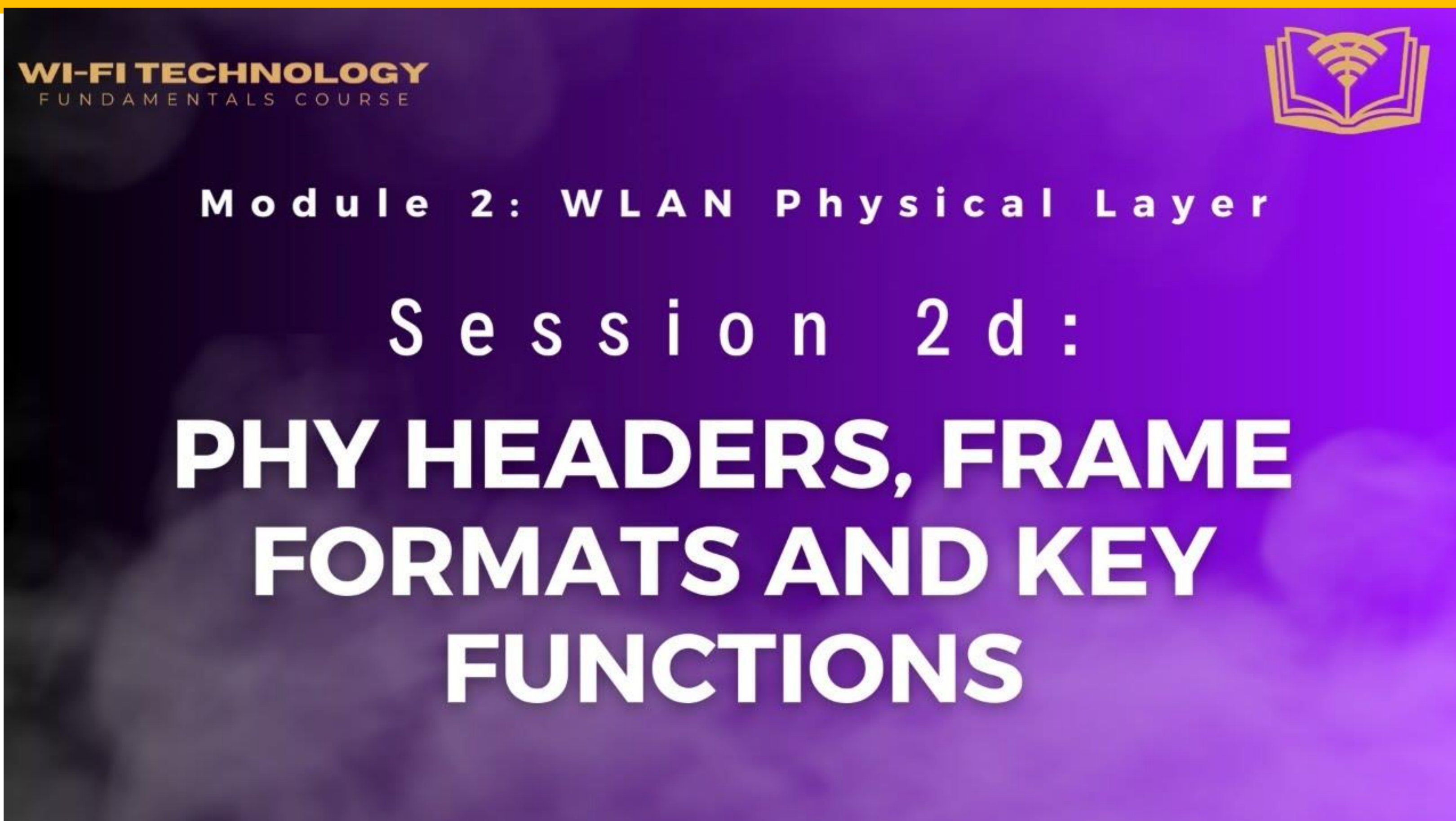
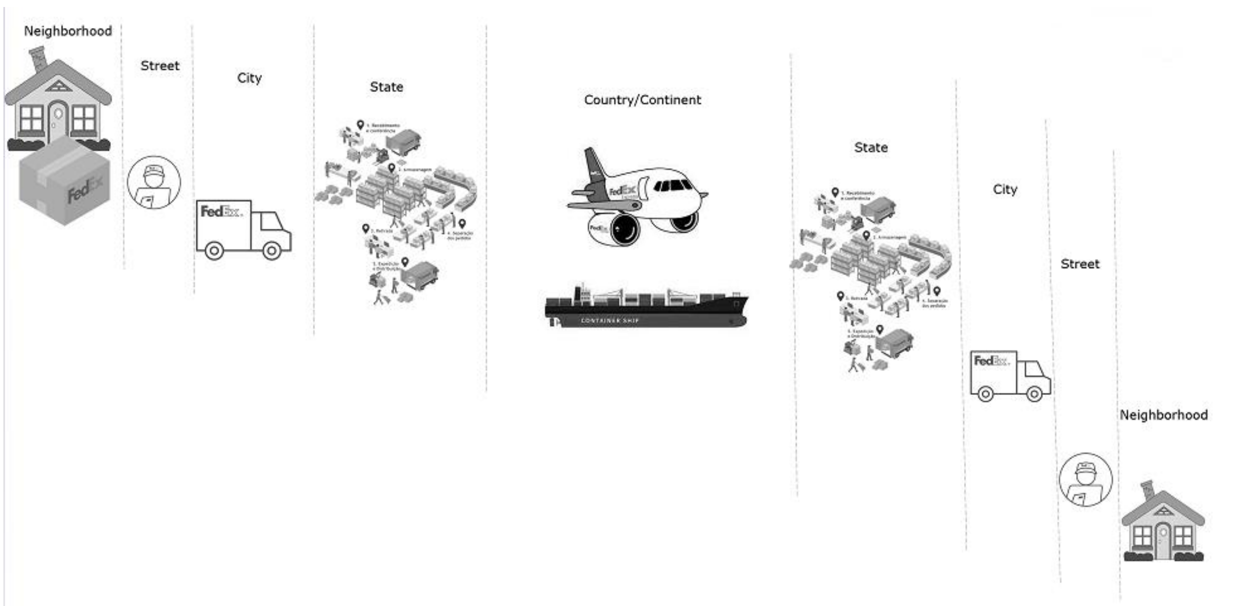


Thanushya Mothikivalasa
Rohini kaparapu
Nishtala Kiranmai
Jami Harika
Shiny Sayyad

From communications to networking

- When information needs to be transferred from one point to the next point, it is **Communications.**
- When information needs to be transferred over several points(hops), it is **Networking.**
- **Network protocols** are a set of rules outlining how connected devices communicate across a network to exchange information easily and safely. Protocols serve as a common language for devices to enable communication irrespective of differences in software, hardware, or internal processes.

