Wi-Fi TRAINING - MODULE 3

Akash S, embedUR Systems

Qn 1:

What are the different 802.11 PHY layer standards? Compare their characteristics.

802.11 Overview:

- 802.11 standards define how Wi-Fi devices communicate at the physical level
- Over time, Wi-Fi has evolved to support more devices, higher data rates, and better coverage
- The standards are backward compatible to ensure older devices can still connect

STD	FREQ	SPEED	MOD TYPE	BW	COMMENTS
802.11a	5 GHz	54 Mb/s	OFDM	20 MHz	Faster but Shorter Range
802.11b	2.4 GHz	11 Mb/s	DSS	20 MHz	Slower but Better range
802.11g	2.4 GHz	54 Mb/s	OFDM	20 MHz	Backward Compatible
802.11n	2.4 & 5 GHz	600 Mb/s	OFDM + MIMO	20/40 MHz	MIMO is introduced
802.11ac	5 GHz	~3.5 Gb/s	OFDM + MU-MIMO	20/40/80/160 MHz	Faster, multiple user support
802.11ax	2.4 & 5 GHz	~10 Gb/s	OFDM + MU-MIMO	Up to 160 MHz	Also Wi-Fi 6, for crowded nw

Qn 2:

What are DSSS and FHSS? How do they work?

Overview:

- DSSS and FHSS are both methods used to spread wireless signals across a wider frequency range
- This is to minimize interference in wireless communication

DSSS:

What it is:

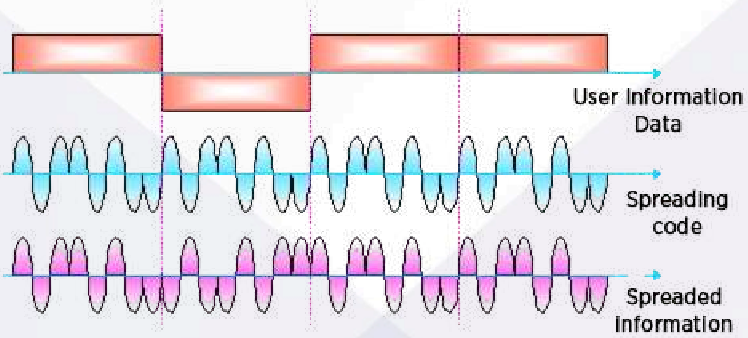
- DSSS - **Direct Sequence Spread Spectrum**
- It is a modulation technique used in telecommunications to reduce interference in signals during transmission
- Frequency of the signal is increased so that the final signal will be wider in bandwidth

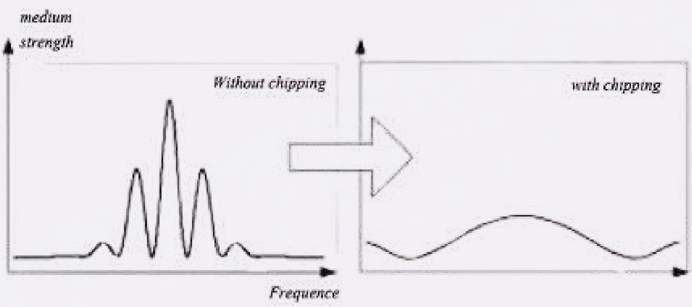
How it works:

- DSSS spreads data by multiplying it with a high-rate pseudo-random code (chipping code).
- The result is a signal that takes up more bandwidth but is more resilient to interference.

Benefits:

- Commonly used in 802.11b WiFi
- Provides strong resistance to signal interference
- Consumes more bandwidth than the original data





FHSS:

What it is:

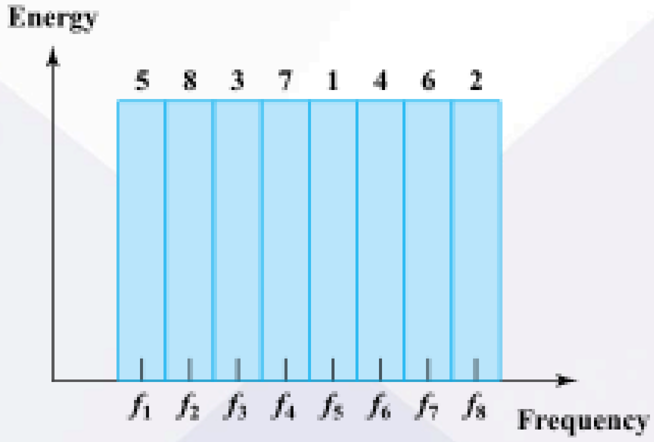
- FHSS - **Frequency Hopping Spread Spectrum**
- FHSS is a method of transmitting radio signals by rapidly switching between different frequencies within a given range
- It helps reduce interference and makes the signal harder to intercept

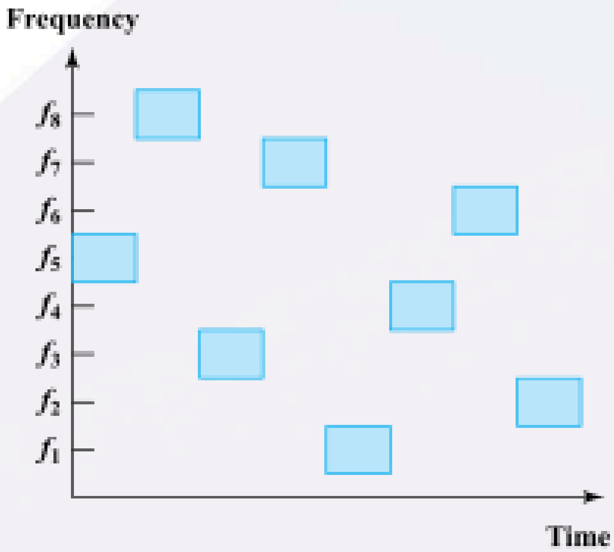
How it works:

- The available frequency range is divided into smaller channels like **79** in bluetooth
- The transmitter and receiver switch frequencies together in a pre-defined sequence called a hopping pattern
- Each hop happens at regular intervals like milliseconds so the signal doesn't stay long on any single frequency
- Even if one frequency channel experiences interference, it only affects a tiny part of the transmission - So no problem
- The hopping makes it difficult for others to intercept or jam the full communication unless they know the exact sequence

Benefits:

- Used in early Wi-Fi versions and Bluetooth
- Highly secure due to rapid hopping
- Less affected by narrowband interference





Qn 3:

How do modulation schemes work in the PHY layer? Compare different modulation schemes and their performance across various Wi-Fi standards.

