format of RTS frame is

2 B	2 B	6 B	6 B	4 B
Frame Control	Duration	Address 1	Address 2	FCS

While the format of CTS and ACK frames is

2 B	2 B	6 B	4 B
Frame Control	Duration	Address 1	FCS

PCF:

It is an optional access method implemented only in infrastructure WLANs. It is used for time sensitive transmission. PCF is centralized contention-free access method. Here a defined set of stations are polled by the Access Point to see if the stations have any data to send. Polling is done by a special software installed in the access point called Point Coordinator (PC).

PCF defines two types of IFSs. PIFS (PCF IFS) and SIFS. PIFS is shorter than DIFS. This gives the priority to an Access Point using PCF over a station tries to access the media using DCF.

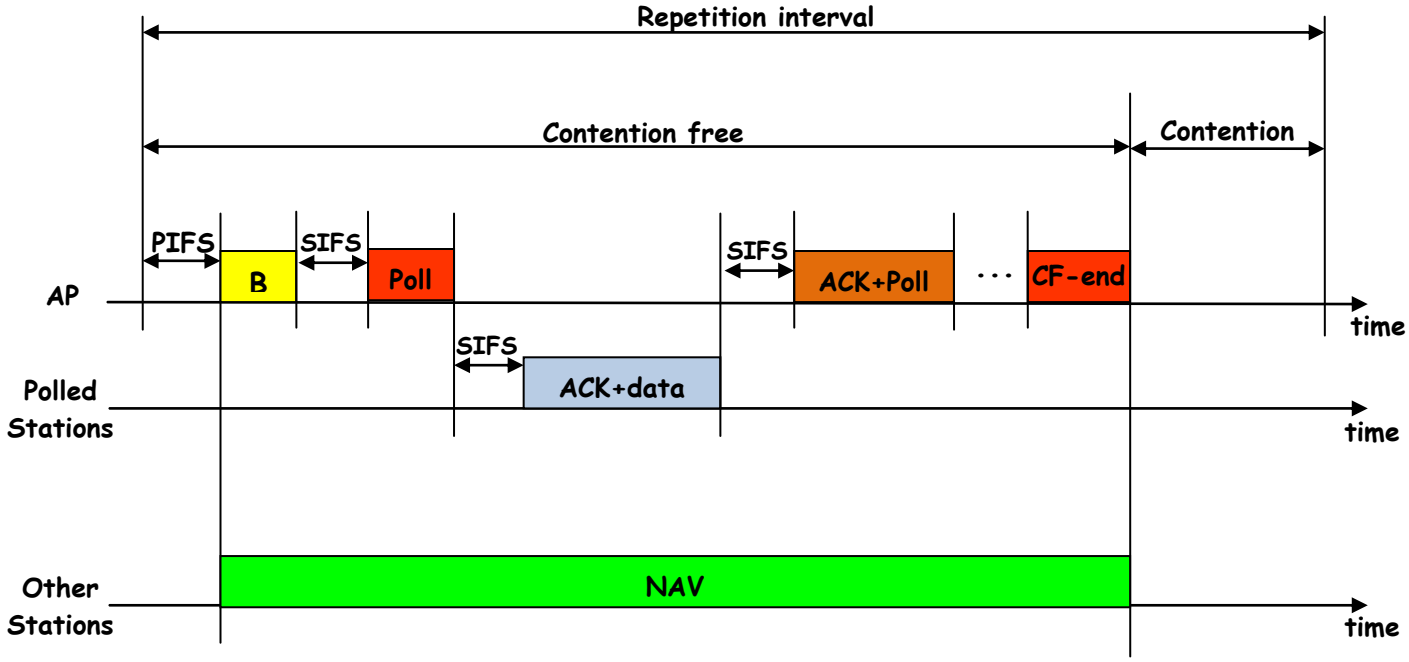
Repetition Interval:

Due to the priority of PCF over DCF; stations that only use DCF may not gain access to the medium. To prevent this situation; a repetition interval has been designed to cover both contention-free (PCF) and contention-based (DCF).

Repetition interval repeated continuously, starts with a special frame sent by the Access Point called "beacon" frame. Beacon frame contains a duration field that sets the NAV of stations receive that frame to the period of the contention-free interval.

After sending the beacon frame, the Access Point sends a "poll" frame to the destination station , receive data, receive an ACK, send an ACK or any combination of these. The Access Point then starts with other polled station and so on.

The contention-free interval ends by a CF-end (Contention Free end) frame sent by the Access Point. It is now the time to start the contention based DCF process.