This can be better understood by referring to the below analogy :



Think of communication as the process of sending a parcel from one country to another. Person A wants to send a parcel, so they hire a delivery agency. Communication starts when Person A provides delivery instructions to the agency, much like devices in a network sending data.Now, instead of just delivering the parcel directly, it goes through a network of locations. The parcel first goes to a local collection point (akin to a local network), then gets grouped with other parcels at a state parcel location (similar to data routing through a network), and eventually joins the national parcels (like data packets in a larger network).At each stage, there are intermediary locations and processes, just like routers and switches in a network, that play a role in directing the parcel toward its final destination. Finally, the parcel is sent to the receiver through various means like air, sea, or road, much like data traveling through various routes. This process is similar to how communication and networking operate: data is sent, directed through a network, and reaches its intended recipient

WHY LAYERS ?

Layers provide a structured, modular approach, simplifying system design and maintenance.
Layers enable diverse components to work together seamlessly, ensuring compatibility.
Layering optimizes system performance and resource usage by focusing on specific tasks.
Layers make problem identification and resolution more efficient.
Layering promotes common protocols and practices, enhancing consistency and compatibility.

Example:

Networking and Overhead in Sending a Ball of Chocolate
- Networking involves sending information from one place to another.
- To send something, layers of overhead are added for protection and transportation.

Example: Sending a Ball of Chocolate
- Ball of chocolate is the desired item for the end customer.
- The goal is to send it to a different location, which involves adding layers of overhead.

Layer 1: Wrapper
- Purpose: Protect the chocolate from melting and damage.
- Adds cost, weight, and volume to the item.

Layer 2: Packing in Boxes
- Purpose: To group chocolates into quantities, e.g., 10 or 12 per box.
- Adds additional weight and cost to the product.

Layer 3: Box Packaging
- Purpose: To facilitate storage on store shelves.
- A different format is needed for display in stores.

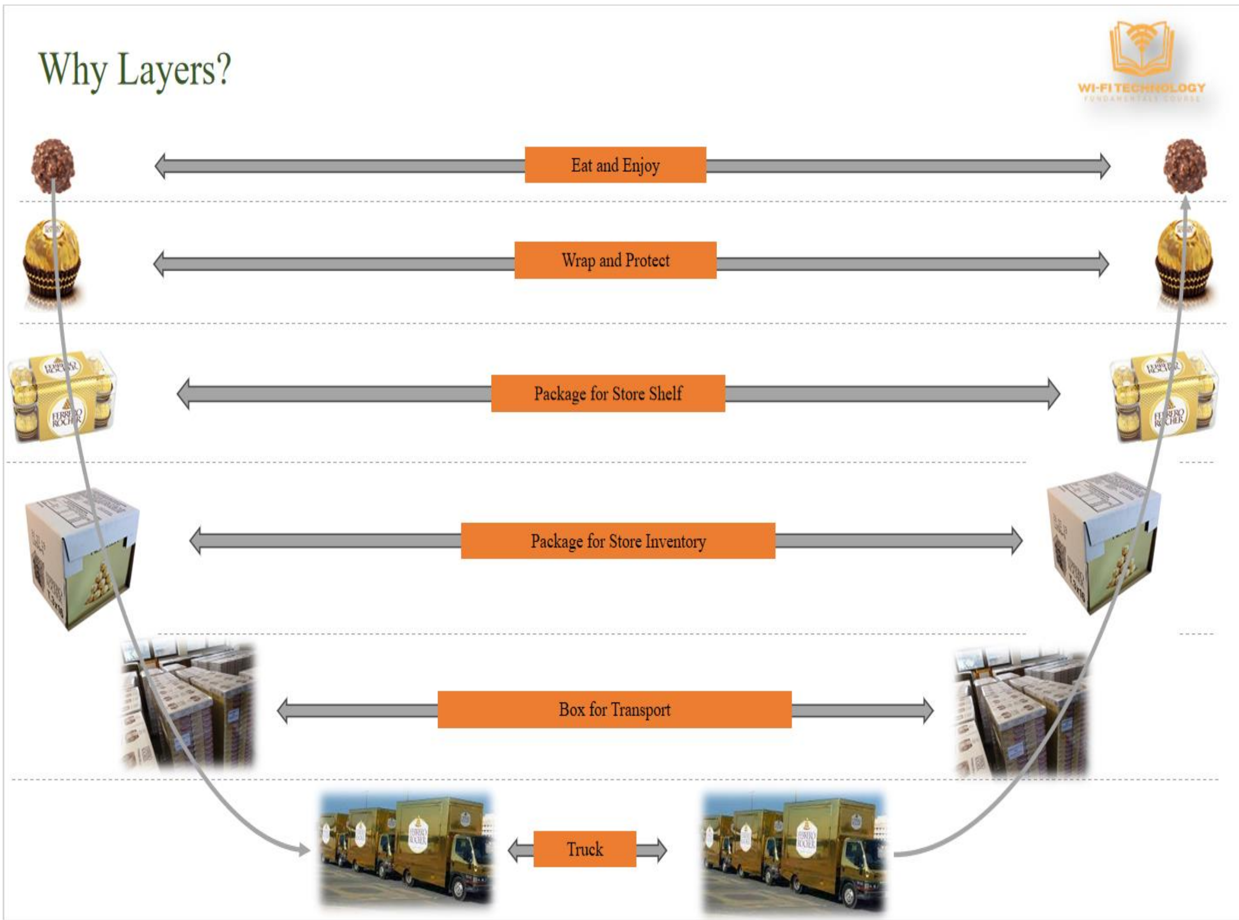
Layer 4: Pallet
- Purpose: To make transportation more efficient.
- Multiple boxes are shrink-wrapped on pallets for ease of handling.

Layer 5: Truck Transportation
- Purpose: To move the items to the receiving location.
- The truck adds an extra layer of overhead to the process.

Unpacking on the Receiving Side

- Pallets are removed, boxes are unpacked, and the individual units are accessed.
- The end customer can finally enjoy the chocolate payload.

