Wi-Fi Technology Fundamentals

WI-FI TECHNOLOGY
FUNDAMENTALS COURSE

Module-2

WLAN Physical Layer

Session-2d

PHY Headers, Frame Formats and Key Functions

Last Session Recap……

Module-2

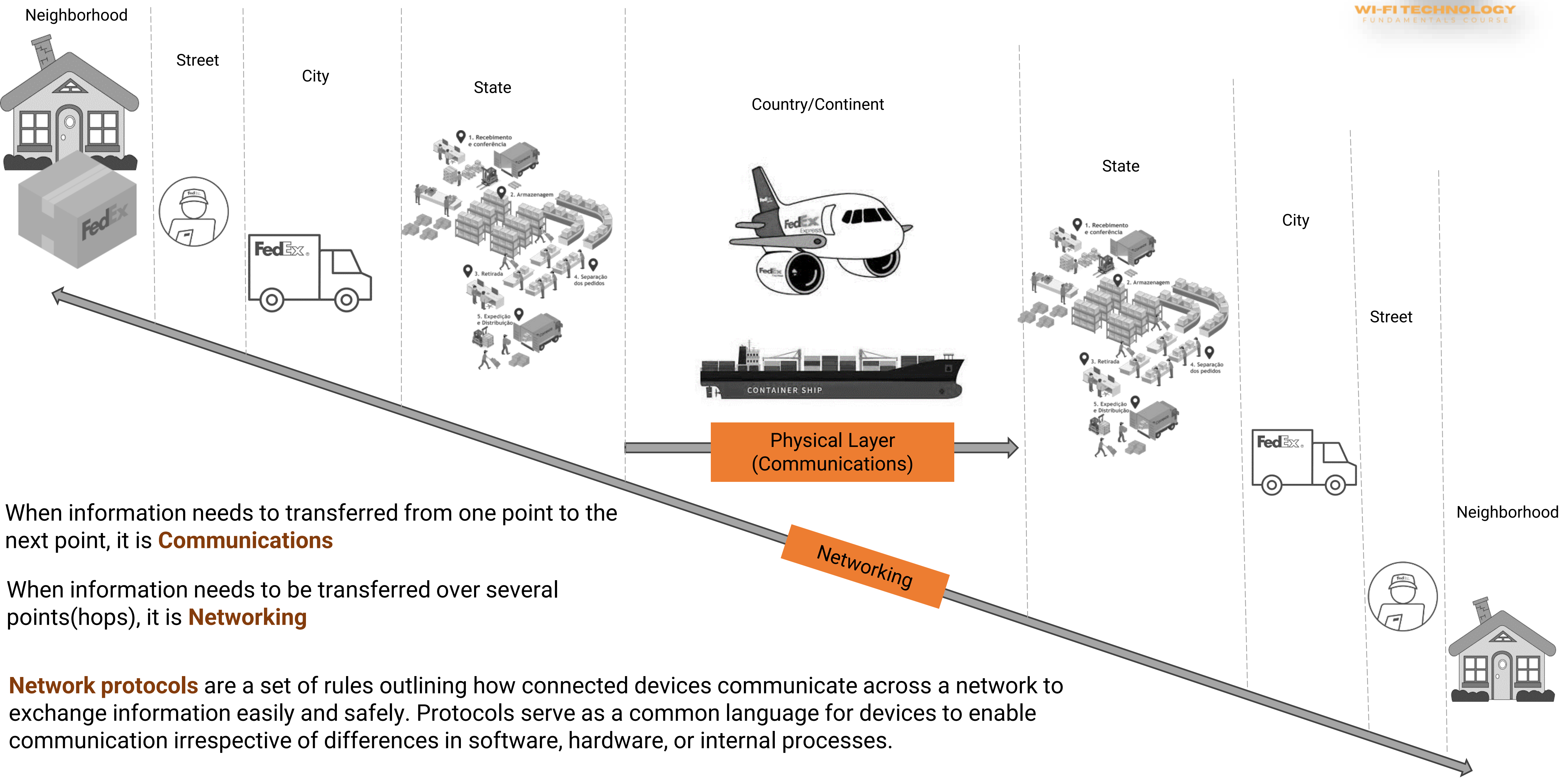
WLAN Physical Layer

Session-2c

MCS Table / PHY Data Rates

- ✓ MCS table data rates for all standards
- ✓ Modulation, Coding, BW, Number of Spatial Streams, Guard Interval
- ✓ Theoretical Throughput
- ✓ Demo of Throughput achieved with different client types.

From Communications to Networking

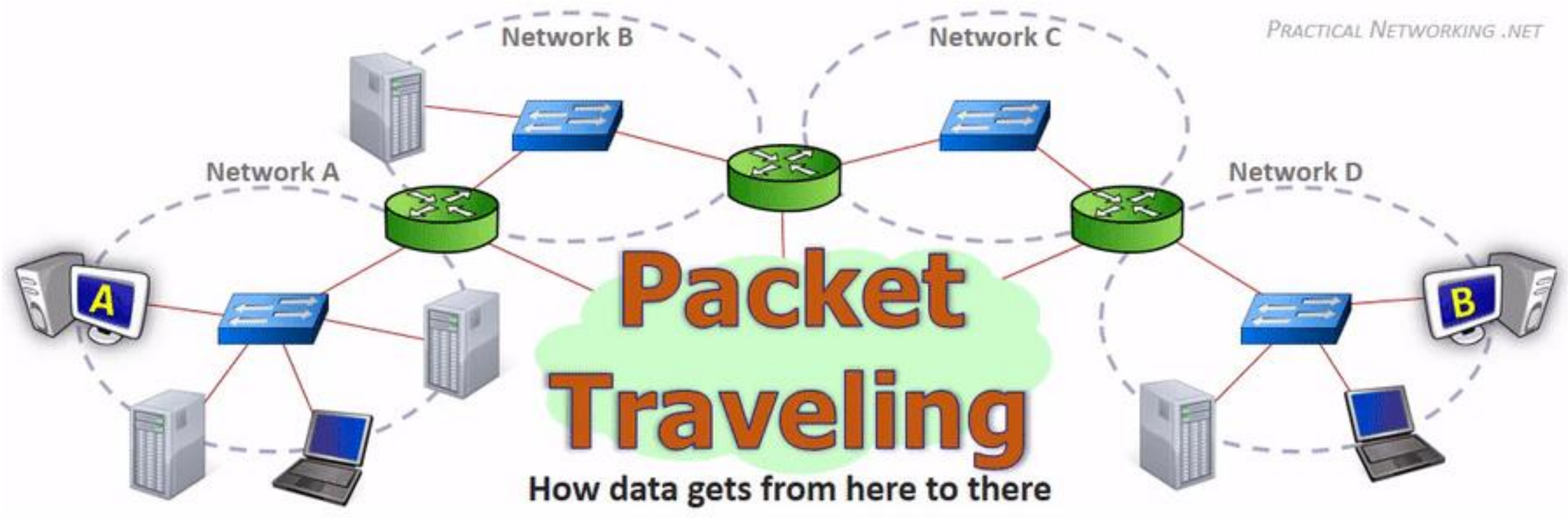


When information needs to transferred from one point to the next point, it is **Communications**