Modulation:

- Modulation is the method used to convert binary data into signals like radio signals
- Physical layer handles this process using different types of modulation based on the Wi-Fi standard and signal conditions

TYPE	SYMBOL	SPEED	NEED
BPSK	1	Low	Very low
QPSK	2	Moderate	low
16-QAM	4	High	Medium
64-QAM	6	Very high	High
256-QAM	8	Extremely high	Very high
1024-QAM	10	Ultra high	Clean signal

Modulation:

- Modulation changes the amplitude, frequency, or phase of the carrier signal to represent digital data
- Goal is to transmit more bits per second without increasing the frequency range too much
- Each symbol can carry multiple bits depending on the modulation type
- Advanced schemes send more bits per symbol so that we can increase the speed but they also require stronger signal quality

Performance Comparison:

- **802.11b**
  - Uses BPSK and QPSK with DSSS
  - Very stable but low throughput - 11Mbps only
- **802.11g and 802.11a**
  - Use OFDM with BPSK, QPSK, 16-QAM and 64-QAM
  - Higher speeds up to 54 Mbps
- **802.11n**
  - MIMO is introduced and used upto 64-QAM
  - Speed increased upto 600 Mbps
- **802.11ac**
  - Added 256-QAM and wider channel bandwidths
  - Boosted performance to Gbps
- **802.11ax (Wi-Fi 6)**
  - Uses 1024-QAM, OFDMA and better efficiency techniques
  - High throughput can be achieved

Qn 4:

What is the significance of OFDM in WLAN? How does it improve performance?

OFDM:

- OFDM - **Orthogonal Frequency Division Multiplexing**
- It's a method of breaking a wide wireless channel into many smaller sub-channels (called subcarriers) that transmit data in parallel.
- OFDM is a method to break a wide wireless channel into multiple small channels and they are called as subchannels or subcarriers
- The speciality in OFDM is to transmit parallely
- Instead of sending data one chunk at a time OFDM sends smaller pieces over multiple frequencies simultaneously
- like sending multiple mini-packs instead of one big one

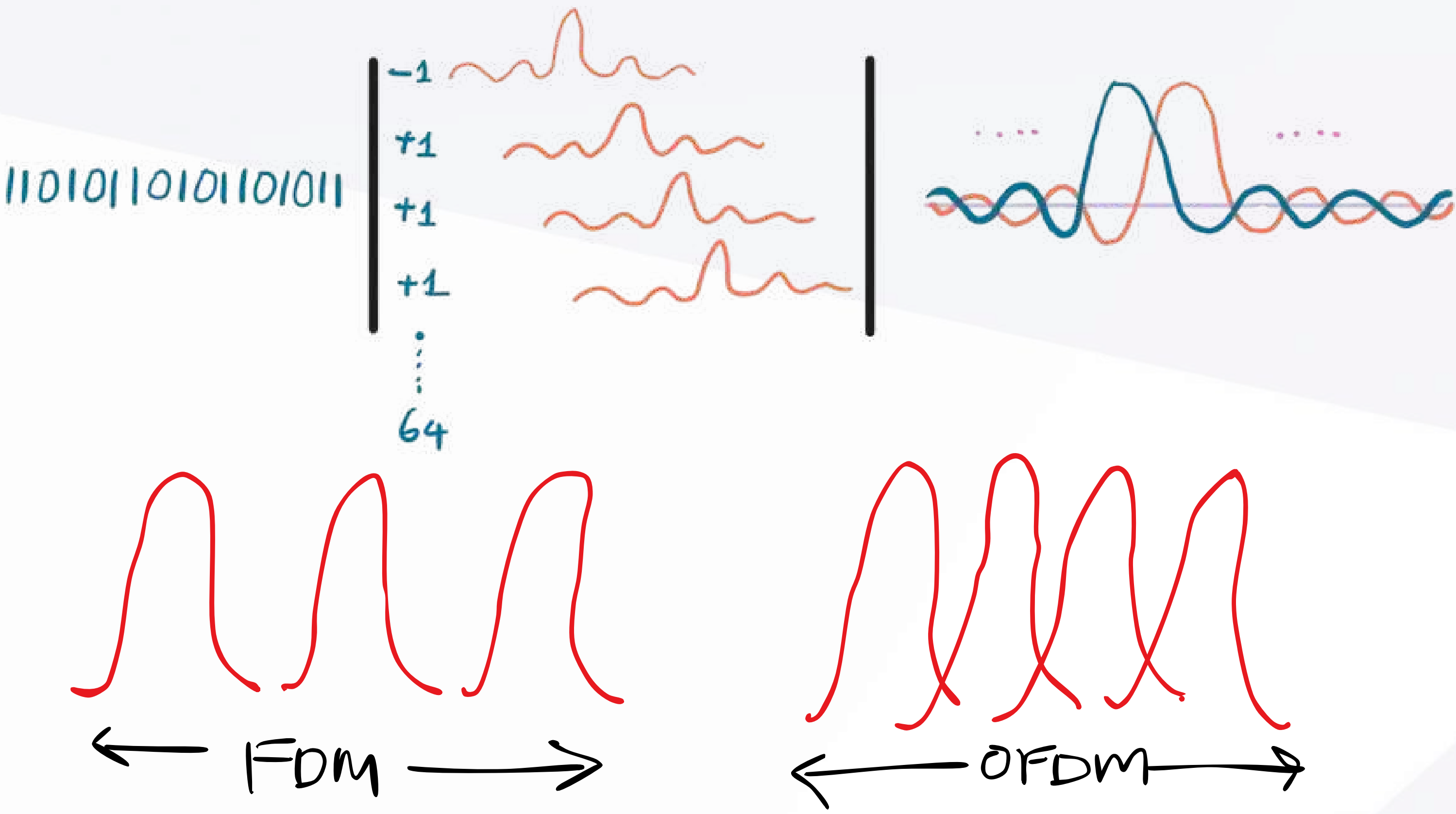
How OFDM works:

- A full channel bandwidth is split into multiple subcarriers
- Like 20 MHz in 802.11a or g or n can be split into 64 each

$$\frac{20\,\text{MHz}}{64} = 312.5\,\text{KHz}$$

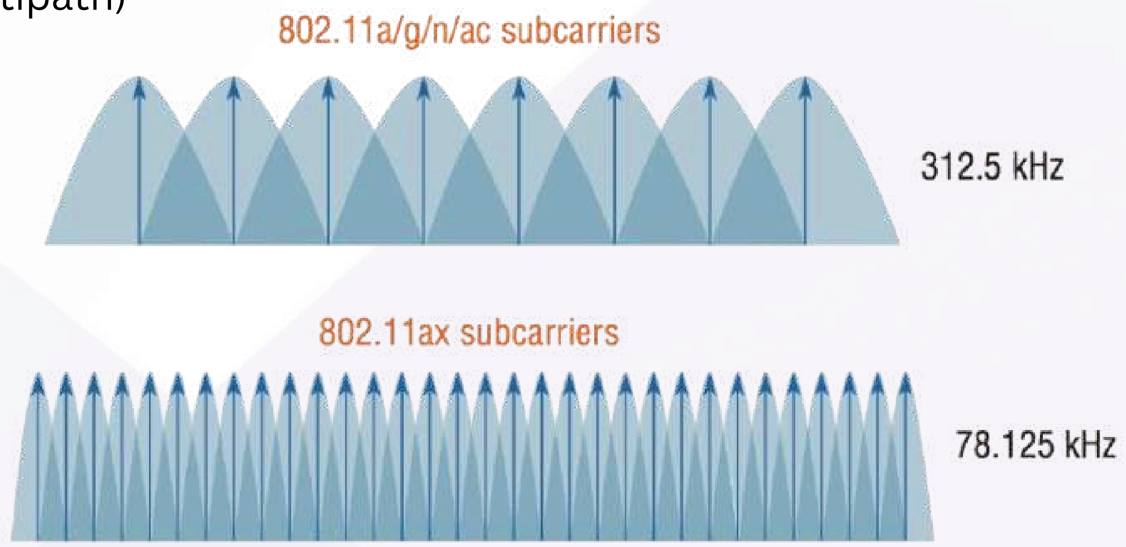
- Each subcarrier sends a part of the data using a modulation scheme like QAM
- These subcarriers are spaced orthogonally - they don't interfere with each other
- OFDM allows all subcarriers to transmit at the same time without overlapping signals

Hand-drawn Illustration:



Why OFDM is important for WLAN:

- Parallel data streams improve overall throughput
- Narrower subcarriers are less affected by interference or multipath fading
- Orthogonal spacing avoids overlap, maximizing channel usage
- Performs well even when signals reflect off walls or objects (multipath)



Qn 5:

How are frequency bands divided for Wi-Fi? Explain different bands and their channels

WiFi Frequency Bands:

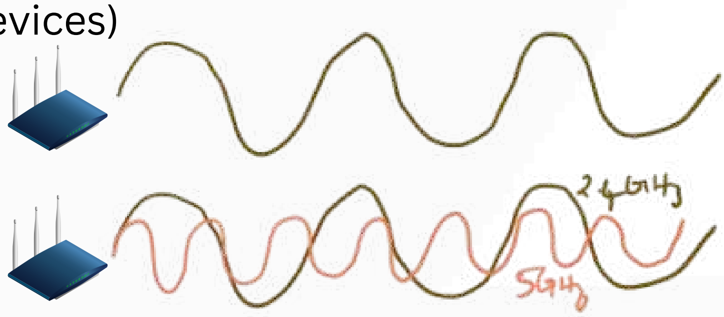
- When we connect to the wifi, it sometimes shows two are three wifi names that is because the routers transmit different frequency bands
- Currently **2.4 GHz, 5 GHz, 6 GHz** are the main bands
- Wi-Fi works over different frequency bands
- Like sections of the radio spectrum allocated for wireless communication
- Each band is divided into channels so multiple networks can coexist without clashing

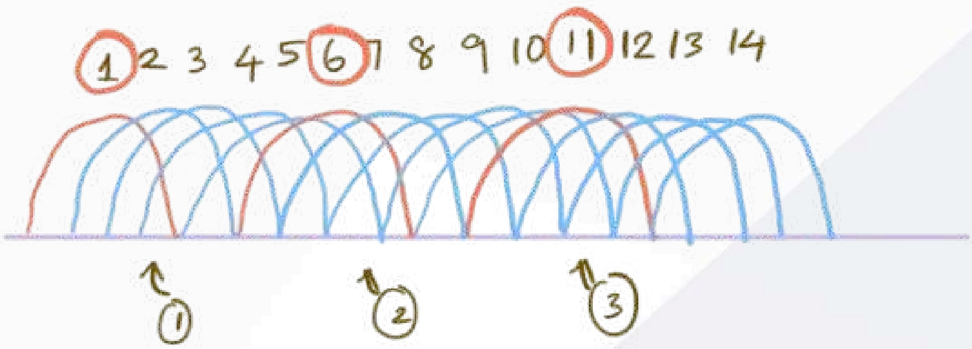
Main Frequency Bands:

BAND	RANGE	USE	FEATURES
2.4 GHz	2.4 – 2.4835 GHz	802.11b/g/n/ax	• Longer range • Fewer channels • more interference
5 GHz	5.15 – 5.825 GHz	802.11a/n/ac/ax	• More channels • less interference • Shorter range
6 GHz	5.925 – 7.125 GHz	802.11ax (Wi-Fi 6E)	• Clean • new band • ultra-fast speed • low congestion

Channel division:

- **2.4 GHz**
  - Has 14 channels (each 22 MHz wide, but only 3 non-overlapping: 1, 6, and 11)
  - Channels overlap, so interference is common
- **5 GHz**
  - Has 24+ non-overlapping channels (each 20 MHz, or bonded to 40/80/160 MHz)
  - Better for high-speed, high-density environments
- **6 GHz**
  - Offers 60+ non-overlapping channels
  - Ideal for future-proof, ultra-fast Wi-Fi
  - Requires compatible hardware (Wi-Fi 6E routers and devices)



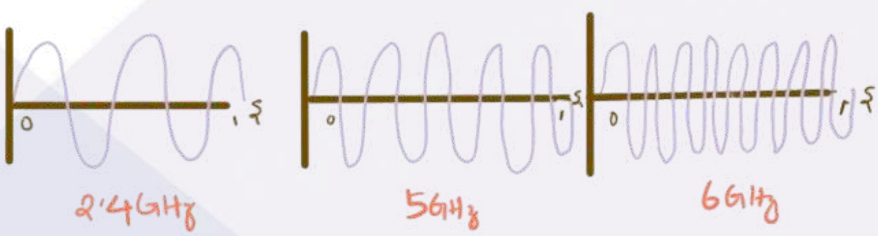


= 3 non-overlapping channels

$C = \lambda \cdot \nu$ ← frequency

speed of light → ; ↑ wavelength

$\lambda \downarrow \quad \nu \uparrow$

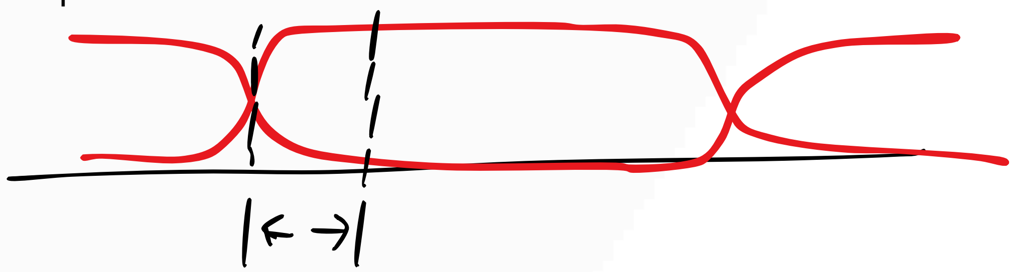


Qn 6:

What is the role of Guard Intervals in WLAN transmission? How does a short Guard Interval improve efficiency?

Guard Interval:

- Guard Interval is a short time gap inserted between symbols during wireless transmission
- It helps prevent signal interference caused by reflections or delays like multipath effects



Why are they used:

- When a Wi-Fi signal reflects off walls or objects, it can arrive late and interfere with the next symbol
- Guard Interval gives extra time between symbols so that these delayed signals don't cause overlap

Types

- **Long Guard Interval:**
  - 800 nanoseconds
  - Default in older Wi-Fi (802.11a/b/g/n)
- **Short Guard Interval:**
  - 400 nanoseconds
  - Optional in 802.11n/ac/ax for better speed
  - **50%** of the long Guard interval