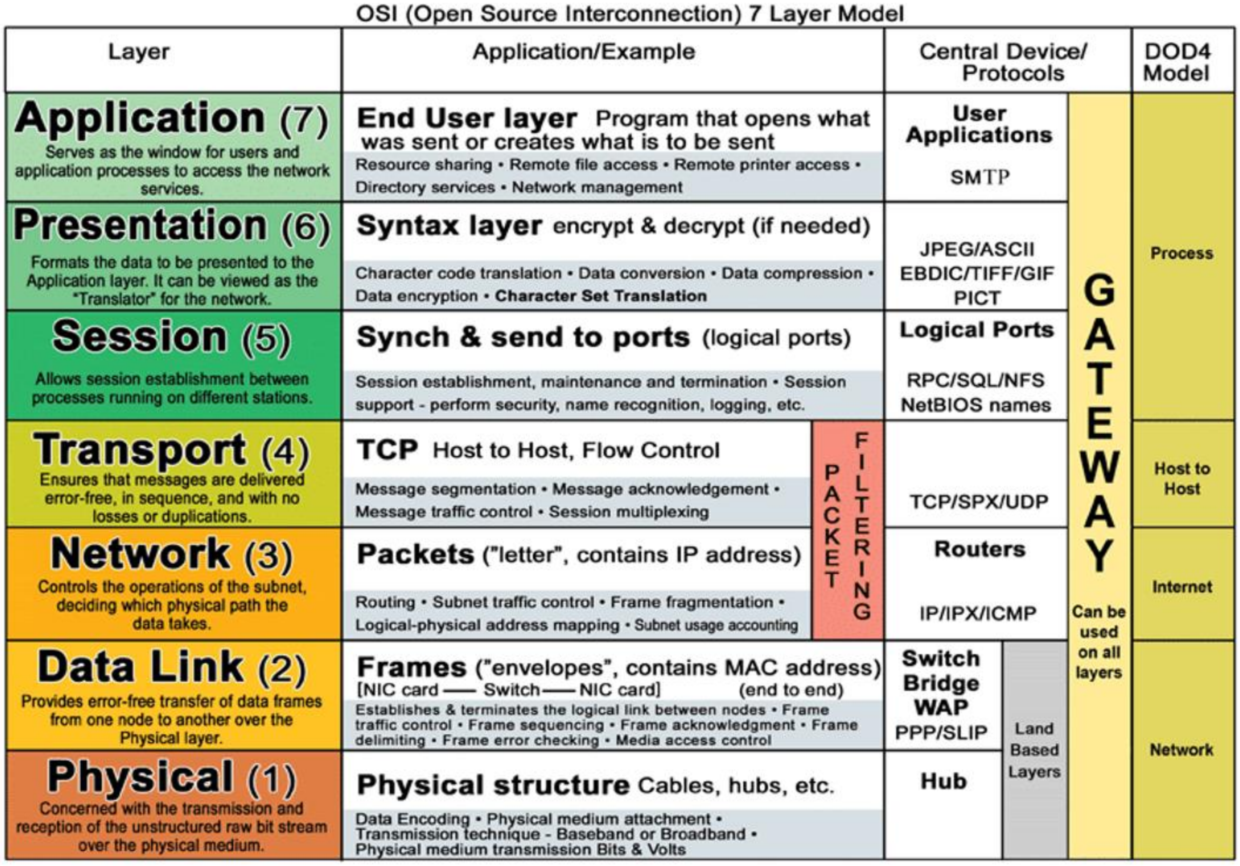
Conclusion: Each Layer Has a Purpose
- Every layer of overhead serves a specific purpose in the process of safely transporting the product.
- The payload is the end goal, but the layers are necessary for protection, display, storage, and transportation.



OSI Network Layers

OSI, which stands for Open Systems Interconnection, is a framework introduced by the International Organization for Standardization (ISO) in 1984. This framework is organized into seven layers, and each layer has its unique role to play. These seven layers cooperate to facilitate the seamless transmission of data between individuals or devices, enabling communication across the world.

OSI (Open Source Interconnection) 7 Layer Model



Layer	Application/Example		Central Device/ Protocols			DOD4 Model
Application (7) Serves as the window for users and application processes to access the network services.	**End User layer** Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management		**User Applications** SMTP		G A T E W A Y Can be used on all layers	Process
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	**Syntax layer** encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • **Character Set Translation**		JPEG/ASCII EBDIC/TIFF/GIF PICT			
Session (5) Allows session establishment between processes running on different stations.	**Synch & send to ports** (logical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.		**Logical Ports** RPC/SQL/NFS NetBIOS names			
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	**TCP** Host to Host, Flow Control Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	PACKET FILTERING	TCP/SPX/UDP			Host to Host
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**Packets** ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting		**Routers** IP/IPX/ICMP			Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control		**Switch Bridge WAP** PPP/SLIP	Land Based Layers		Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts		**Hub**			

Physical Layer:

The first layer in the OSI reference model is called the physical layer. This layer deals with the actual physical connections between devices and is responsible for transmitting data in the form of individual bits. When data is received, the physical layer converts the incoming signals into 0s and 1s and then passes them to the Data Link layer, which reassembles the data.

Functions of the Physical Layer:

1.Bit Synchronization: This layer provides a clock that synchronizes the bits. It ensures that both the sender and receiver are on the same page, maintaining synchronization at the bit level.
2.Bit Rate Control: The Physical layer also sets the transmission rate, which determines the number of bits sent per second.
3.Physical Topologies: It specifies how devices or nodes are arranged in a network. This can be in the form of a bus, star, or mesh topology.

4.Transmission Modes: The Physical layer defines how data flows between two connected devices. It supports various transmission modes, including Simplex (one-way communication), half-duplex (two-way, but one at a time), and full-duplex (simultaneous two-way communication).

Data Link Layer

The Data Link Layer is responsible for ensuring that messages are delivered reliably from one node to another in a network. Its main job is to oversee error-free data transfer over the physical layer. When a packet arrives in a network, the Data Link Layer handles its transmission to the correct destination by using the MAC address.

The Data Link Layer itself is split into two sublayers:
1.Logical Link Control (LLC):This sublayer deals with the flow and control of data between devices.
2.Media Access Control (MAC):The MAC sublayer is responsible for managing access to the physical transmission medium, ensuring that devices take turns sending data.

To get the packet ready for transmission, the Data Link Layer breaks it into smaller units known as frames, based on the Network Interface Card's frame size. It also includes the MAC addresses of the sender and receiver in the frame's header. To obtain the receiver's MAC address, it uses the Address Resolution Protocol (ARP), essentially asking, "Who has that IP address?" and receiving the corresponding MAC address in response.

