Answers for Session 3a - Basic AP Management and Control Functions

1.Can we see ack for management frames?

According to 802.11 any directed message (unicast message) needs to have an acknowledgment.
It doesn't matter which frame it is, any frame having not having multicast / broadcast address as the destination address will get a acknowledgement

One of the Example is directed probe requests, at times the probe requests are directed, if there is not acknowledgment either a new frame is sent/ the frame is retried

2. If there is no ack for management frames then how does the sender know that frame is received by the receiver or not?

There is acknowledgment for all unicast frames, apart from what frame it is.. It can be management frames, control frames or anything.

1. **Sequence Numbers:** Some management frames carry sequence numbers, which allow the sender to track the progress of the management exchange and detect if any frames have been lost or received out of order. This is particularly useful for multi-stage management exchanges, where the sender needs to ensure that all frames have been received and processed in the correct order.

3. **Can we see the retry flag enabled for management frames?**

Yes we can see the retry flag for the Management frames as well. If there is no acknowledgement for the unicast management frame the frames will be retried.

4. At which rate the beacon frames are transmitted?

The transmission rate for beacon frames is typically the lowest mandatory data rate supported by the access point (AP). This is to ensure that beacon frames can be received by stations with a wide range of capabilities, including older stations that may not support higher data rates.

5. What happens if we transfer beacon frames at a higher data rate?

Transferring beacon frames at a higher data rate in a wireless network can have both advantages and drawbacks.

Advantages:

Faster Transmission: Beacon frames are used to announce the presence of a wireless network. Transmitting them at a higher data rate can make this announcement faster and more efficient.

Reduced Channel Occupancy: Transmitting beacons at higher data rates can decrease the time each frame occupies the wireless channel, potentially reducing interference and improving overall network performance.

Drawbacks:

Reduced Range: Higher data rates often come with reduced signal range. If the higher rate is used for beacon frames, it might limit the range at which devices can detect and connect to the network.

Compatibility Issues: Some devices might not support or be able to reliably receive beacon frames at higher data rates. This can lead to connectivity issues for devices that cannot properly interpret the faster transmissions.

6. Imagine a scenario where two clients connected to an Access point, The client1 transmitting data to AP, At that time client2 senses the medium and detects a transmission is happening. So, will client2 send the RTS frame to AP at that time?If it sends then shall we expect a collision because of that RTS?

No, client2 will not send an RTS frame to AP while client1 is transmitting data to AP. This is because the medium is already busy with client1's transmission, and any attempt by client2 to transmit would result in a collision.

When the client deletects the medium is busy (when it detects valid 802.11 frame) It won't transmit anything

7. What is the function of association request and what does it consist of?

When a device wants to join a wireless network, it sends an association request to the access point (AP) or router. This request includes information about the device, such as its identity and capabilities.

The association request consists of:

SSID (Service Set Identifier): The name of the wireless network the device wants to join.

BSSID (Basic Service Set Identifier): The MAC address of the access point.

Supported Rates: The data rates supported by the device, indicating its capabilities.

RSN Information: This allows devices and access points to understand each other's security capabilities and negotiate the strongest possible connection.

The RSN IE includes several subfields, each containing specific

information: Version: Indicates the version of the RSN protocol used.

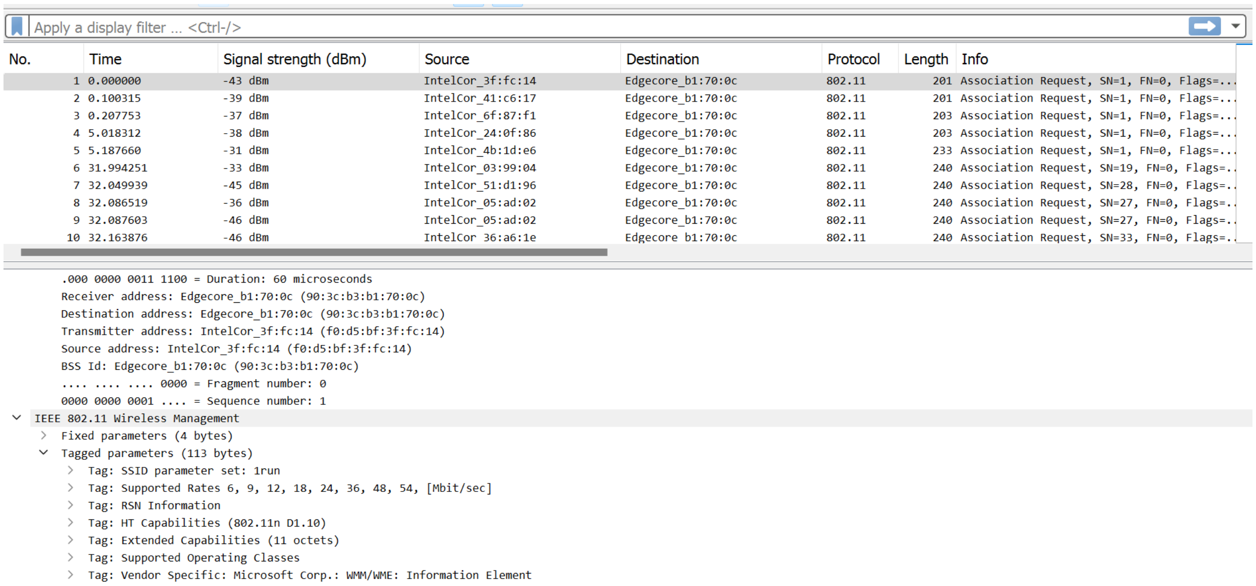
Group Cipher Suite: Indicates the encryption algorithm used for group communication (broadcast/multicast traffic).