For example, if we are sending 1000 symbols

Long GI : Total GI time = 1000 × 800ns = 8,00,000 ns

Short GI : Total GI time = 1000 × 400ns = 4,00,000ns

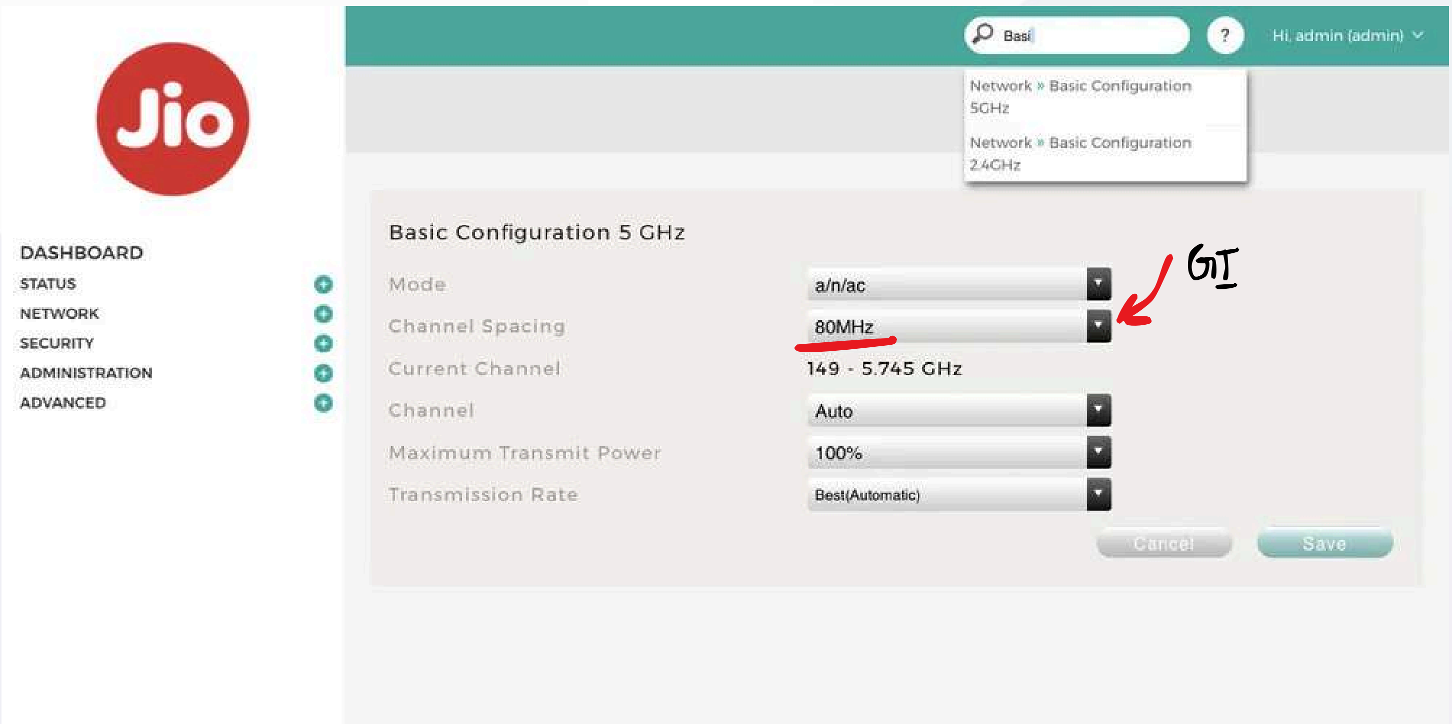
Sol.

Short Guard Interval for better efficiency:

- Short GI reduces the gap between signals, so more data can be sent in less time
- Improves overall Wi-Fi speed by around 10%
- Smaller intervals allow more symbols to be transmitted every second
- Works best when there's less interference or echo like in small rooms
- Overall network efficiency increases when Short GI is used correctly

Practical implementation:

- I logged into my Jio Broadband - **192.168.29.1**
- There I found the frequency division - **5 GHz**



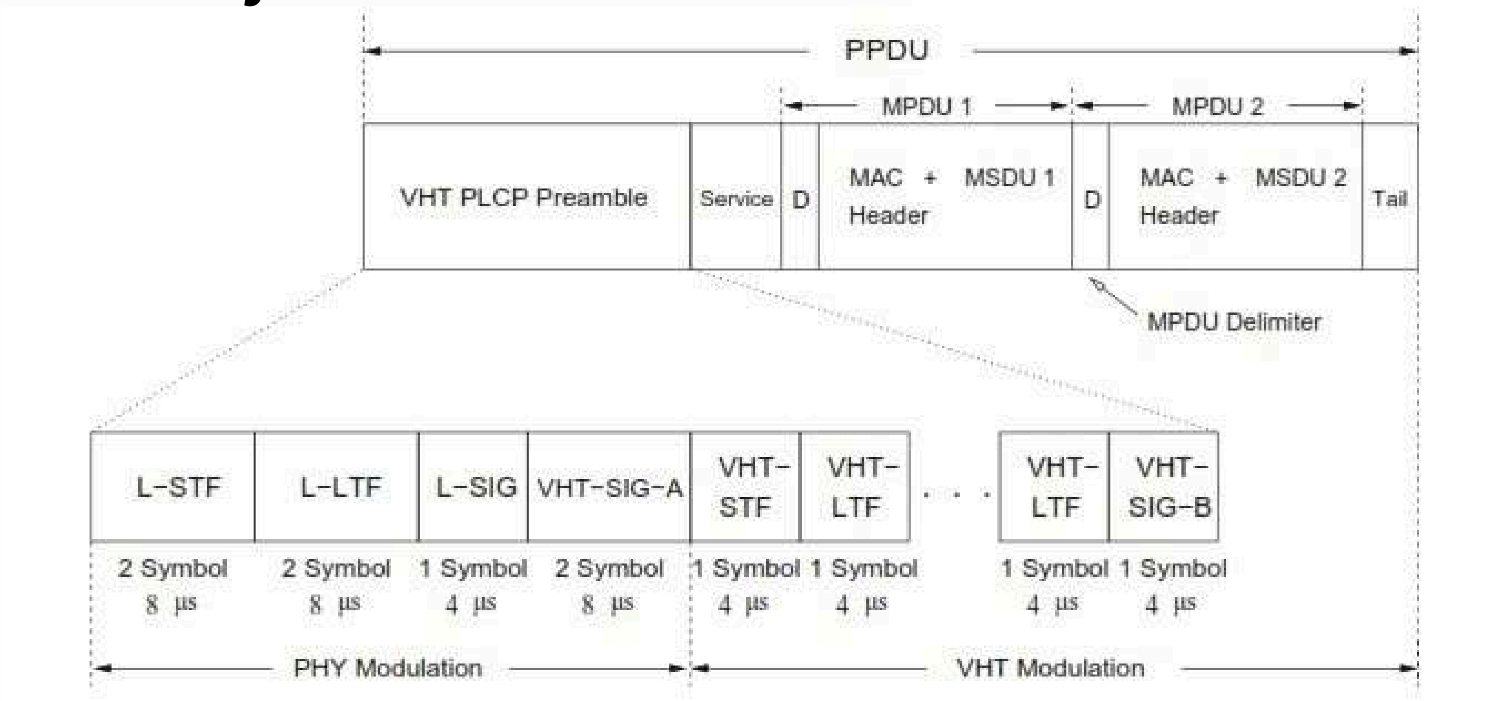
Qn 7:

Describe the structure of an 802.11 PHY layer frame. What are its key components?