Key Functions of the Data Link Layer:

1.Framing: This function allows the sender to transmit a set of bits that have meaning for the receiver. It does so by adding special bit patterns at the beginning and end of the frame.
2. Physical Addressing: After framing, the Data Link Layer inserts the physical addresses (MAC addresses) of both the sender and receiver into the frame's header.
3.Error Control: It provides mechanisms for detecting and retransmitting frames that are damaged or lost during transmission.
4.Flow Control: To prevent data corruption, the Data Link Layer ensures a constant data rate on both ends by coordinating the amount of data sent before requiring an acknowledgment.
5.Access Control:In situations where multiple devices share a single communication channel, the MAC sub-layer helps determine which device has control over the channel at a given time. This prevents data collisions and ensures orderly communication.

Network Layer

The Network Layer handles the transfer of data between different hosts located in separate networks. It also plays a crucial role in packet routing, which involves choosing the most efficient path to send a packet among the available options. To ensure data reaches the right destination, the network layer includes the IP addresses of both the sender and receiver in the packet's header.

Key Functions of the Network Layer:

1.Routing: Network layer protocols determine the best path from the source to the destination. This process is known as routing and is vital for efficient data transmission.

2.Logical Addressing: To uniquely identify each device on the larger network (the Internet), the network layer establishes an addressing system. This system involves placing the sender's and receiver's IP addresses in the header. These IP addresses serve as unique and universal identifiers for each device.

Transport Layer

The Transport Layer serves as a bridge between the Application Layer and the Network Layer, offering services to the former and receiving services from the latter. At this layer, data is referred to as "Segments." Its primary responsibility is to ensure the complete end-to-end delivery of messages. Additionally, it provides acknowledgment for successful data transmission and retransmits data in case of errors.

Sender's Side: The Transport Layer receives formatted data from higher layers, segments the data, and implements flow and error control to guarantee proper transmission. It also includes source and destination port numbers in the header and forwards segmented data to the Network Layer.

Key Functions of the Transport Layer:

1.Segmentation and Reassembly: This layer takes messages from the Session Layer, breaks them into smaller units, and attaches a header to each segment. At the receiving end, the Transport Layer reassembles the message from these segments.
2.Service Point Addressing: To ensure the message reaches the correct process, the Transport Layer's header includes a service point address or port address. This ensures precise delivery to the intended process.

Services Provided by the Transport Layer:

1.Connection-Oriented Service: This involves a three-phase process: connection establishment, data transfer, and termination/disconnection. It's characterized by the receiver acknowledging the receipt of packets, making it a reliable and secure mode of transmission.
2.Connectionless Service: This is a one-phase process that includes only data transfer. In this mode, the receiver doesn't send acknowledgments for received packets, allowing for faster communication between devices. However, it's less reliable compared to connection-oriented service.

Session Layer

The Session Layer plays a crucial role in managing connections, sessions, authentication and security in network communication.

Key Functions of the Session Layer:

1.Session Establishment, Maintenance, and Termination: This layer enables two processes to set up, maintain, and end a connection. It's responsible for the initiation and closure of communication sessions.

2.Synchronization: The Session Layer allows processes to insert checkpoints within data streams, serving as synchronization points. These points help identify errors and ensure proper re-synchronization, preventing data from being prematurely cut and minimizing data loss.
3.Dialog Controller: The Session Layer lets two systems commence communication, whether in a half-duplex or full-duplex mode, allowing for effective back-and-forth interaction between them.

Presentation Layer

The Presentation Layer, also known as the Translation Layer, focuses on transforming data from the Application Layer into a suitable format for network transmission.

Key Functions of the Presentation Layer:

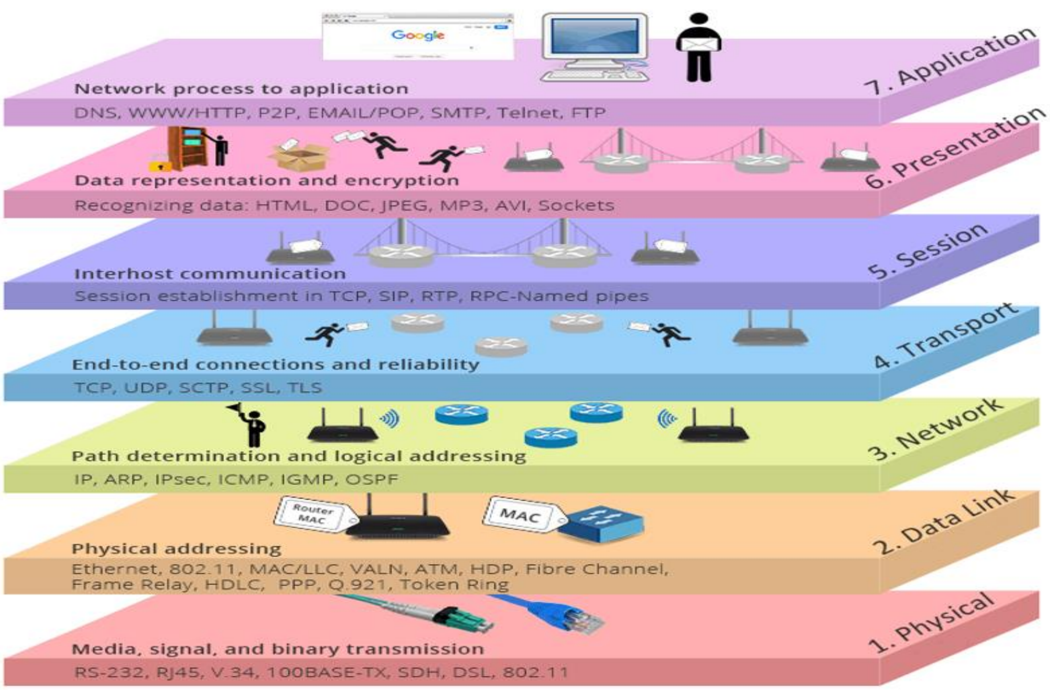
1.Translation: This layer can convert data between different formats, such as from ASCII to EBCDIC, ensuring data compatibility between sender and receiver.
2.Encryption/Decryption: Data encryption involves translating data into a different code, making it secure for transmission. The encrypted data is known as ciphertext, and it can be transformed back into plaintext using a key value, ensuring data security.
3.Compression: The Presentation Layer reduces the number of bits required for transmission on the network, making data transfer more efficient and faster.

