**QUESTION : IN WHICH OSI LAYER THE WIFI STANDARD/PROTOCOL FITS ?**

Wifi primarily comes under LAYER 1 AND 2 (Physical and Data Link layer) of OSI Model.

1. With respect to Physical Layer, Wifi ensures following:
2. RF Frequency selection (2.4 GHz , 5 GHz or 6 GHz – ISM Band)

Lower frequency can be selected to get higher coverage since it experiences less attenuation and thereby can travel to higher distances. However, 2.4 GHz frequency especially is so crowded since Bluetooth, microwave oven is using the same frequency. It is limited to less data rate but vice versa for higher frequencies usage which also helps in integrating more antennae elements in MIMO in narrowing down the beamwidth thereby precoding can be done at transmitter side with beamforming for targeted user data transmission.

1. Antenna Technology (single or multiple antennae in both Tx and Rx side – MIMO)

In basic mode, MIMO increases throughput by multiplexing different data in parallel data streams (multiple independent fading channels) however increasing computational load in receiver in understanding the channel in real time. It is also possible for transmitter to understand channel in prior (CST) and does appropriate precoding in Tx side itself thus enabling receiver just to pickup the signal with considerable strength.

1. Channel width selection (it is one of the crucial elements in wireless communication systems which stands as fundamental element that enables wifi communication. Channel in this context refers to the band of frequencies based on the frequency of wifi it uses. From that frequency, there will be multiple channels based on defined width of the channel. For example, while using 2.4 GHz wifi – (the entire range of this frequency is 2.4 to 2.483 GHz . similarly for 5 GHz wifi, 5.180 – 5.825 GHz) lets say channel width of 20 MHz, there are around 3 to 5 non overlapping channel exist. The channels are expected to be non overlapping in adjacent sites to reduce adjacent channel interference. In farther distance, it is also possible to reuse the same channel by any access point howerver, co channel interference will be taken care of. In higher frequencies, wider channel can be allocated thereby achieving higher data rates but at the cost of getting interference due to less availability of non overlapping channels unless having higher bandwidth in wifi technology. Higher width channels leads to reduced range due to spread of applied power. Thus in 5 GHz wifi, DFS (Dynamic Frequency Selection) is used in selecting the suitable channel in real time. In 6 GHz wifi, by default around 59 non overlapping channels for low latency applications.
2. Modulation scheme selection (predominantly, DSSS , FHSS, OFDM or OFDMA will be chosen)

DSSS – Direct Sequence Spread Spectrum Modulation techniques is one of the very popular modulation schemes that was in use in wifi technology. It basically extends or widens the bandwidth of the data being transmitted to larger bandwidth for reducing Power Spectral Density so as to avoid Narrow Band Interference and to get hidden under environmental noise to avoid information tapping. It also enables the security to avoid eavesdropping by using unique PN sequence per session/user to extend the bandwidth by multiplying each bit of information with this chip sequence and transmits with 2.4 GHz carrier signal (spreading )thus making it harder to decode without using proper PN sequence in receiver side. It also enables continuous transmission instead of FHSS which switches Frequency in realtime and expects frequency synchronization in receiver side for proper decoding. It also offers spreading gain while dispreading the information in receiver side.

It helps in achieving higher data rates like 11 Mbps in 802.11b wifi standard.

(Cons – limited scalability due to unique PN sequence requirement, can’t avoid Wide Band Interference and inefficient spectrum usage)

OFDM AND OFDMA – OFDM(Orthogonal Frequency Division Multiplexing) is a digital modulation scheme that splits the single carrier width into multiple sub carriers each are ensured to be orthogonal to each other reducing the chance of interference between carriers and each are accompanied with QAM modulations to boost the data rate and to reduce ISI further, guard bands are installed between sub carriers and also last part of the ofdm symbols are attached in front – Cyclic prefix. Thereby, data can be multiplexed across different sub carriers boosting data rate. The extended version of OFDM is OFDMA (Orthogonal Frequency Division Multiple Access) , which make use of sub carriers in transmitting the data belonging to different users at same time increasing capacity or through put , which when combined with QAM with greater levels yields to maximum throughput (which is expected to be 40 Gbps if OFDMA with 4096 – QAM is used in Wifi-7 ).