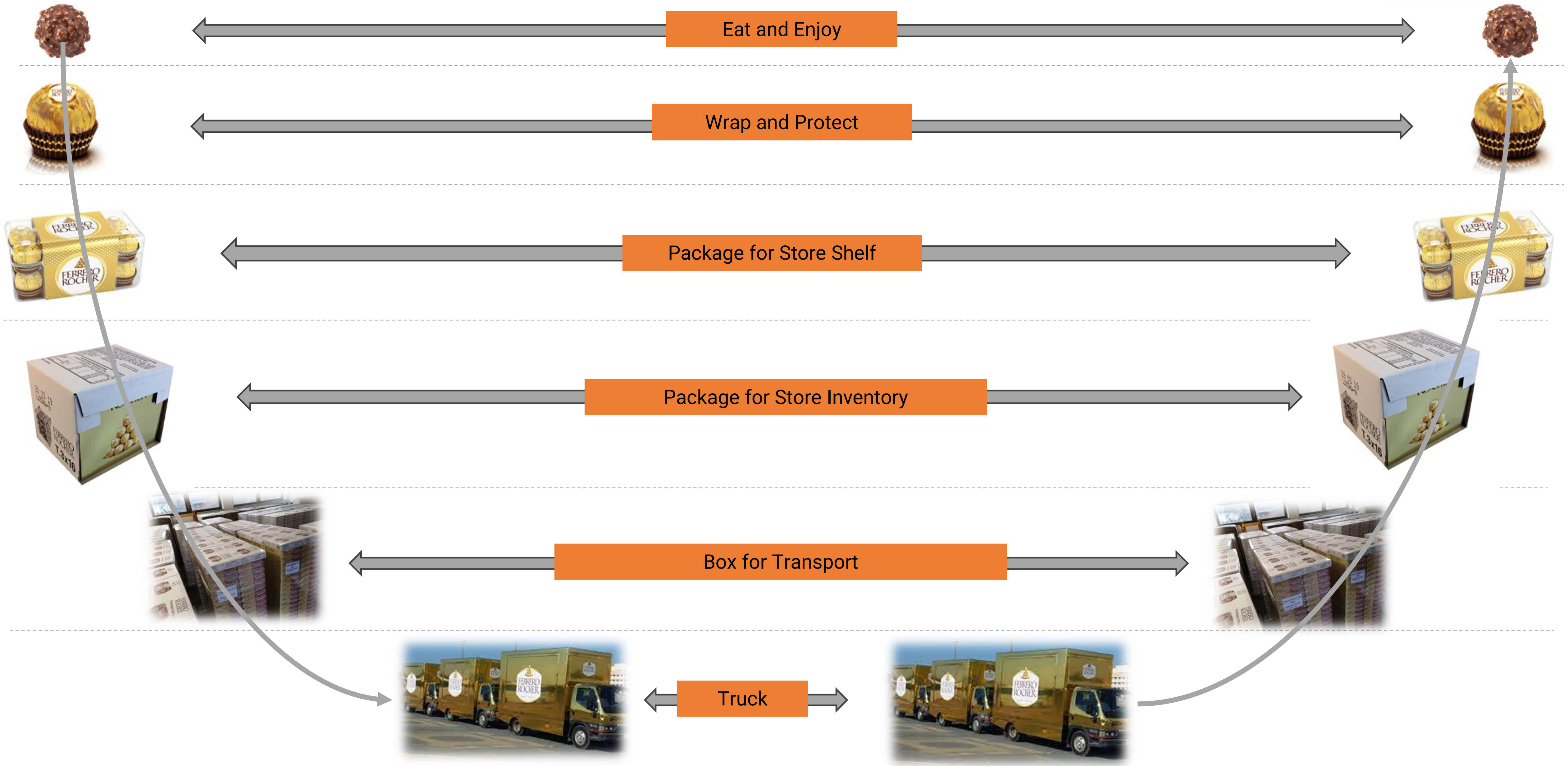
When information needs to be transferred over several points(hops), it is **Networking**

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.

Path of a Packet on the Internet



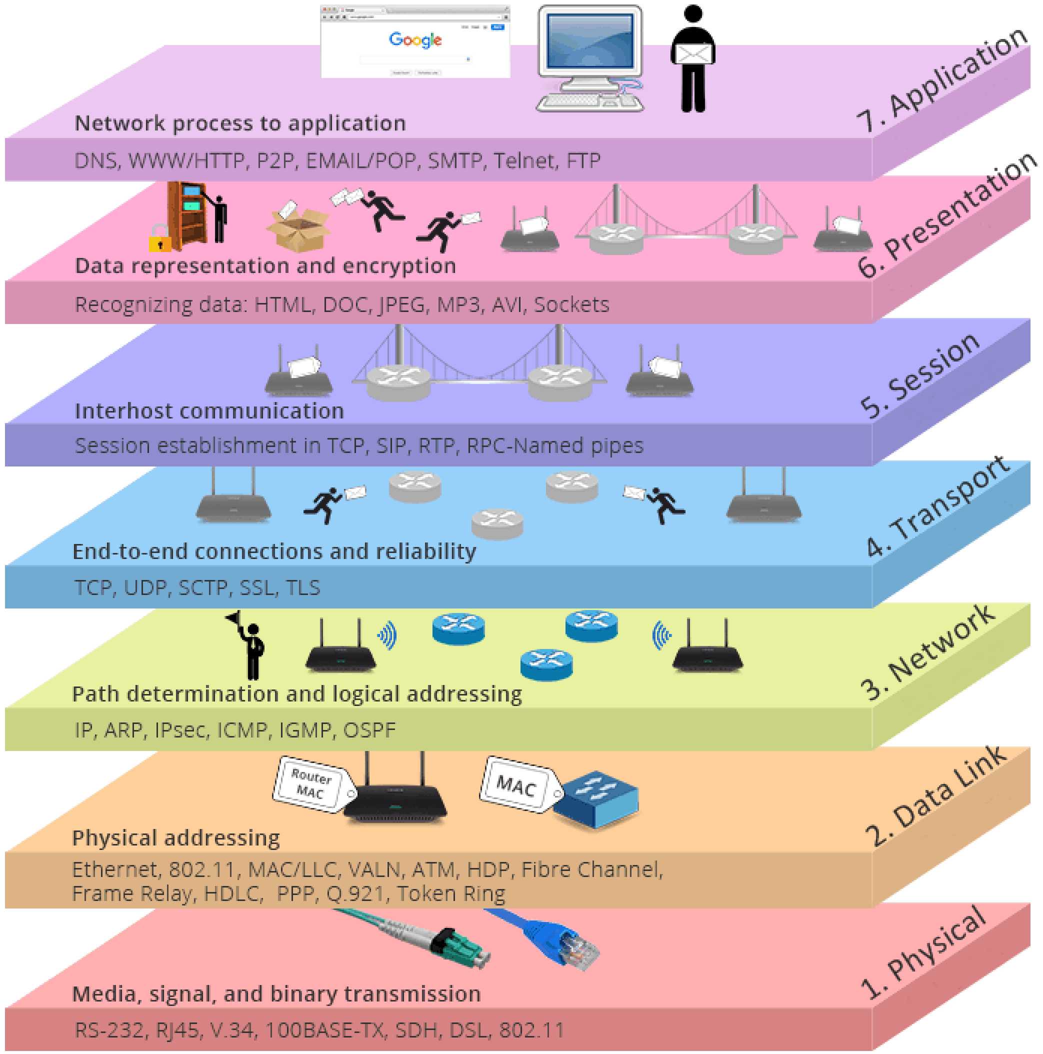
Why Layers?