802.11 PHY Layer:

- The PHY layer frame is the physical format of how Wi-Fi data is transmitted over radio waves.
- It ensures proper signal detection, synchronization, and data decoding at the receiver's end.
- The frame is made up of multiple sections that guide the receiver in reading the data correctly.

PHY Layer Frame Format:



Key Components:

Preamble:

- helps the receiving device detect, synchronize, and prepare for the incoming signal

- **Sync / Short Training Field (STF)** - used for signal detection and timing synchronization
- **Long Training Field (LTF)** – used for channel estimation and fine synchronization
- **Signal Field (SIG)** – carries details like modulation type and data rate for the rest of the frame

PLCP Header (Physical Layer Convergence Protocol Header)

- Provides information on how to decode the frame
    - Indicates frame length, modulation scheme, coding rate, and transmission rate
    - Ensures compatibility between sender and receiver, even if they support different versions of 802.11

PSDU (PLCP Service Data Unit)

- This is the actual data payload coming from the MAC layer.
- Contains:
    - **MAC Header** – Source/destination addresses, control info, etc
    - **MSDU** – The MAC-level data to be transmitted
    - **Tail bits** – Help in returning the decoder to a known state
    - **Padding** – Ensures total bits match symbol size required by modulation

VHT PLCP Preamble

- used for synchronization and channel estimation

Field	What It Does
L-STF	Helps detect the signal and timing sync (Legacy devices)
L-LTF	Legacy training sequence for channel estimation
L-SIG	Legacy signal info (e.g., length of PSDU)
VHT-SIG-A	Provides MCS, bandwidth, and other VHT info
VHT-STF	Short training field for VHT signal detection
VHT-LTF	VHT training fields — used for MIMO channel estimation
VHT-SIG-B	Contains information about user allocation and data

Qn 8:

What is the difference between OFDM and OFDMA?

OFDM:

- OFDM - **Orthogonal Frequency Division Multiplexing**
- OFDM is a technique where a single user's data is split across multiple closely spaced subcarriers
- All subcarriers are used by one user at a time
- Commonly used in older Wi-Fi standards like 802.11a/g/n/ac
- Helps improve speed and resistance to interference

OFDMA:

- OFDMA - **Orthogonal Frequency Division Multiple Access**
- OFDMA allows multiple users to transmit data simultaneously by assigning different subcarriers to each one
- Introduced in **802.11ax (Wi-Fi 6)** for better efficiency in crowded networks
- Reduces latency and improves throughput, especially when many devices are connected

Comparison:

FEATURE	OFDM	OFDMA
Users per time	One user	Multiple users at once
Efficiency	Lower in dense networks	Higher in dense environments
Used in Wi-Fi	802.11a/g/n/ac	802.11ax (Wi-Fi 6)
Subcarrier use	All subcarriers to one user	Divides subcarriers across users

Qn 9:

What is the difference between MIMO and MU-MIMO?

MIMO:

- MIMO - **Multiple Input Multiple Output**
- MIMO uses multiple antennas on both the transmitter and receiver to send and receive multiple data streams simultaneously
- Increases speed and reliability by using spatial streams
- Used in standards like 802.11n and 802.11ac
- Only one user is served at a time, but with multiple data streams

MU-MIMO:

- MU-MIMO - **Multi-User Multiple Input Multiple Output**
- An upgrade of MIMO that allows multiple users to be served at the same time using different spatial streams
- Used in 802.11ac (downlink only) and 802.11ax (uplink & downlink)
- Great for environments with many devices (homes, offices, stadiums)

Comparison:

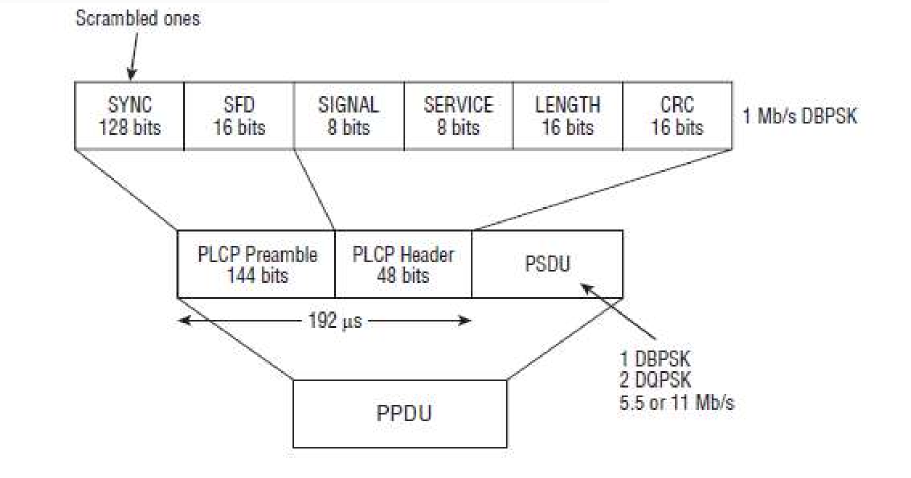
FEATURE	MIMO	MU-MIMO
Users per time	One user	Multiple users
Spatial streams	Sent to one device	Shared between multiple devices
Used in Wi-Fi	802.11n, 802.11ac	802.11ac (DL), 802.11ax (UL & DL)
Benefit	Speed boost	Speed + efficiency in multi-user

Qn 10:

What are PPDU, PLCP, and PMD in the PHY layer?