Addressing:

According to the values of the "To DS" and "from DS" subfields in the "frame control" field , IEEE 802.11 addressing mechanism specify four cases:

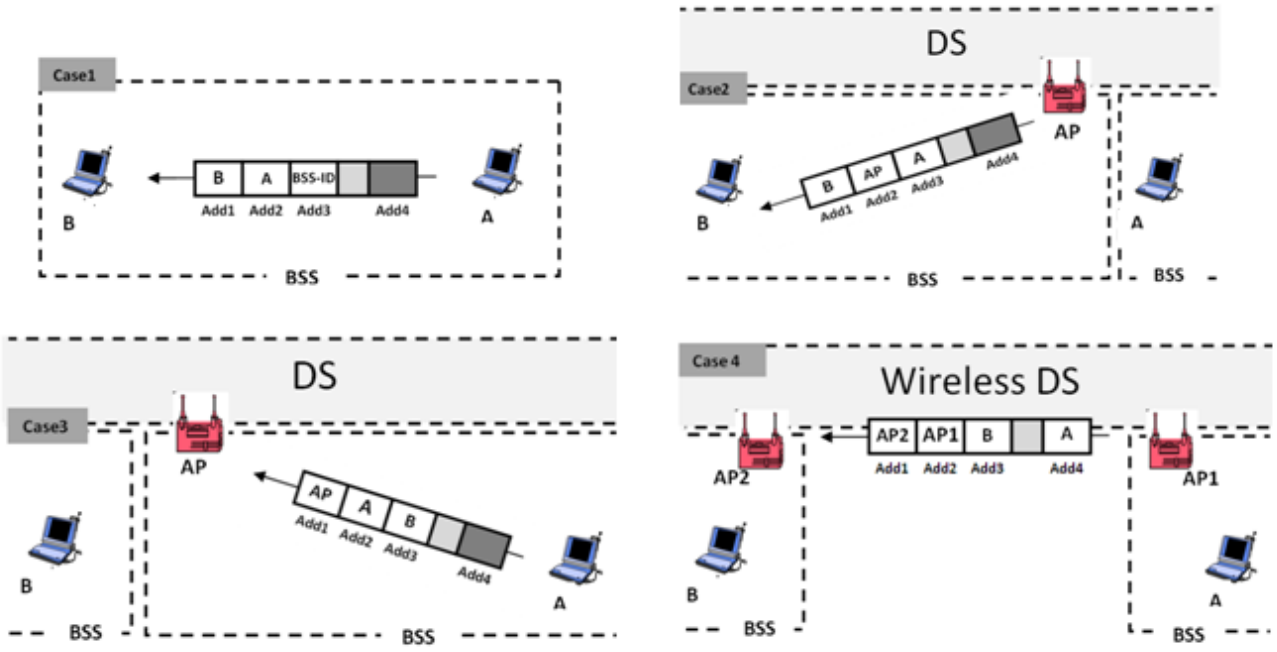
Case	To DS	From DS	Address 1	Address 2	Address 3	Address 4
1	0	0	Destination	Source	BSS ID	N/A
2	0	1	Destination	Sending AP	Source	N/A
3	1	0	Receiving AP	Source	Destination	N/A
4	1	1	Receiving AP	Sending AP	Destination	Source

- Case 1 (00): The frame is going from one station in a BSS to another without passing through the distribution system. The ACK frame should be sent to the original sender.

- Case 2 (01): The frame is coming from an AP and going to a station. The ACK should be sent to the AP. Note that address 3 contains the original sender of the frame (in another BSS).

- Case 3 (10): The frame is going from a station to an AP. The ACK is sent to the original station. Note that address 3 contains the final destination of the frame (in another BSS).

- Case 4 (11): This is the case in which the distribution system is also wireless. The frame is going from one AP to another AP in a wireless distribution system. We do not need to define addresses if the distribution system is a wired LAN because the frame in these cases has the format of a wired LAN frame (Ethernet, for example). Here, we need four addresses to define the original sender, the final destination, and two intermediate APs.



Management Frames:-

Management frames are divided into several subtypes extinguished by the value of the "subtype" in the "frame control" field of the frame. The most important subtypes of management frames are:

1. Association: used by a station to associate itself with an access point.
2. Beaconing: used by an access point periodically to scan if any station needs association.
3. Reassociation: used by a station to associate itself with a new access point when it moves to new BSS.
4. Disassociation: used by an access point or a station to terminate association.

Laith Wajeeh