Eat and Enjoy
Wrap and Protect
Package for Store Shelf
Package for Store Inventory
Box for Transport
Truck

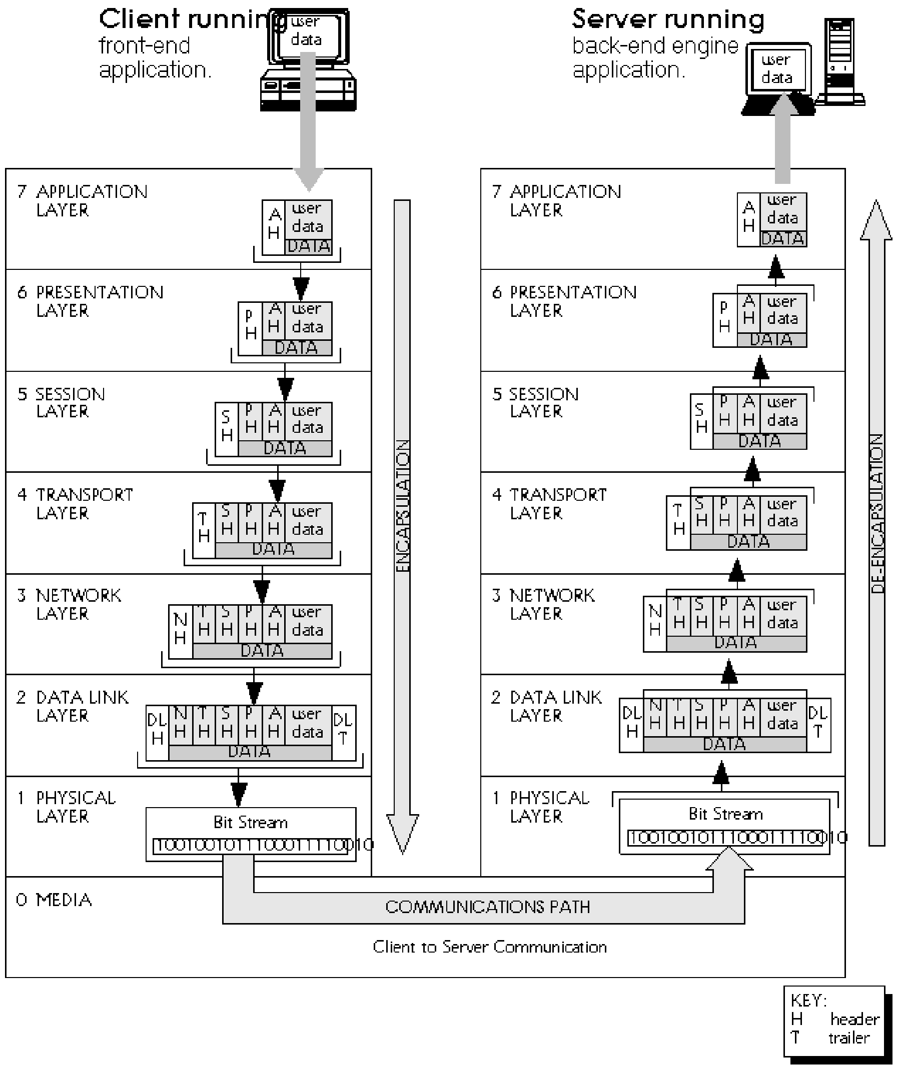
OSI Network Layers

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		GATEWAY 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	TCP/SPX/UDP	PACKET FILTERING		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**			



Segment/Packet/Frame Headers/Encapsulation



GOLDMAN: LAN
FIG. 07-02

TCP Segment Header Format

Bit #	0 – 7	8 – 15	16 – 23	24 – 31
0	Source Port		Destination Port	
32	Sequence Number			
64	Acknowledgment Number			
96	Data Offset / Res	Flags	Window Size	
128	Header and Data Checksum		Urgent Pointer	
160...	Options			

UDP Datagram Header Format

Bit #	0 – 7	8 – 15	16 – 23	24 – 31
0	Source Port		Destination Port	
32	Length		Header and Data Checksum	

IPv4 Packet Header Format

Bit #	0 – 7	8 – 15	16 – 23	24 – 31
0	Version / IHL	DSCP / ECN	Total Length	
32	Identification		Flags / Fragment Offset	
64	Time to Live	Protocol	Header Checksum	
96	Source IP Address			
128	Destination IP Address			
160	Options (if IHL > 5)			

Ethernet (802.3) Frame Format

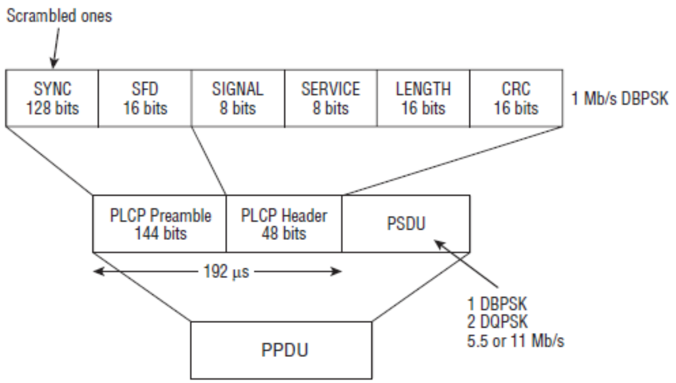
7 bytes	1 byte	6 bytes	6 bytes	2 bytes	42 to 1500 bytes	4 bytes	12 bytes
Preamble	Start of Frame Delimiter	**Destination MAC Address**	**Source MAC Address**	Type	Data (payload)	CRC	Inter-frame gap