PPDU:

- PPDU - **PLCP Protocol Data Unit**
- The complete physical layer data unit that's sent over the air
- Includes
    - Preamble (for synchronization)
    - PLCP header (for decoding instructions)
    - PSDU (actual data from MAC layer)
- Different Wi-Fi generations have different types of PPDUs (legacy, HT, VHT, HE)
- Format varies depending on whether the device is using 802.11a/b/g/n/ac/ax
- The receiver starts decoding only after it gets the full PPDU



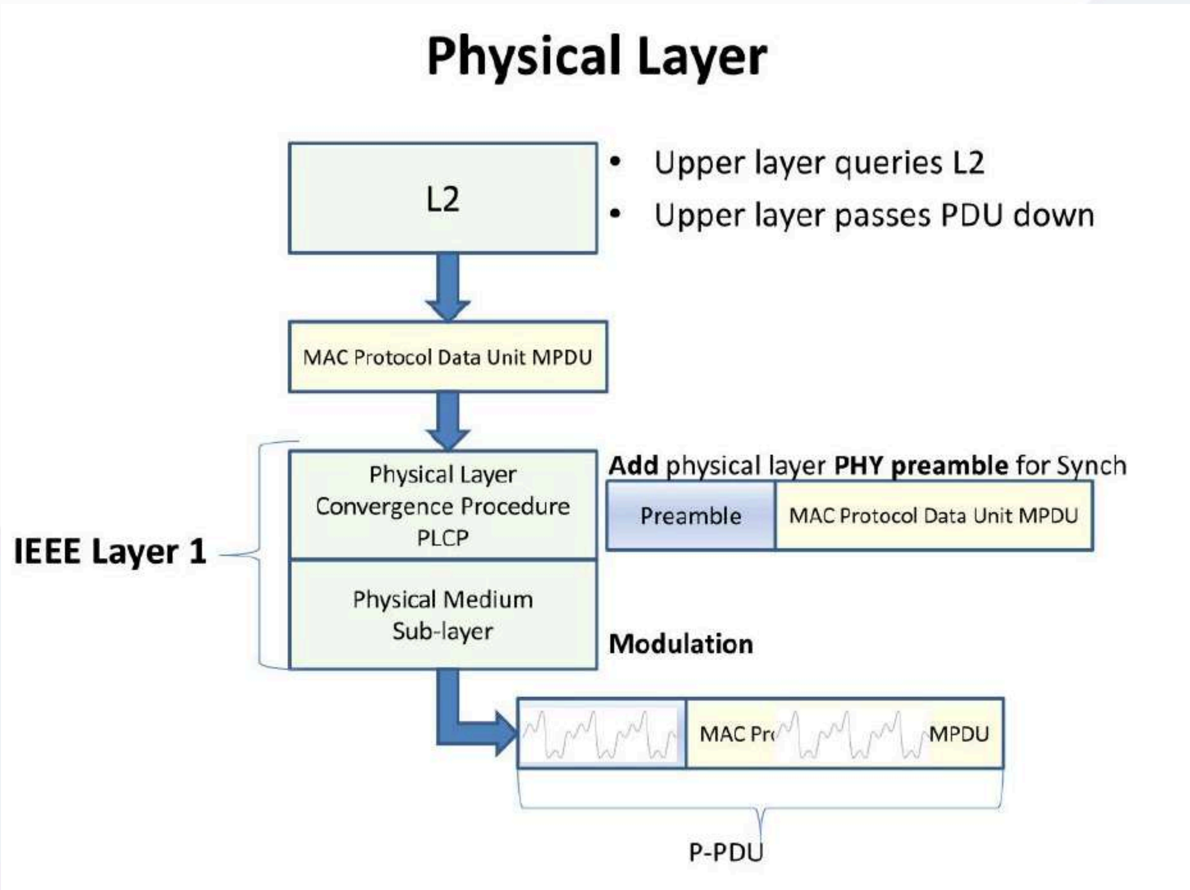
PLCP:

- PLCP - **Physical Layer Convergence Protocol Sublayer**
- Responsible for preparing MAC data for physical transmission
- Adds important control info (like rate, length, modulation type) to the frame
- Ensures interoperability between different PHY types and the MAC layer

- Adds:
  - Training sequences (used for estimating the channel)
  - Signal field (helps the receiver understand how to decode the data)
- PLCP makes sure the data is properly packaged and understood by the receiver

PMD:

- PMD - **Physical Medium Dependent Sublayer**
- Converts digital data into analog RF signals for over-the-air transmission
- Handles modulation/demodulation, frequency selection, and antenna signaling
- Closely tied to the radio hardware
- Responsible for
  - Signal power control
  - Frequency hopping or channel selection
  - Managing noise, interference, and errors
- It's where bits become radio waves and vice versa



Qn 11:

What are the types of PPDU? Explain the PPDU frame format across different Wi-Fi generations.

PPDU:

- PPDU - **PLCP Protocol Data Unit**
- It's the complete physical layer frame that gets transmitted over the air
- It includes everything needed for the receiver to understand and decode the data:
    - Preamble (for synchronization)
    - Header (with control info like rate, length, etc.)
    - Payload (the actual data to be delivered)

Types of PPDU:

Legacy PPDU
- Used in 802.11a/b/g
- Only supports one user at a time
- Simple structure with basic fields

HT PPDU (High Throughput)
- Used in 802.11n
- Adds support for MIMO and 40 MHz channels
- Includes HT-specific fields for improved performance

