**Wifi Training Module 5 Assignment**

**Q1.**

WIFI - 6

1. It follows IEEE 802.11ax standard

2. It uses both 2.4 and 5 GHz frequencies

3. It uses 1024-QAM OFDMA Modulation scheme

4. Target Wake Time based power saving method was introduced

5. BSS coloring was introduced to avoid unnecessary transmission deferring.

6. Improvises MU-MIMO by supporting around 16 users

7. Offers enhanced security using WPA3

WIFI - 6E

1. Along with wifi-6 , it introduces 6 GHz frequency in use

2. Thereby offers congestion less high bandwidth and lower latency services.

3. Used channel bandwidth around 160 MHz

4. Maximum theoretical speed of around 9.6 Gbps is expected.

WIFI-7

1. It follows IEEE 802.11be

2. It uses 2.4,5,6 GHz frequencies

3. Channel bandwidth is extended upto 320 MHz.

4. It uses 4096 QAM with OFDMA

5. It introduced MLO (Multi Link Operation - to transmit using multiple frequencies, channels sequentially based on decisions or actively on multiple channels or handling multi radio multi link operations)

6. Maximum theoretical speed of around 9.6 Gbps is expected.

Comparing these advanced generations to their previous counterparts.

Modulation scheme -> Older generation wifi used DSSS, FHSS, OFDM. but these advanced generations uses OFDMA which essentially splits contiguous set of subcarriers into RU and allocates RU dynamically based on priority of traffic or in scheduled manner (TBRA) thereby ensuring multiple users can send simultaneously with same contention and CSMA/CA

Frequency of Use -> Older generation wifi uses 2.4 GHz and some newer standards may have used 5 GHz, but these advanced generation wifi uses all three 2.4,5,6 GHz frequencies thereby effectively increasing the channel bandwidth since wider frequencies are allocated in 6 GHz thereby boosting data rate and reduced interference due to other technologies.

Advanced Scheme -> Older generations might not have introduced MIMO but these advanced generation wifi uses MU\_MIMO that uses many spatial streams which are frequency flat and independent to each other thereby ensuring both multiplexing and diversity based on environment dynamics and receiver collobration (training sequences based channel analysis and feedback to transmitter for effective precoding and beamforming)

Data rate -> Upto wifi-5 itself, maximum theoretical data rate was around 6.9 Gbps but due to the usage of OFDMA with MU-MIMO and some other advanced features, data rate got pushed to 9.6 Gbps and 40 Gbps (in wifi-7)

BSS Coloring, TWT, MU-MIMO in both uplink and downlink, MLO, preamble puncturing for effective channel aggregation were utilized in recent wifi generations.

**Q2.**

OFDMA

1. Stands for Orthogonal Frequency Division Multiple Access. It is the simple extension of OFDM.

2. In OFDM, all subcarriers generated were used by single user at a time leading to reduced efficiency in terms of multi user support.

3. In OFDMA, in the name of Resource Units, users will be allocated with some contiguous subcarriers for use.

4. APs send Trigger frames in TBRA for Uplink OFDMA thereby assigning appropriate RU, timing, power settings for which clients respond in their allocated time slot. (Uplink)

5. It sends common preamble followed by each user's data in their assigned RU. (Downlink)

6. It is more useful in the case of IoT transmission where many devices send small packets may not occupy the entire channel in OFDMA.

7. Since multiple devices can transmit simultaneously, latency is avoided leading to predictable performance.

8. RU based TWT allocation can be done for power saving.

9. Replaces CSMA/CA + backoff for STAs with Uplink scheduling.

10. QoS is enhanced by Dynamic RU allocation.

**Q3.**

TARGET WAKE TIME

1. One of the important enhancements in wifi-6 (802.11ax)

2. Legacy wifi power save mode -> client enters doze state - AP buffers downlink frames -> client periodically (based on beacon frame interval), wakes up and sends PS-poll frame after checking TIM PVB in beacon frame to identify any buffered data in AP.

3. Unschedule Automatic Power save delivery is also one of the legacy power saving methods in 802.11e where client once after waking up sends trigger frame to AP and AP replies by sending multiple buffered frames in aggregated form and works per access category (as WMM power save)

4. Target Wake Time allows stations to negotiate sleep and wake time with AP for optimized power consumption instead of waking up periodically based on beacon interval.