For TCP/IP communications, the payload for a frame is a packet

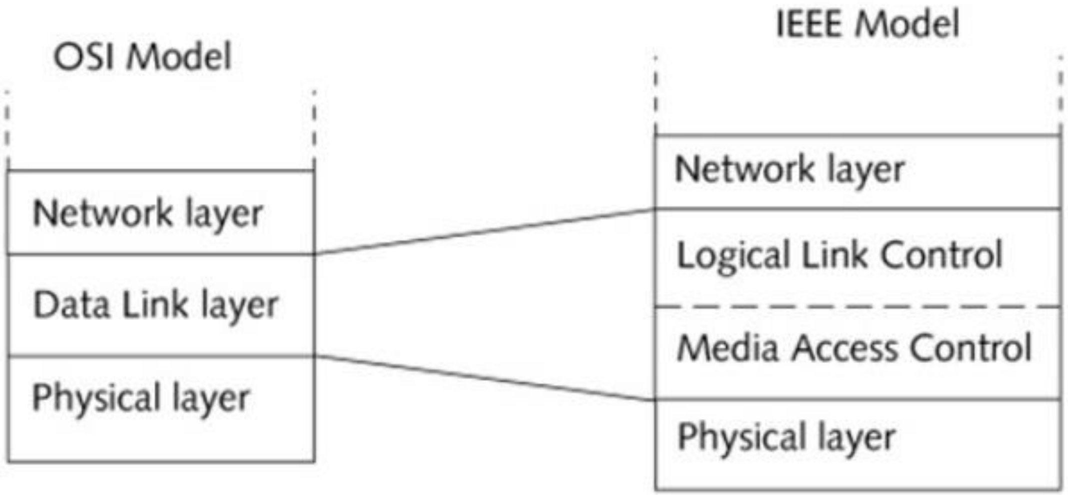
WiFi (802.11) Frame Format

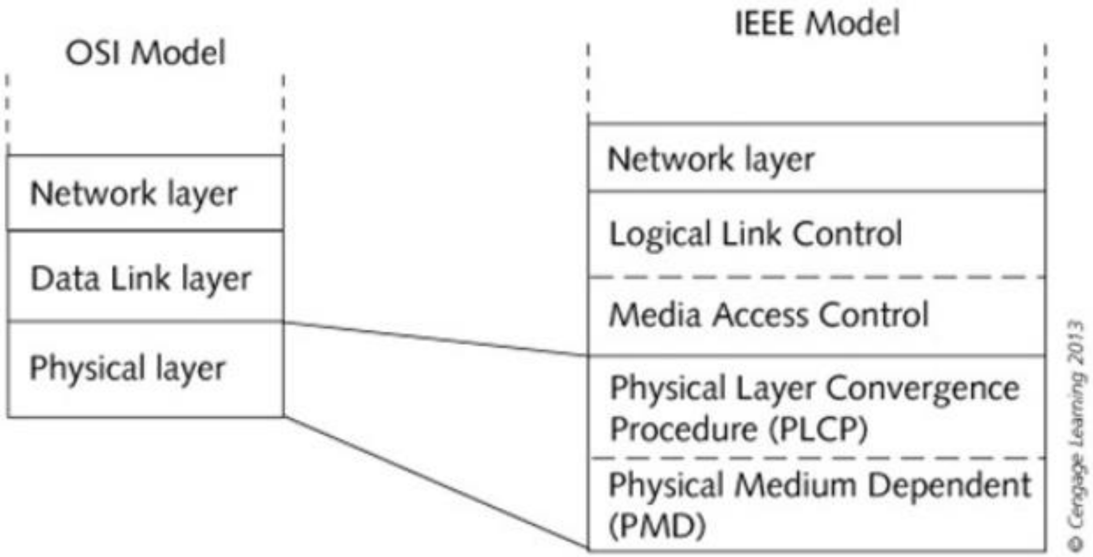
2 bytes	2 bytes	6 bytes	6 bytes	6 bytes	2 bytes	6 bytes	0 to 2312 bytes	4 bytes
Frame Control	Duration	MAC Address 1 (Destination)	MAC Address 2 (Source)	MAC Address 3 (Router)	Seq Control	MAC Address 4 (AP)	Data (payload)	CRC

FIGURE 2.2 Long PPDU format



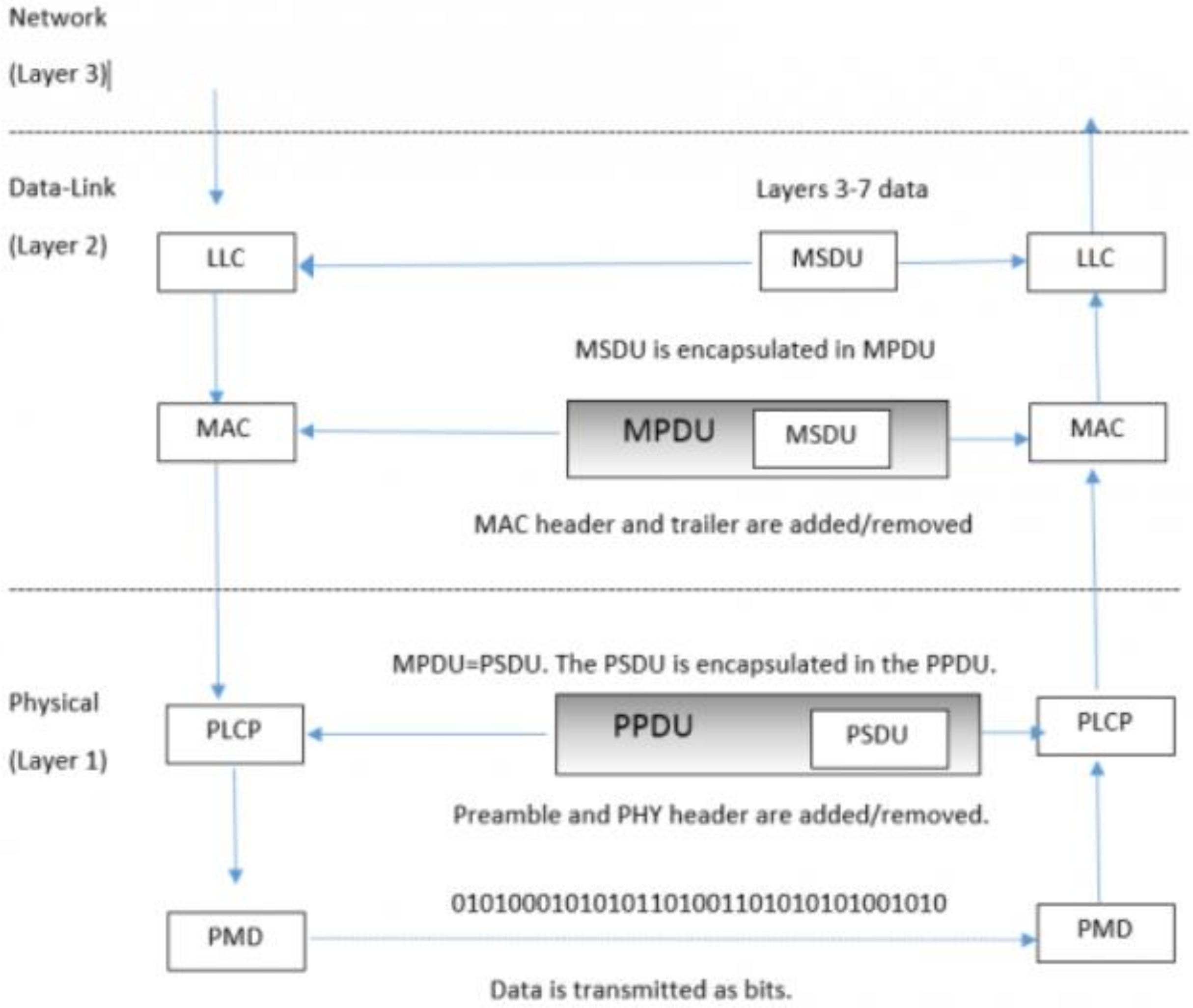
The Wi-Fi Layers





There are 2 Layers and 4 sub-layers in the 802.11 standard:

- Layer 1 with PLCP and PMD as sub-layers plus PSDU and PPDU as encapsulation units
- Layer 2 with LLC and MAC as sub-layers plus MSDU and MPDU as encapsulation units