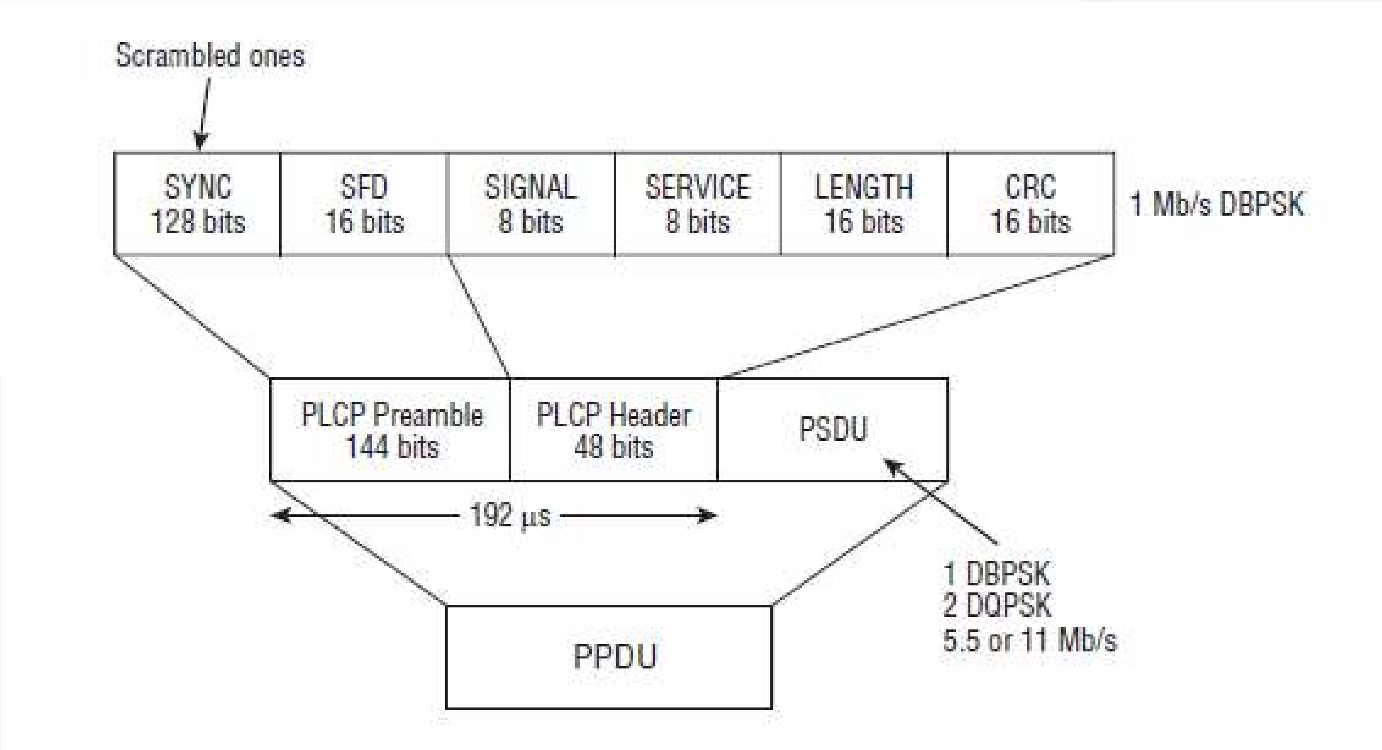
VHT PPDU (Very High Throughput)
- Used in 802.11ac
- Introduces MU-MIMO, 80/160 MHz bandwidths
- Has more detailed headers like VHT-SIG-A and VHT-SIG-B

HE PPDU (High Efficiency)
- Used in 802.11ax (Wi-Fi 6)
- Supports OFDMA and uplink/downlink MU-MIMO
- Designed for dense environments and more users

PPDU Frame Format Across WiFi generations:

GENERATION	PREAMBLE	MAIN FEATURES
Legacy	Short Training → Long Training → Signal → Data	Basic transmission, single user
HT (n)	Legacy fields + HT-SIG + HT-STF/LTF → Data	MIMO, 20/40 MHz support
VHT (ac)	Legacy preamble + VHT-SIG-A/B + VHT-STF/LTF → Data	MU-MIMO, wide channels (80/160 MHz)
HE (ax)	HE-SIG-A/B + HE-STF/LTF + Trigger + Data	OFDMA, UL/DL MU-MIMO, power saving

PPDU Frame Format:



Qn 12:

How is the Data Rate Calculated?

Formula:

$$\underset{(\text{Mbps})}{\text{Data rate}} = N_{\text{subcarriers}} \times \text{Bits per subcarrier} \times \text{Coding rate} \times \text{Symbol rate}$$

here

- Nsubcarriers = Number of data subcarriers
    - Varies by channel width and modulation
    - For 20 MHz in OFDM 52 data subcarriers are there
- Bits per subcarrier = Based on modulation scheme
    - BPSK = 1
    - QPSK = 2
    - 16-QAM = 4,
    - 64-QAM = 6
- Coding rate = Error correction ratio like 1/2, 2/3, 3/4, 5/6
- Symbol rate = OFDM symbols transmitted per second
    - for 20MHz it is 250000

Scenario based calculations:

Let us take two examples

- One with **802.11a** with 20MHz
- One with **802.11n** with 20MHz
- For error correction, I have chosen the coding rate as **¾** for simpler calculation

Calculation Examples:

Example 1: 802.11a (20MHz)

$N_{subcarrier} = 52$

Bits/subcarrier = 6 $\longrightarrow$ 64-QAM

Coding rate = 3/4

Symbol rate = 250,000 symbols/sec

$\therefore$ Data rate $= 52 \times 6 \times \frac{3}{\cancel{4}} \times \overset{62,500}{\cancel{250,000}}$ bps

$= 58,500,000$ bps

$= 58.5$ Mbps

Example 2: 802.11n

$N_{subcarrier} = 52$

Bits/subcarrier = 4 $\rightarrow$ 16-QAM

Coding rate = 3/4

Symbol rate = 250,000

Spatial streams = 2

$\therefore$ Data rate $= 52 \times \cancel{4} \times \frac{3}{\cancel{4}} \times 250,000$

$= 39,000,000$

$= 39$ Mbps

Total Data rate $= 39$ Mbps $\times 2$

$= 78$ Mbps

THE END

AKASH S

embedUR