Application Layer

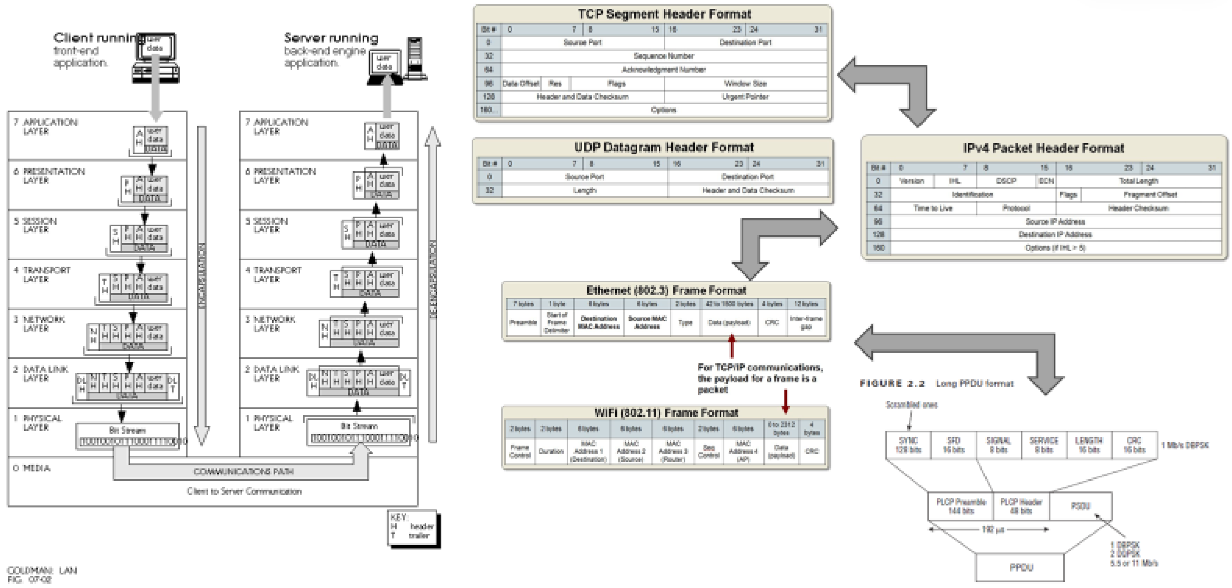
At the highest point in the OSI Reference Model's layer stack, we encounter the Application Layer, which is managed by network applications. These applications generate the data that needs to be sent across the network. Additionally, this layer acts as a gateway for application services to interact with the network and for presenting received information to users.

Key Functions of the Application Layer:

1.Network Virtual Terminal: This feature permits a user to log in to a remote host, effectively creating a virtual connection to a remote computer.
2.FTAM (File Transfer Access and Management):FTAM allows users to access files on a remote host, retrieve files from a remote host, and control or manage files located on a remote computer.
3.Mail Services: This application layer provides email services, allowing users to send, receive, and manage electronic mail.
4.Directory Services: This application is responsible for offering distributed database sources and access, enabling users to obtain global information about various objects and services.



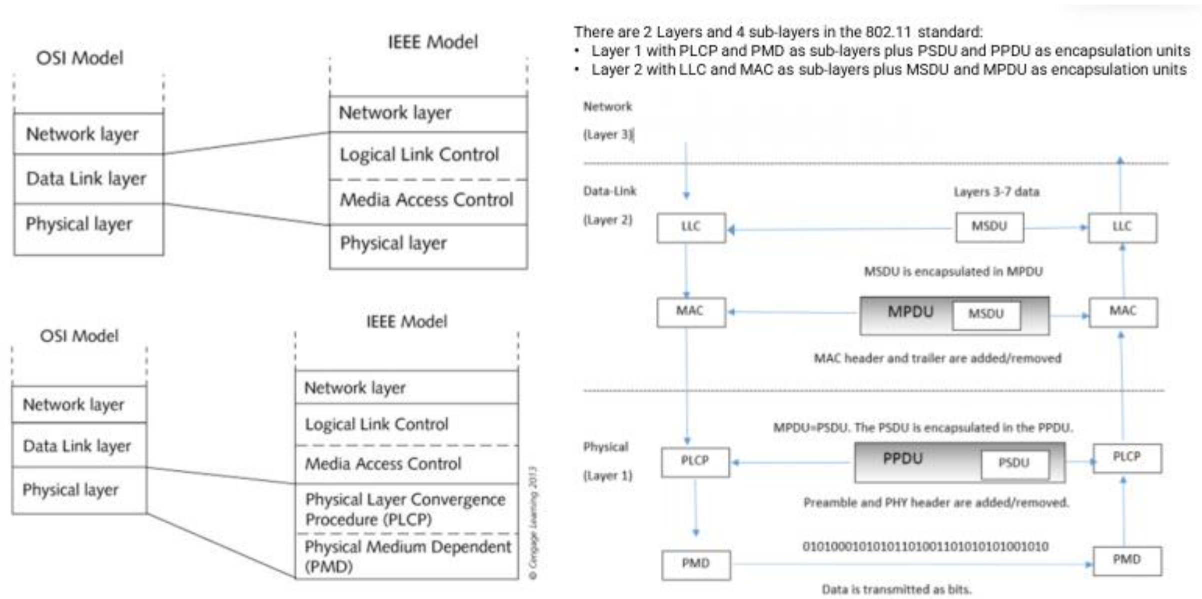
Segment/Packet/Frame Headers/Encapsulation:



In networking, the communication process involves the division of data into smaller units, often referred to as segments, packets, or frames, depending on the layer of the OSI model in which they are operating. These units serve as carriers for the data. To ensure the successful transmission and reception of data, each unit is accompanied by a header that contains vital information. These headers are added at each layer as data moves from higher layers to lower layers.

- **At the Application Layer (Layer 7)**, data is divided into segments. Segments include the application-specific data and a segment header. This header often contains source and destination port numbers, as well as a sequence number for reordering the segments at the receiving end.
- **In the Transport Layer (Layer 4)**, segments are further divided into packets. Packets include the transport layer header, which typically holds information like the source and destination port numbers, as well as the error-checking information, which is essential for the recipient to verify the data's integrity.
- **At the Network Layer (Layer 3)**, packets are encapsulated into frames. Frames have a frame header that contains source and destination IP addresses, among other information. These IP addresses enable routing to the correct destination across different networks.
- **The Data Link Layer (Layer 2)** further encapsulates frames into bits, ready for physical transmission. This layer adds a frame header and trailer, which include source and destination MAC addresses, as well as error-checking information for ensuring that the data is received accurately.