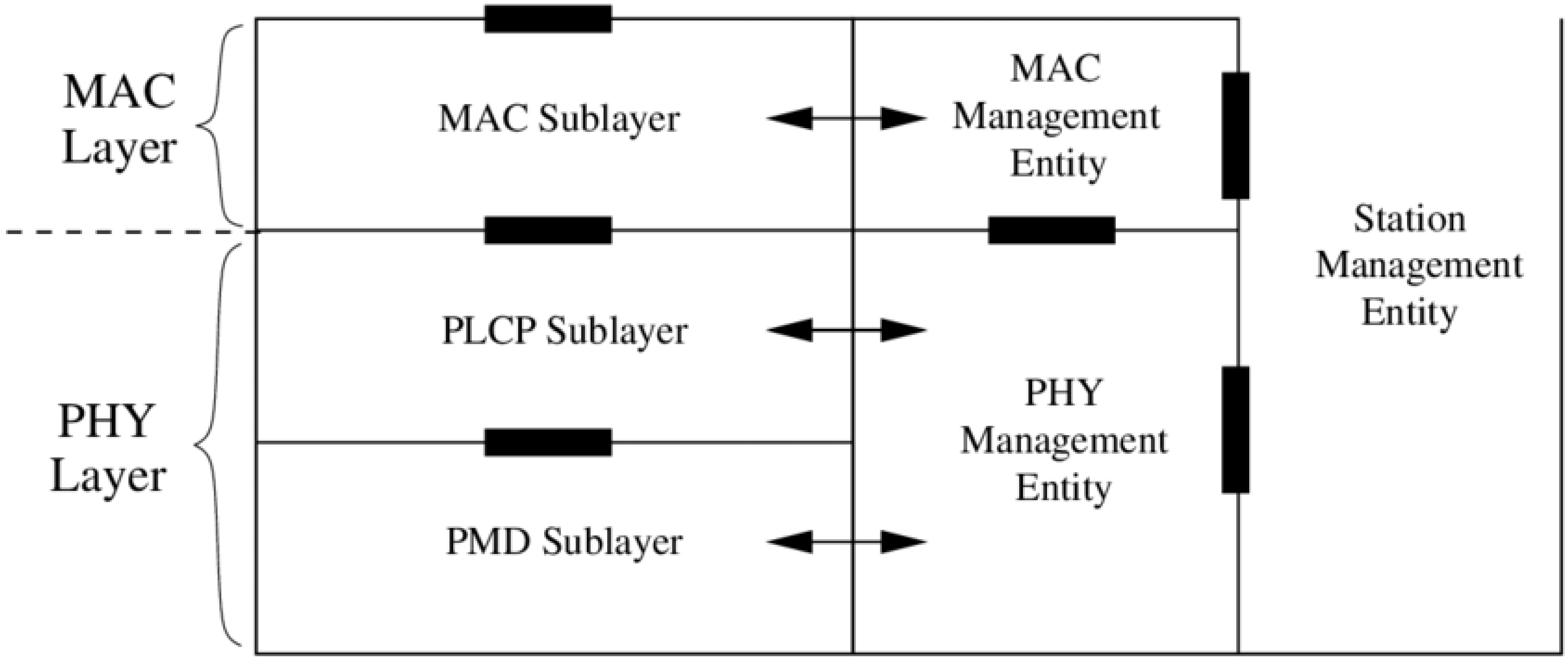


Wi-Fi Physical Layer

The physical layer is divided into two sublayers:

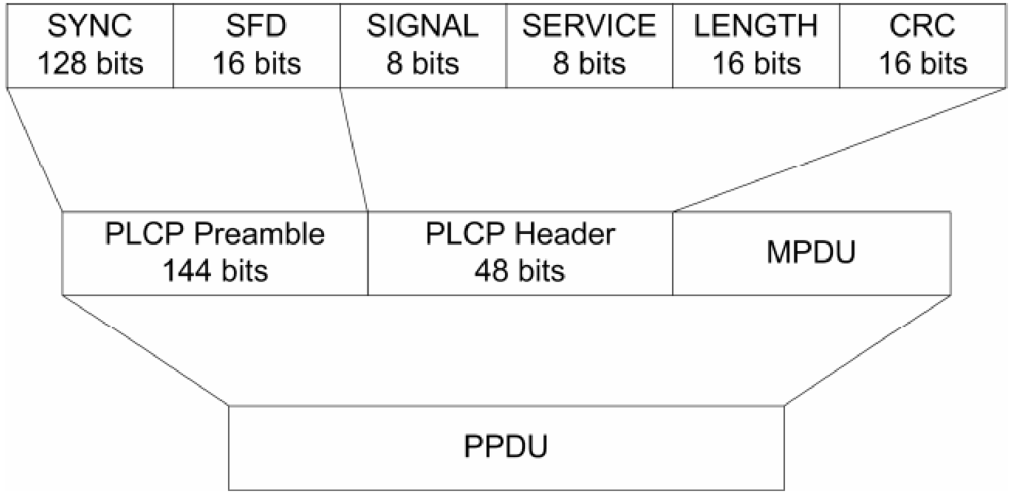
- **Physical Layer Convergence Procedure (PLCP)** sublayer
  - Adds PHY layer headers to MAC frame including preamble and other information
- **Physical Medium Dependent (PMD)** sublayer.
  - Responsible for transmitting any bits it receives from the PLCP into the air using the antenna

The physical layer also incorporates a clear channel assessment (CCA) function to indicate to the MAC when a signal is detected.