5. If AP accepts TWT request from STA, it maintains TWT schedule per accepted STA.

6. During TWT request itself, waking time and duration upto it remains active , TWT identifier for broadcast, will be negotiated with AP.

7. During wake time, if trigger enabled, it listens for AP trigger for UL scheduling or else it directly sends and receives frames.

8. TWT scheduling can be either implicit (once negotiated, periodically same schedule will be followed unless renegotiated) or explicit (varies per session)

9. It is particularly beneficial for IoT devices since they are mostly battery operated therefore strict power conservation to be maintained. In this case, they can negotiate with AP a very comfortable timing as per data collection and processing requirement and it can optionally set trigger access to UL communication if needed. Thus, it offers better QoS and reduces unwanted contention and in the perspective of AP, scalability can be improved with optimized spectrum usage.

10. Real time use case : IoT enabled smart energy meter which may need to communicate every 30 minutes and the duration of communication may be around 2 seconds then TWT will be the effective choice since it can be uninterrupted for around 29 minutes 58 seconds leading to massive power saving.

**Q4.**

6 GHz in Wifi-6E

1. In case of 2.4 GHz band, it is technologically congested with either microwave oven or Bluetooth and etc. Moreover, it has only 3 non-overlapping channels for use.

2. In case of 5 GHz band, though it has around 25+ non overlapping channels (might not suffice in dense environments though), those are subjected to Dynamic Frequency Selection due to radar interference.

3. 6 GHz frequency often offers true 160 and 320 MHz ultra wide channels without congestion for high throughput applications.

4. It offers around 60+ non overlapping 20 MHz channels for use.

5. Devices with 6 GHz wifi will not get interference from previous wifi generation devices due to new spectrum usage (green field)

6. Recent wifi generations with 6 GHz support BSS coloring, TWT, MLO, OFDMA like advanced techniques promoting speed, safety, efficiency, QoS etc.

7. Though it offers only very small range, within that range, very high throughput can be achieved and moreover this easily isolates very closely spaced networks.

8. 6 GHz wifi generations use very advanced wifi security like SAE with Management frame protection techniques.

9. It is even advantageous to combine it with IoT devices since they can communicate without interference with many RU possible reducing overall latency in communication.

**Q5.**

COMPARING WIFI-6 AND WIFI-6E

1. 2.4 and 5 GHz were used in wifi-6. But, 6 GHz was introduced in wifi-6E

2. Wifi-6 can cover much higher range and supports good penetration but wifi-6E cannot support because of higher frequency and higher path loss. Therefore, it is well suited on open environments and line of sight shorter range communications.

3. Bandwidth of around 500 MHz is allocated in wifi-6, but 1200 MHz in case of wifi-6E

4. 25+ non-overlapping 20 MHz channels are available in wifi-6 but around 60+ non-overlapping 20 MHz channels are available in wifi-6E

5. 5+ non-overlapping 80 MHz channels are available in wifi-6 but around 12+ non-overlapping 80 MHz channels are available in wifi-6E

6. 2+ non-overlapping 160 MHz channels (with DFS) are available in wifi-6 but around 7+ non-overlapping clean 160 MHz channels are available in wifi-6E

7. In case of MU-MIMO, many users (around 16 users) can be accommodated simultaneously with single AP.

8. In case of MLO, efficient channel aggregation can be done for extremely higher data rate in both uplink and downlink.

9. Use cases for wifi-6E , ultra HD video streaming, AR/VR applications, URLLC, Localisation etc.

10. Wifi-6E doesn't get affected by legacy wifi devices, Bluetooth, zigbee , microwave ovens operation in vicinity, DFS constraints, Other APs in co-channel (chances are less due to wider spectrum availability)

**Q6.**

MAJOR INNOVATIONS IN WIFI-7

1. Introduction of 320 MHz channels for higher throughput in single transmission and in high bandwidth demanding real time applications like AR/VR applications

2. 4096-QAM was used along with OFDMA to encode each symbol using 12 bits in input.

3. Multi Link Operation technique enables devices to simultaneously transmit and receive data across multiple frequency bands using Multilink Multiradio concept. It also ensures devices can switch between bands based on priority, data to be transmitted etc.

4. Enhanced MU-MIMO increases the number of available spatial streams to be 16 from 8.

5. Single user can be allocated multiple RUs based on data within same channel reducing latency

6. It enables preamble puncturing so to use wider channels even when parts of the spectrum are corrupted.

7. BSS coloring and TWT got improvised for efficient data delivery.

8. Time Sensitive Networking ensures deterministic data delivery with low latency by using OFDMA, MU-MIMO, TBRA , Time sync support.