The Wi-Fi Layers:



In the context of Wi-Fi communication, two primary layers in the OSI model are critical for understanding how data is transmitted wirelessly.

1.Data Link Layer (Layer 2):

This layer is often subdivided into two sub-layers:

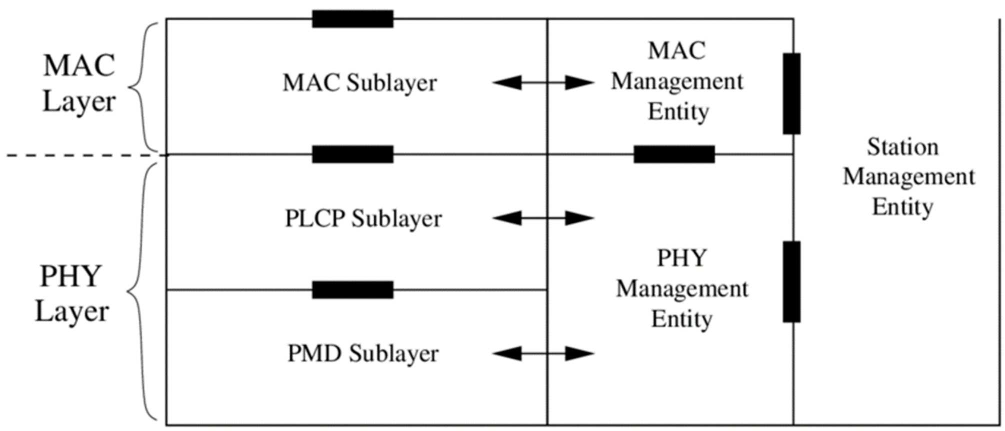
- Logical Link Control (LLC) Layer: The LLC sub-layer is responsible for managing logical addressing and error control. It ensures that data is correctly transmitted between connected devices, independent of the specific medium used.
- Medium Access Control (MAC) Layer: The MAC sub-layer controls access to the shared wireless medium. It handles aspects like channel access methods, frame transmission, and dealing with contention on the wireless network. Different wireless technologies may use various MAC protocols, such as CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) in Wi-Fi.

2.Physical Layer (Layer 1):

The Physical Layer also consists of two sub-layers:

- PLCP (Physical Layer Convergence Procedure) Layer: The PLCP sub-layer deals with the actual modulation and demodulation of signals. It ensures that data from the MAC layer is appropriately encoded for wireless transmission and decoded at the receiver.
- PMD (Physical Medium Dependent) Layer: The PMD sub-layer is responsible for managing the physical characteristics of the wireless medium, which can include radio frequencies, signal propagation, and modulation techniques. It adapts the data for successful transmission over the specific wireless medium being used, whether it's radio waves in the case of Wi-Fi or other wireless technologies.

Wi-Fi Physical Layer



The physical layer serves as the foundation upon which data is transmitted and received. This layer involves intricate processes facilitated by sublayers such as PLCP (Physical Layer Convergence Protocol) and PMD (Physical Medium Dependent). This discussion aims to shed light on these sublayers, unraveling their roles and significance in the transmission of data across networks.

The physical layer is divided into two sublayers:

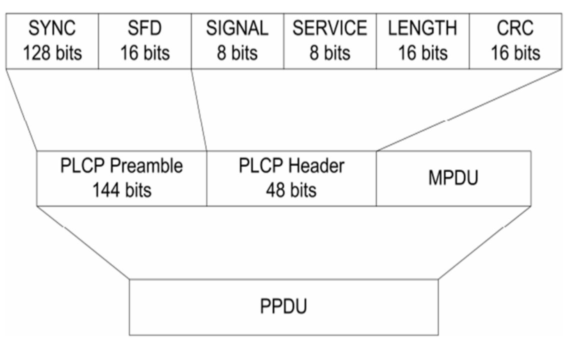
- **PLCP Sublayer: Adding Intelligence to Data Transmission:** Within the physical layer, the PLCP sublayer stands as a crucial element. PLCP, short for Physical Layer Convergence Protocol, operates at the interface between the MAC (Media Access Control) layer and the physical layer. Its primary responsibility lies in adding essential physical layer headers to MAC frames. These headers include preamble, synchronization bits, and other vital information. By incorporating this intelligence into data frames, PLCP ensures seamless communication between devices.
- **PMD Sublayer: Ensuring Efficient Transmission:** Parallelly, the PMD sublayer, or Physical Medium Dependent sublayer, takes center stage in the transmission process. PMD is accountable for the actual transmission of signals over the physical medium, be it through copper cables, fiber optics, or wireless channels. Its role is to convert digital data into

signals suitable for the specific physical medium in use, ensuring that the data reaches its destination accurately and efficiently.

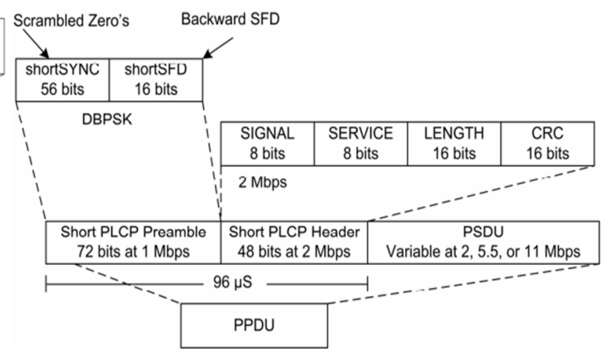
- **Synchronization and Collaboration:** The harmonious collaboration between the PLCP and PMD sublayers is essential for successful data transmission. PLCP prepares the data for transmission by adding necessary information, while PMD converts this data into signals appropriate for the physical medium. This synchronization ensures that data travels across networks reliably, enabling seamless communication between devices.