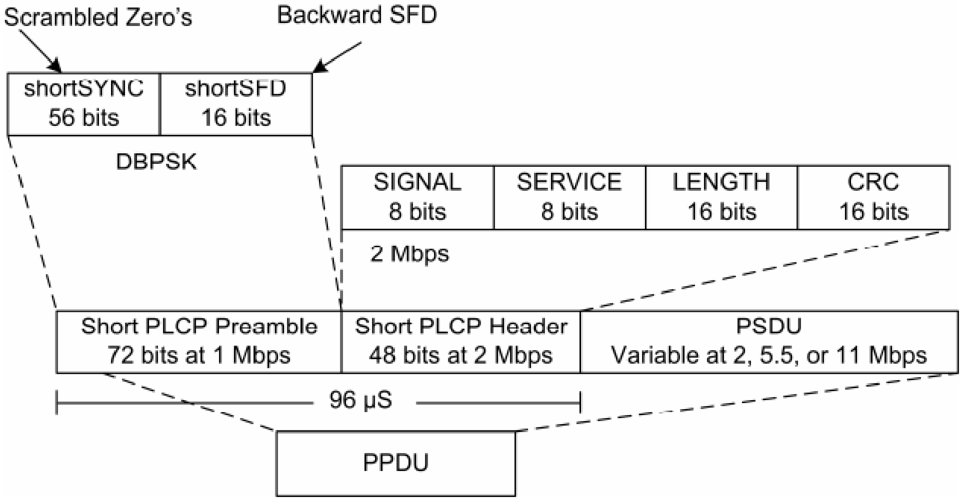


PLCP Protocol Data Unit (PPDU) Frame Formats

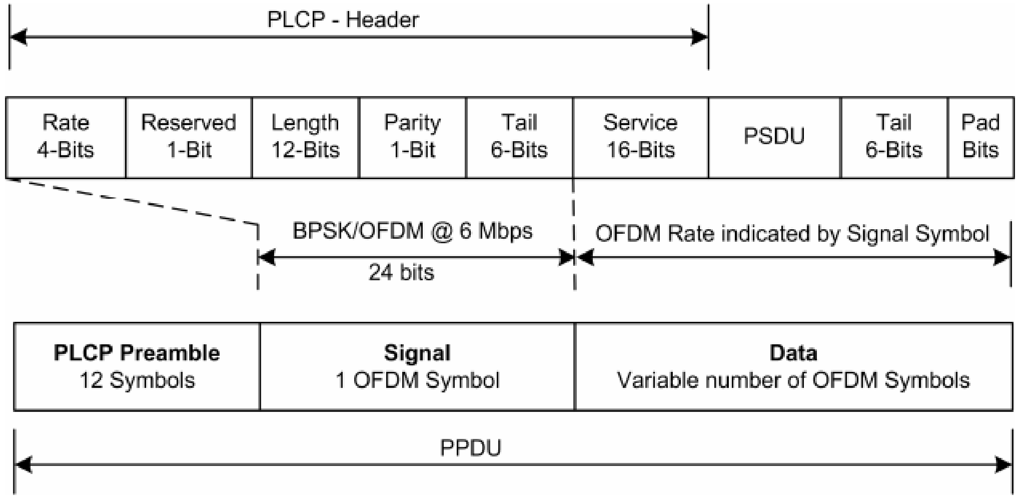
DSSS PPDU, 802.11-1999 (R2003)



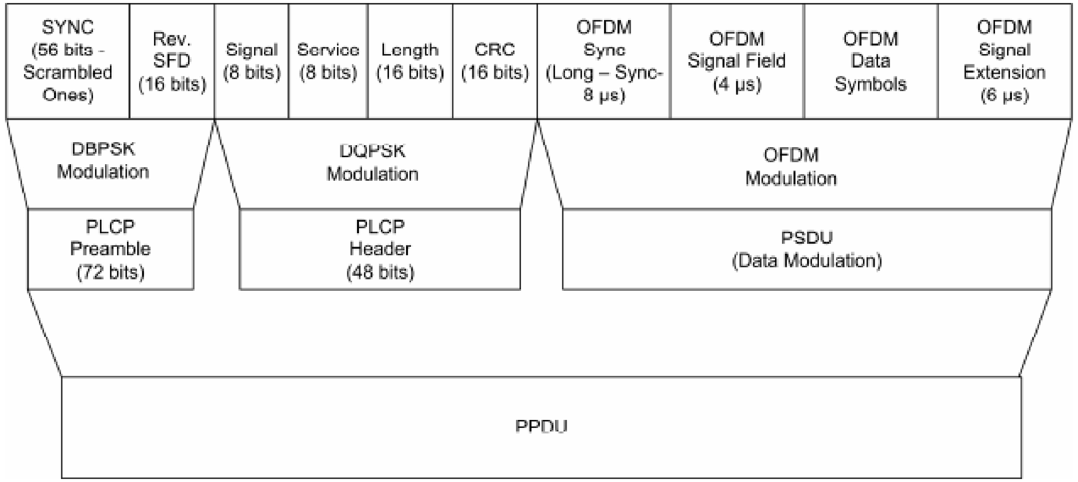
802.11b, DSSS PPDU, Short Preamble



ERP-OFDM PPDU (802.11a/g)



802.11g, DSSS-OFDM PPDU, Short Preamble

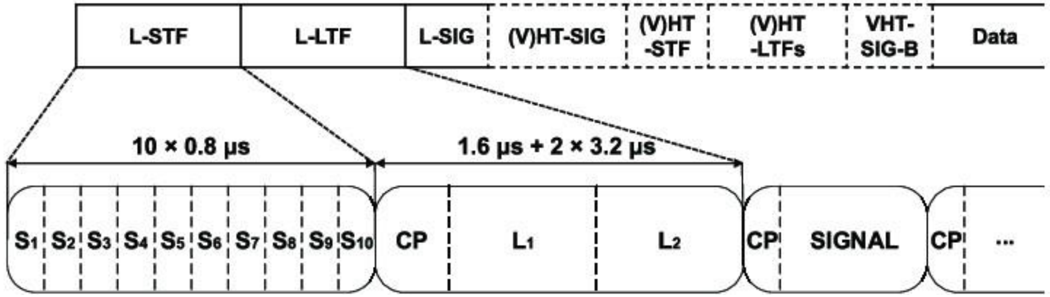


Concept of Preamble

The 802.11 Physical Layer uses bursted transmissions or packets. Each packet contains a Preamble, Header and Payload data

The preamble defines a series of transmission criteria that indicates when someone is preparing to transmit data. When the information begins to transmit, all systems must begin interpreting the start of the transfer at the right time

The Preamble allows the receiver to obtain time and frequency synchronization and estimate channel characteristics for equalization. It is a bit sequence that receivers watch for to lock onto the rest of the transmission



Ambulance Siren Preamble to emergency Situation

802.11 Preamble is divided into two portions.

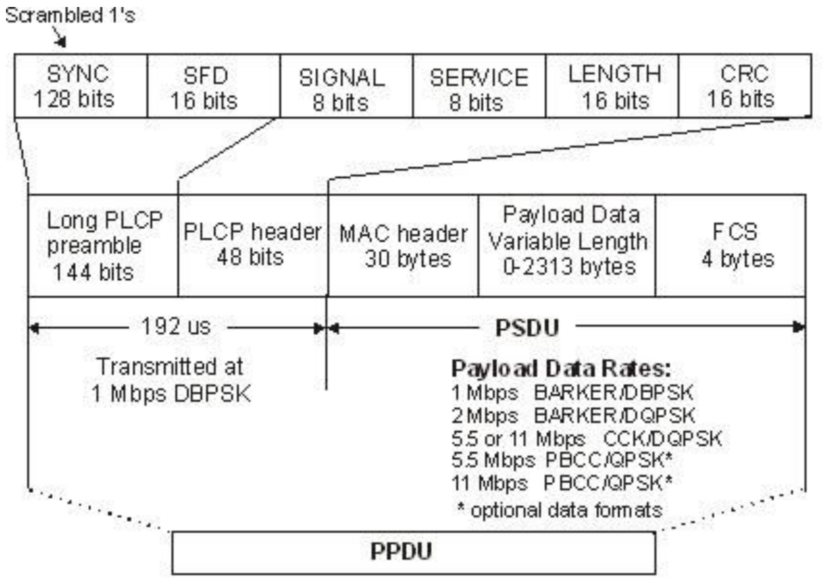
L-STF
The first is legacy short training field (L-STF), which consists of ten repetitions of a 0.8 μs short training symbol. This field, by virtue of its repetitive nature and good correlation properties, is utilized for: Frame detection, Automatic gain control (AGC), Symbol timing synchronization, Coarse frequency offset estimation

L-LTF
The other portion is legacy long training field (L-LTF), which contains two repetitions of a 3.2 μs long training symbol with a 1.6 μs Cyclic Prefix (CP). The main purposes of L-LTF are: Symbol timing synchronization, Fine frequency offset estimation, Channel estimation.