**Q7.**

MLO

1. It stands for Multi Link Operation. It is one of the groundbreaking innovation in wifi-7.

2. It allows devices to establish and utilize multiple wireless links simultaneously across different frequency bands and channels.

3. It enhances concurrent data transmission, throughput, reduces latency.

4. Simultaneous Transmit Receive MLO (STR) -> it leverages full potential of MLO by simultaneously using different frequency bands using Dual radios. Use case : AR/VR devices that streams HD video in one channel and receives user interaction in other ensuring seamless experience.

5. Non-STR MLO switches rapidly between transmission and reception links and it is advantageous in some configurations than single link operating devices.

6. Effective throughput is approximately the sum of capacity across each possible links.

7. It is also possible to do Load balancing with channel aggregation using multiple links or bandsteering based on environment dynamics and data rate requirements.

8. It enables data transmission even if one link is interrupted via preamble puncturing in channel aggregation.

**Q8,Q9,Q10.**

WIFI ROAMING :

1. It is the process by which a wireless client seamlessly transitions its connection from one AP to another within same network as it moves through different coverage areas.

2. Goal is to maintain uninterrupted connectivity for clients so that real time data access continue without noticeable disruptions.

3. Intra Controller Roaming occurs when client moves between APs managed by same controller. Here, controller facilitates the handoff and maintains the client's IP and session. It preserves authentication information during transition (over the air) and reduces latency during transition.

4. Inter controller roaming happens client moves between APs managed by different controllers within same network in this case to maintain connectivity complex communications happen between controllers via EoIP tunnel with actual controller as anchor and target controller as foreign and tries to maintain same IP by tunnelling all communication from station to anchor via foreign controller.

5. Mostly in centralized management (controller based), roaming standards are applied. That is, 802.11k,v,r standards for roaming optimization.

802.11k

1. It enables current AP to provide reports on neighbouring APs including details like channel number, frequency, SSID, signal strength and so on.

2. Clients can quickly evaluate the obtained report from AP instead of scanning in all channels for valid AP reducing its performance.

3. Improvised decision making from AP via report however, final decision to be made by stations to roam into.

4. Stations whenever it senses the weak signals from AP (RSSI) or missing beacons or persistent packet missing , it initiates roaming and seeks help from AP by asking for neighbour report.

5. During roaming, if any information intended to that particular station is obtained by AP, then it buffers those and relays those to new AP via DS over the air ensuring no data loss.

802.11v

1. It is the power optimization and network management substandard that heavily helps on wifi roaming. It is also called as wireless network management standard.

2. It enables network to communicate the network assisted decisions on client association to stations to ensure intelligent roaming with optimal power and load management.

3. Here, AP sends BSS transition management request frame to clients to steer them to better APs with strong signal and less load after detecting weak signal or request from high priority client to join but AP has much load.

4. Reduces decision making latency and also scanning latency

5. It also filters the traffic what client wants to receive at that instant.

6. To ensure indoor navigation tracking or coordinated roaming optimization, clients may exchange timing info for synchronization and location tracking.

802.11r

1. It also stands for Fast BSS Transition.

2. For time critical applications, re-authentication with new AP is not acceptable since it consumes significant time. For this, pre-authentication happens while roaming and efficient IP and session management based on inter and intra controller roaming happens.

3. Over the air FT -> here, client directly performs fast transition with target AP by sending authentication request expecting response and sending reassociation request and expecting response , for this keys were already negotiated based on previous APs authentication.

1. Over the DS FT -> STA doesn't directly communicate with target AP but via current AP. It sends FT auth req to current AP which forwards the same to target AP and responses will also be relayed via current AP. 4-tier Key hierarchy is used here for fast transition. MSK is derived in previous RADIUS server authentication. PMK is derived from MSK and provided to AP during association. PMK-R0 is derived from PMK and held by key holder typically original AP. PMK-R1 is derived by original AP and distributed to neighbouring APs (under same mobility domain) for fast roaming.
2. In over the DS FT case, During FT auth req and response, FT Information element was exchanged. Here, necessary credentials like mobility domain, sta-mac, identifier for who holding R0 key will be known by sta and it locally computes R0 and R1 key during roaming which will be used in target AP association thereby reducing latency.