PLCP Protocol Data Unit (PPDU) Frame Formats

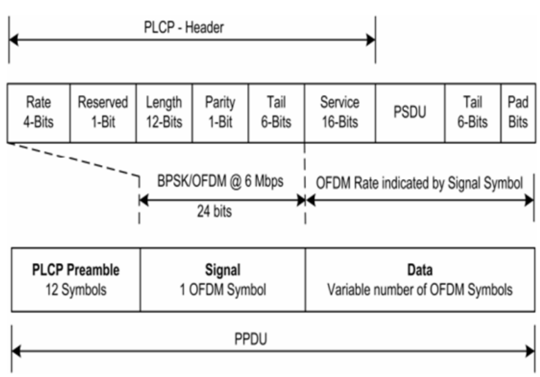
DSSS PPDU, 802.11-1999 (R2003)



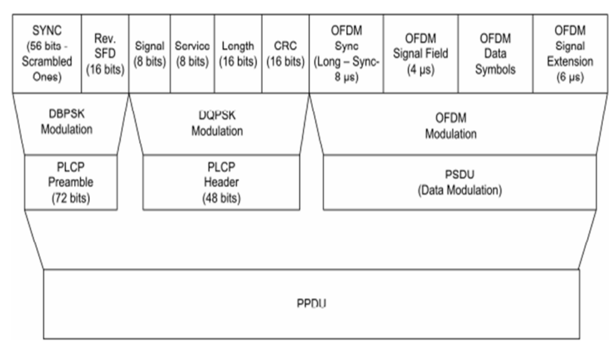
802.11b, DSSS PPDU, Short Preamble



ERP-OFDM PPDU (802.11a/g)



802.11g, DSSS-OFDM PPDU, Short Preamble



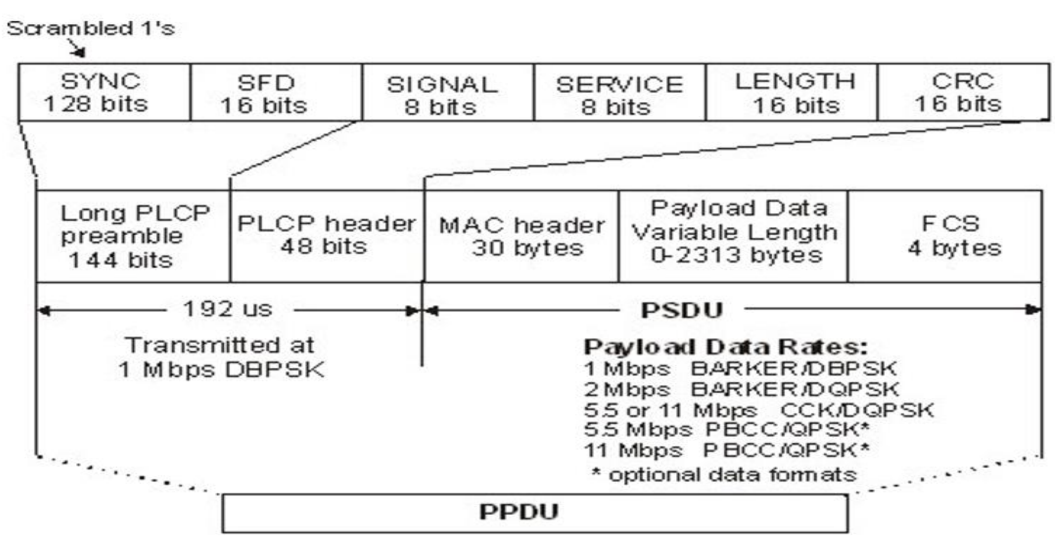
PLCP (Physical Layer Convergence Protocol) Protocol Data Unit (PPDU) Frame Format:

When examining the PLCP Protocol Data Unit (PPDU) frame format, it's important to understand that it consists of two main components: the preamble and the PLCP header. These components play a crucial role in the transmission of data over different network technologies.

- **Preamble:** The Preamble is a vital part of the PPDU frame format. It serves as an introduction to the data to be transmitted and helps in the synchronization of communication between devices. The Preamble typically includes synchronization bits and other essential information to prepare the receiver for the incoming data.

- **PLCP Header:** The PLCP header, standing for Physical Layer Convergence Protocol header, is the second part of the PPDU frame format. It contains important information related to the data being transmitted. This information helps the receiving device interpret and process the incoming data accurately.
- **Variations in PPDU Frame Formats:** It's crucial to note that different network technologies, such as Direct Sequence Spread Spectrum and various versions of Orthogonal Frequency Division Multiplexing (OFDM), may have distinct PPDU frame formats. These variations in frame formats are necessary to cater to the unique requirements and characteristics of each technology. The specific details of these variations can be complex and depend on the technology in use.
- **The Importance of Header Elements:** The header of a PPDU frame format, comprising the preamble and PLCP header, is essential for successful communication between devices. The preamble aids in synchronization, ensuring that the receiver is prepared to receive data. The PLCP header contains critical information that allows the receiver to interpret the data accurately, such as data rate, modulation scheme, and other necessary parameters.

802.11b PLCP Frame Format



IEEE std 802.11b PPDU frame with Long PLCP Preamble

t

PLCP Header in Networking

- The PLCP header is an essential component in networking, responsible for conveying crucial information about data transmission.

Components of the PLCP Header:

1.Preamble:

- Consists of both a long preamble and a short preamble.
- Used for synchronization and to prepare the receiver for incoming data.

2. Signal Field:

- Describes the modulation type to be used for the payload.
- The header provides the receiver with information on how the data has been coded and modulated.
- This field defines what type of modulation must be used to receive the incoming PSDU.
  00001010 – 1 Mbit/s , 00010100 – 2 Mbit/s, 00111110 – 5.5 Mbit/s, 01101110 – 11 Mbit/s

3. Payload:

- Comprises a sequence of bits that have been modulated using various coding mechanisms.
- The signal field specifies the modulation and coding rate used in the payload.

4. Service Field:

- Part of the PLCP header.
- Serves a specific purpose, potentially related to services in the network.
- Three bits of the service field are used by 802.11b . The rest of the service field bits are zero
  Bit 2 – determines whether the transmit frequency and symbol clocks use the same oscillator
  Bit 3 – indicates whether CCK or PBCC is used (PBCC was a competing technology by TI to CCK – however it was rejected by the 802.11 standards committee)
  Bit 7 – bit 7 of the service field is used with the Length field to determine the time in microseconds.

5. Length Field:

- Indicates the duration of the frame in microseconds.
- Helps in coordinating data transmission timings.
- It is an unsigned 16- bit integer that indicates the number of microseconds necessary to transmit the PSDU

6.CRC (Cyclic Redundancy Check):

- Used for error checking.
- Ensures data integrity during transmission.