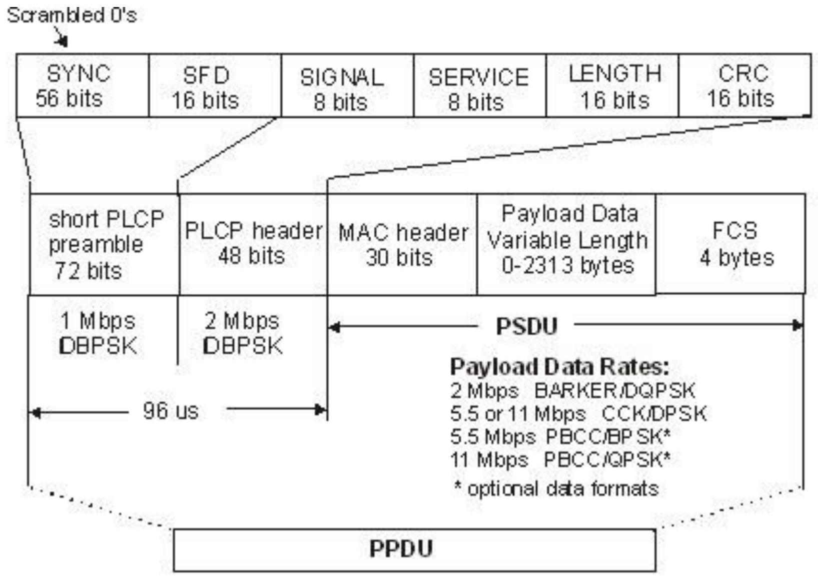
L-SIG
The L-SIG field is a symbol where each of the 48 data subcarriers is BPSK modulated. All stations on the channel read the Rate and Length information subfields and use this for different purposes. All of the receivers use this information to calculate the duration of time for this full-frame.

HT/VHT/HE preamble and Data field
Next after the legacy preamble, it is either the HT/VHT/HE preamble, if the frame is those frame types and the data field. Or only the data field (non-HT/ERP-OFDM).
Note: both managements-, control-, and data frames has the data field

802.11b PLCP Frame Format



IEEE std 802.11b PPDU frame with Long PLCP Preamble

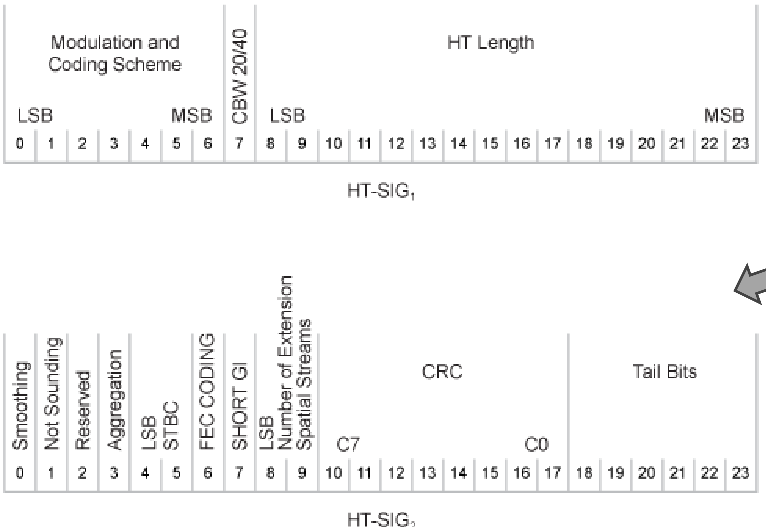


IEEE std 802.11b PPDU frame with Short PLCP Preamble

- **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
- **SFD** – (Start of Frame De-limiter) 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
- **SIGNAL** - field defines what type of modulation must be used to receive the incoming PSDU.
  - 00001010 – 1Mbit/s , 00010100 – 2 Mbit/s, 00111110 – 5.5 Mbit/s, 01101110 – 11 Mbit/s
- **SERVICE** - 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
- **LENGTH** – is an unsigned 16- bit integer that indicates the number of microseconds necessary to transmit the PSDU
- **CRC** – Cyclic Redundancy Check for Error Checking.

PHY Frame Format for Various Standards

Newer Standards adding more information about Beamforming, new coding techniques, Multi-User etc…