In OFDMA, multiple user data transmission is efficiently handled by RU (Resource Units) which are **group of contiguous subcarriers** within a channel that is allocated to a specific user or device. Number of RU allocated depends on the wifi frequency being used and data size to be transmitted.

1. With respect to Data Link Layer, wifi does following :
2. In general, Data Link Layer has two sublayers. Those are, LLC (Logical Link Control) and MAC (Medium Access Control) sublayers.
3. Logical Link Control sublayer is the upper sublayer of Data Link Layer by considering Error control and Flow control services of Data Link Layer and also helps in multiplexing and de-multiplexing internet layer protocol information via single network interface.

Wifi uses IEEE 802.2 LLC – in case of Ethernet, there is a dedicated field in Ethernet frame format which assigns unique ID for important network layer protocols like IPv4, IPv6 , ARP etc. however, wifi doesn’t use Ethernet frame rather it uses 802.11 MAC frame for Wifi thus it makes use of 802.2 LLC which assigns SSAP (Source Service Access Point) and DSAP (Destination Service Access Point) fields which enhances the identification of many network layer protocols by allocating 5 bytes (LLC + SNAP)instead of Ethernet field which identifies only few protocols by allocating 1 byte.

Example SAP values:

1. IPv4 SAP = 0x06
2. IPv6 SAP = 0x86DD
3. ARP SAP = 0xAA

1. Medium Access Control Layer – it is the lower sublayer of Data Link Layer that handles Access control (defines CSMA-CA, ACK, Roaming and Handoff, Encryption Schemes), Framing, Fragmentation and MAC addressing.

CSMA – CA (Carrier Sense Multiple Access – Collision Avoidance) :

* 1. Station should check the state of wireless channel by estimating RSSI (Received Signal Strength Indicator) and comparing it with the Clear Channel Assessment (CCA) and identifying the BSS Color.
  2. By above procedure, if channel is continuously estimated to be idle for DIFS (Distributed Inter Frame Space ) duration (= slot time \* SIFS), then transmitted will wait for the random time calculated by contention window (slot time \* random number), whose size increases exponentially in case of repeated collision (no ACK received)
  3. Then, it transmits Control Frame (RTS) to the AP or peer (in case of AD-HOC) and expects CTS (RTS contains the protocol used, duration , length of data to be communicated).
  4. Once destination responds, Actual payload transmission begins.
  5. Hidden node problem is solved by sending RTS (not received by interfering node thus farther from it) to AP which sends back CTS (received by interfering node), any node which receives CTS should abort the transmission for the specified duration of communication (NAV – Network Allocation Vector).
  6. Exposed node problem is solved by sending RTS to destination device , since RTS would be received by adjacent node, it identifies itself to be closer to the sending device however, it will not receive CTS thus it can ignore that conversation and proceed with its own transmission.

1. 802.11 WIFI FRAME FORMAT :

There are three types of wifi frames. They are management, control and data frames.

Wifi frame format has following fields.

1. Frame control (2 bytes) – helps in identifying the type of wifi frame with flags. It defines the protocol (.11), type of frame , subtype (beacon – passive scanning, probe – active scanning, association – for security handshakes, authentication, rts,cts,ack,power saving poll), to DS? , from DS?, retransmitted frame?, protected frame?, fragmented frame?
2. Duration/ID (2 bytes) – discloses NAV (Network Allocation Vector) (rts time   
   + cts time + ack time + inter frame space) representing the duration upto which the channel will be occupied. In case of power saving mode, it contains Association ID which will be obtained by station from access point after authentication for ensuring the connection.
3. Address – 1 : receiver MAC address
4. Address – 2: sender MAC address
5. Address – 3: BSSID
6. Address – 4: used in Wireless Distribution System (multi hop routing)
7. Sequence number: This field tracks the order of frames and handles fragmentation. (if a data frame is fragmented, then each fragment will have same sequence number but with different fragment number)
8. Frame Body – it contains the actual payload or management information depending on the frame type. (standard payload , QoS payload from IEEE 802.11e , Null data frame in case of power saving mode)
9. Frame Check Sequence - Uses CRC-32 (Cyclic Redundancy Check) for error detection.