7.SYNC

- The SYNC field is used by the receiver to acquire the incoming signals and to synchronize the receiver's carrier tracking and timing prior to receiving SFD

8.SFD

- (Start of Frame Delimiter) contains information regarding the start of a PPDU frame. The SFD is F3A0hex for the long preamble and the bit reversed value 0x05CF hex for the Short Preamble

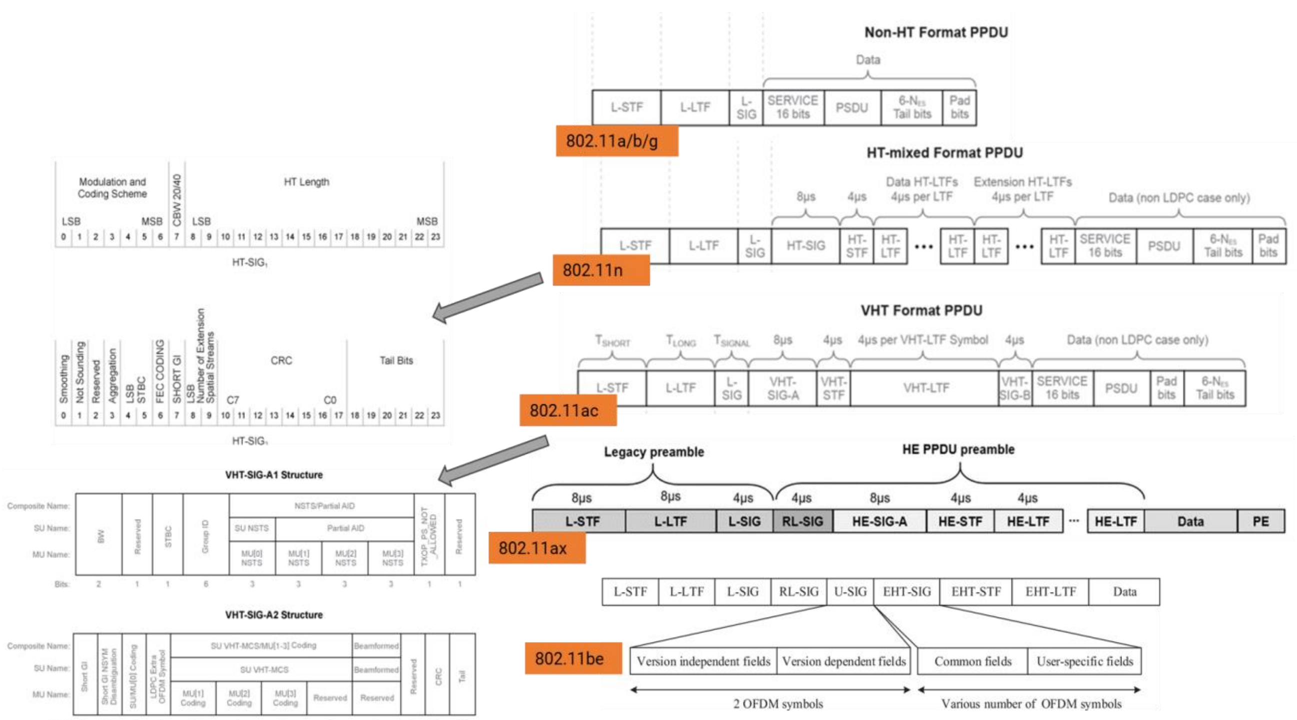
Significance of the PLCP Header:

- The signal field in the header informs the receiver about the modulation and coding rate used in the payload.
- This information enables the receiver to demodulate and decode the incoming data correctly.
- The header is crucial for ensuring that data is transmitted and received accurately in a Network.

PHY Frame Format for Various Standards

1. Legacy Fields in Wi-Fi Protocols: Starting from the ABG protocol to the more recent standards like 11n, 11ac, and 11ax, legacy fields remain a crucial aspect of the PHY protocol data unit (PPDU).

2. Evolution of Wi-Fi Standards: With the introduction of each new standard, additional complexities and features have been incorporated, such as MIMO, guard intervals, Space-Time Block Coding, aggregation, beamforming, and multi-user support.
3. Incorporation of New Fields: The headers of the newer standards include information about these new features and technologies, expanding the scope and capabilities of Wi-Fi networks.



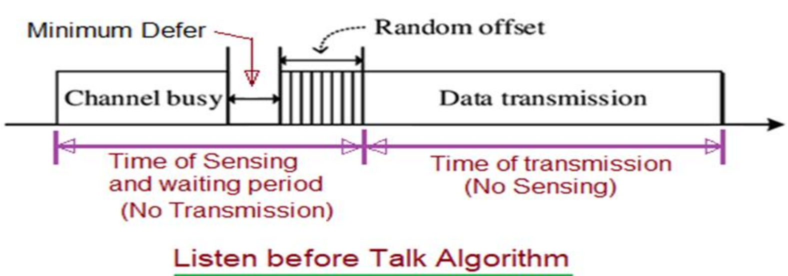
Source: https://www.mathworks.com/help/wlan/gs/wlan-ppdu-structure.html

4. Backward Compatibility Requirement: The persistence of legacy fields is essential to ensure backward compatibility. Newer devices and access points must communicate effectively with older devices that might not understand the new signal fields.

5. Legacy Protection Mechanism: The inclusion of legacy fields enables devices to communicate effectively across different versions of the Wi-Fi standard, similar to how a teacher in a multilingual classroom might first communicate the intention to switch to a local language, ensuring everyone can follow the conversation.

Understanding the importance of legacy fields in Wi-Fi protocols helps ensure seamless communication between devices, even in mixed networks with different Wi-Fi standards.

Clear Channel Assessment (CCA)



1. Purpose of Clear Channel Assessment (CCA): CCA is a critical function in Wi-Fi networks as it helps devices assess whether the channel is available for transmission or if there's any data to be received.

2.Understanding the Medium in Wi-Fi: Unlike cellular technologies that allocate specific time slots for communication, Wi-Fi functions as a shared medium. Hence, CCA ensures that devices follow a "listen before you talk" protocol.

3. Importance of Half Duplex in Wi-Fi: Wi-Fi being half duplex implies that devices cannot transmit and receive simultaneously. The CCA process helps avoid collisions by allowing devices to check the channel's availability before transmission.

4. Signal Detect (SD) and Energy Detect (ED) Thresholds: These thresholds help devices determine whether the received signal-to-noise ratio is sufficient for reception (SD) of 802.11 frames. On the other hand, ED helps detect the presence of any energy above the SD level, indicating that the medium might already be in use due to noise.

5. ED and SD in Wi-Fi Layer: These parameters are essential components of the Physical Medium Dependent (PMD) layer. They aid in the Clear Channel Assessment process, helping devices decide when to receive data and when to back off during transmission.

Understanding Clear Channel Assessment is vital for ensuring efficient communication and preventing collisions within a Wi-Fi network, ultimately leading to enhanced network performance and reliability.