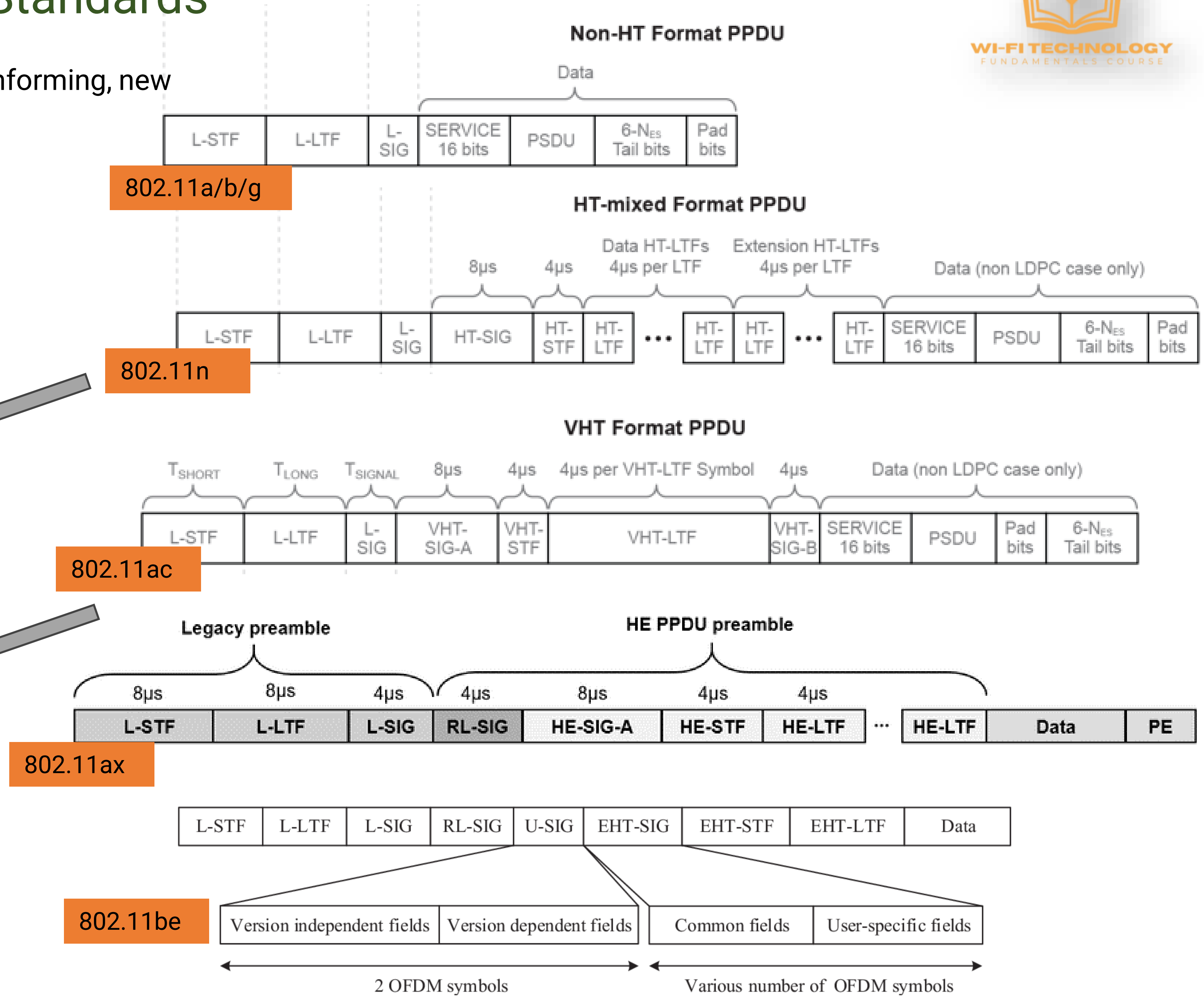


VHT-SIG-A1 Structure

Composite Name:	BW	Reserved	STBC	Group ID	NSTS/Partial AID				TXOP_PS_NOT_ALLOWED	Reserved
SU Name:					SU NSTS	Partial AID				
MU Name:					MU[0] NSTS	MU[1] NSTS	MU[2] NSTS	MU[3] NSTS		
Bits:	2	1	1	6	3	3	3	3	1	1

VHT-SIG-A2 Structure

Composite Name:	Short GI	Short GI NSYM Disambiguation	SU/MU[0] Coding	LDPC Extra OFDM Symbol	SU VHT-MCS/MU[1-3] Coding				Beamformed	Reserved	CRC	Tail
SU Name:					SU VHT-MCS				Beamformed			
MU Name:					MU[1] Coding	MU[2] Coding	MU[3] Coding	Reserved	Reserved			
Bits:	1	1	1	1	1	1	1	1	1	1	8	6



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

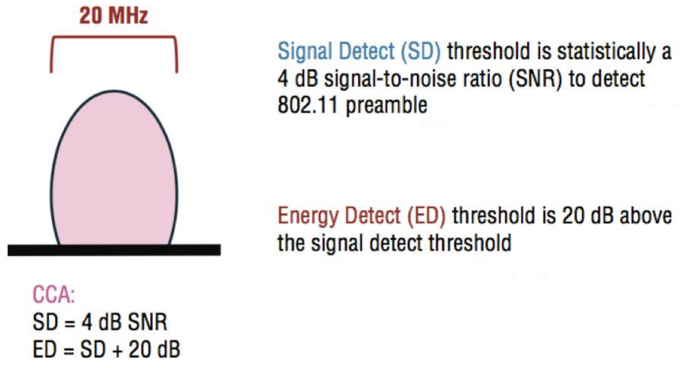
Clear Channel Assessment (CCA)

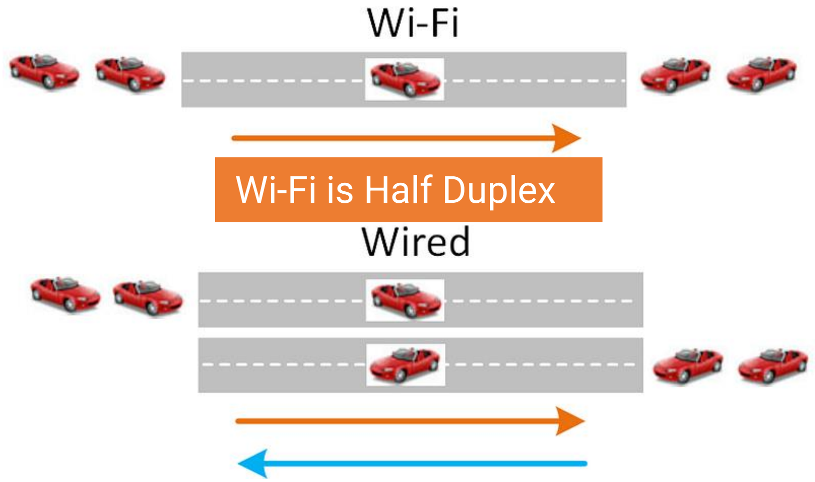
Wi-Fi used a "Listen Before Talk" mechanism for accessing the medium

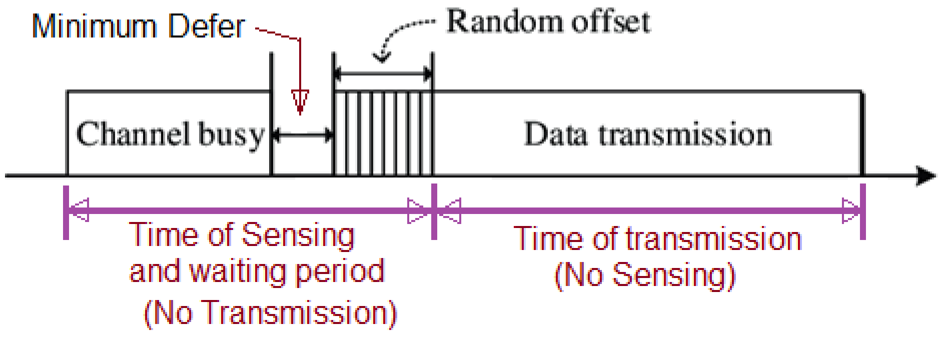
CCA also known as Physical Carrier Sensing, is a method used to determine if the medium is busy. Physical carrier sense is performed constantly by all Wi-Fi radios that are not transmitting or receiving.

Physical carrier sense has two purposes:

1. Determine in the receiver has any information to receive.
2. Determine if the medium is busy before transmission







Listen before Talk Algorithm

802.11 radios use two separate CCA thresholds when listening to the RF medium:

Signal detect (SD) threshold is used to identify any 802.11 preamble transmissions from another transmitting 802.11 radio. SD threshold is statistically around 4 SNR. In other words, an 802.11 radio can usually decode any incoming 802.11 preamble transmissions at a received signal at about 4 dB above the noise floor.

The energy detect (ED) threshold is used to detect any other type of RF transmissions during the CCA so that the receiver can not initiate any transmission during that time.

References

Computer Networking: A top down approach
http://gaia.cs.umass.edu/kurose_ross/online_lectures.htm

WLAN PHY PPDU Structure
https://www.mathworks.com/help/wlan/gs/wlan-ppdu-structure.html

The Importance of Detecting the 802.11 Preamble
https://gjermundraaen.com/2020/11/22/the-importance-of-detecting-the-802-11-preamble/

What is Clear Channel Assessment
https://www.extremenetworks.com/resources/blogs/what-is-a-clear-channel-assessment-cca

Example Wi-Fi Analyzer Tool
https://www.acrylicwifi.com/en/wifi-analyzer/

WI-FI TECHNOLOGY
FUNDAMENTALS COURSE

WI-FI TECHNOLOGY
FUNDAMENTALS COURSE

Quiz 2c Results

Number of participants - 126

Winners

S Sushmitha

Akhil S (10/10)