Pairwise Cipher Suite(s): Indicates the encryption algorithms supported for pairwise communication (unicast traffic between a device and the access point).

Authentication Protocol(s): Indicates the supported methods for verifying the identity of devices (e.g., PSK, EAP).

PMKID List (optional): Contains a list of pre-authenticated keys for faster connection.

This information helps the access point determine if the device is allowed to join the network and how the connection should be established.



No.	Time	Signal strength (dBm)	Source	Destination	Protocol	Length	Info
1	0.000000	-43 dBm	IntelCor_3f:fc:14	Edgecore_b1:70:0c	802.11	201	Association Request, SN=1, FN=0, Flags=...
2	0.100315	-39 dBm	IntelCor_41:c6:17	Edgecore_b1:70:0c	802.11	201	Association Request, SN=1, FN=0, Flags=...
3	0.207753	-37 dBm	IntelCor_6f:87:f1	Edgecore_b1:70:0c	802.11	203	Association Request, SN=1, FN=0, Flags=...
4	5.018312	-38 dBm	IntelCor_24:0f:86	Edgecore_b1:70:0c	802.11	203	Association Request, SN=1, FN=0, Flags=...
5	5.187660	-31 dBm	IntelCor_4b:1d:e6	Edgecore_b1:70:0c	802.11	233	Association Request, SN=1, FN=0, Flags=...
6	31.994251	-33 dBm	IntelCor_03:99:04	Edgecore_b1:70:0c	802.11	240	Association Request, SN=19, FN=0, Flags=..
7	32.049939	-45 dBm	IntelCor_51:d1:96	Edgecore_b1:70:0c	802.11	240	Association Request, SN=28, FN=0, Flags=..
8	32.086519	-36 dBm	IntelCor_05:ad:02	Edgecore_b1:70:0c	802.11	240	Association Request, SN=27, FN=0, Flags=..
9	32.087603	-46 dBm	IntelCor_05:ad:02	Edgecore_b1:70:0c	802.11	240	Association Request, SN=27, FN=0, Flags=..
10	32.163876	-46 dBm	IntelCor_36:a6:1e	Edgecore_b1:70:0c	802.11	240	Association Request, SN=33, FN=0, Flags=..

```
    .000 0000 0011 1100 = Duration: 60 microseconds
    Receiver address: Edgecore_b1:70:0c (90:3c:b3:b1:70:0c)
    Destination address: Edgecore_b1:70:0c (90:3c:b3:b1:70:0c)
    Transmitter address: IntelCor_3f:fc:14 (f0:d5:bf:3f:fc:14)
    Source address: IntelCor_3f:fc:14 (f0:d5:bf:3f:fc:14)
    BSS Id: Edgecore_b1:70:0c (90:3c:b3:b1:70:0c)
    .... .... .... 0000 = Fragment number: 0
    0000 0000 0001 .... = Sequence number: 1
v IEEE 802.11 Wireless Management
  > Fixed parameters (4 bytes)
  v Tagged parameters (113 bytes)
    > Tag: SSID parameter set: 1run
    > Tag: Supported Rates 6, 9, 12, 18, 24, 36, 48, 54, [Mbit/sec]
    > Tag: RSN Information
    > Tag: HT Capabilities (802.11n D1.10)
    > Tag: Extended Capabilities (11 octets)
    > Tag: Supported Operating Classes
    > Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Information Element
```

8.Can AP set greenfield mode to any particular channel, or it sets to all supported channels?

In general, an access point (AP) that supports greenfield mode can enable it on specific channels, typically within the 5 GHz band. The AP doesn't automatically set greenfield mode on all supported channels; rather, it can be configured to use greenfield mode on selected channels based on the network's requirements and the capabilities of the connected devices.

9.What is an aggregated acknowledgment?

An aggregated acknowledgment, often referred to as Block Acknowledgement (Block ACK) allows a device to acknowledge the receipt of multiple data frames with a single acknowledgment frame. Instead of sending a separate acknowledgment for each received frame, which can introduce overhead, the Block ACK consolidates acknowledgments, improving efficiency in data transmission and reducing airtime usage.

10.In our mobile, when we try to scan for the first time, whether it is passive or active?

Phones are like sneaky listeners. They mostly eavesdrop on beacons (passive scan) to gather nearby Wi-Fi names. But if they're searching for a specific network, they turn into shouty detectives (active scan), calling out its name to see if it's hiding.

Also In passive scan, the power consumption is more than compared with active scanning os the mobile.

11. After an active scan and deciding a ssid, the next phase is auth request or probe requests?

Once your device has identified the desired Wi-Fi network through the active scan, it initiates the authentication process by sending an authentication request to the chosen access point. This is part of the process that establishes a secure connection between your device and the Wi-Fi network.