EEN 1043/EE452 Wireless and Mobile Communication

Wireless LAN

Sobia Jangsher
Assistant Professor
sobia.Jangsher@dcu.ie
School of Electronic Engineering

Wireless LANs

Advantages

- Key Benefits:
  - Not being tethered to a wire
  - Mobility
  - Requires less infrastructure
  - Transient deployments
  - Often more cost-efficient
  - Easily expandable
  - Ad-hoc networking

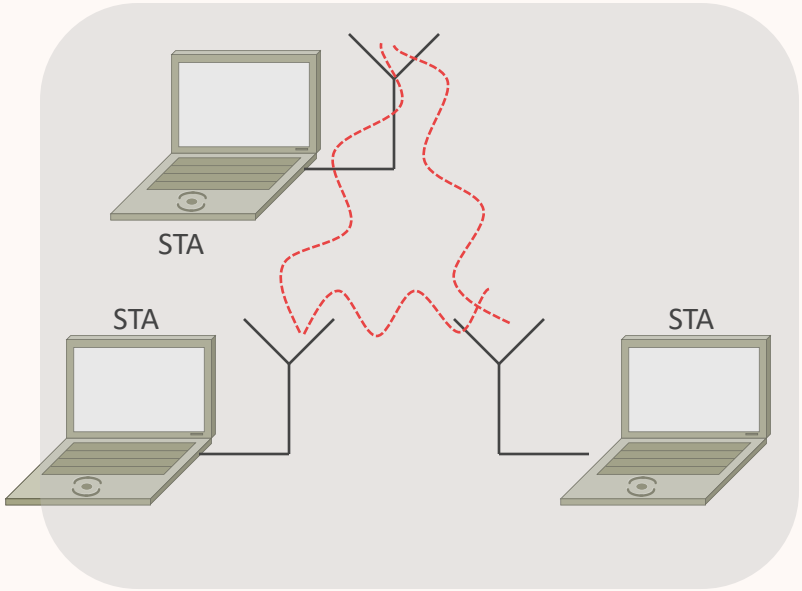
Wireless LANs

Disadvantages

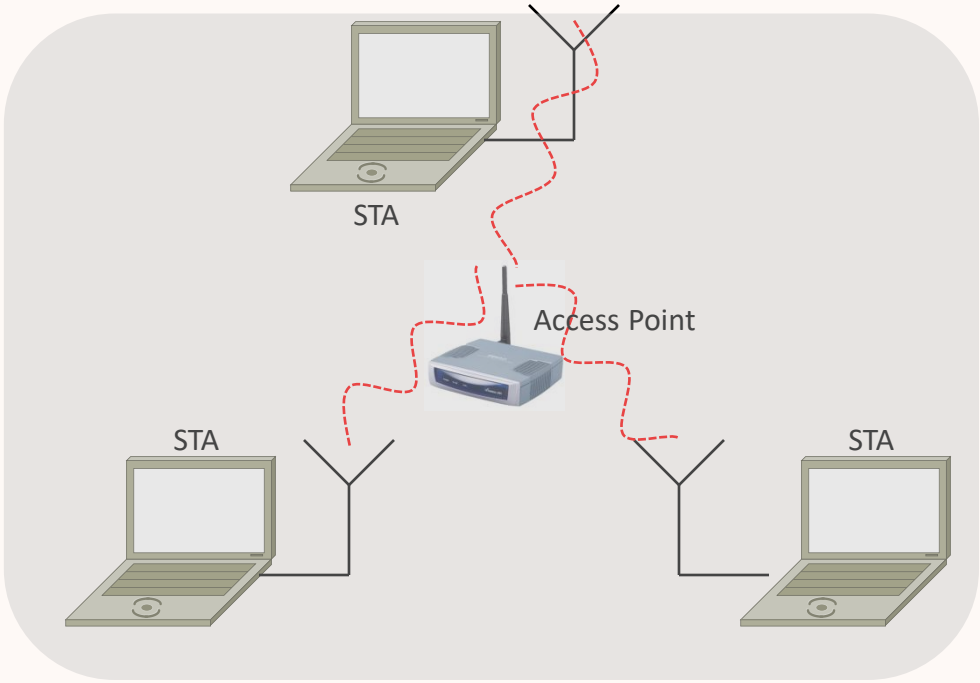
- Speed – Slower than wired networks, but still fast!
- Security – Much harder to secure than wired
- Reliability – Radio suffers from interference
- Range – Typical ranges under normal indoor conditions are 20m-50m
- Coverage – not the same infrastructure as cellular systems.

WLAN Types

Independent BSS / Ad-hoc



Infrastructure BSS



- BSS (Basic Service Set) – A group of stations that can communicate
  - Defined by propagation characteristics of the wireless medium
- SSID (Service Set Identifier) – Advertised Network Name
- STA (Station) – User terminal connected to other STA or AP
- AP (Access Point) – Station with access to external network

802 Standards

Name	Description	Note
IEEE 802.1	Higher Layer LAN Protocols (Bridging)	active
IEEE 802.2	LLC	disbanded
IEEE 802.3	Ethernet	active
IEEE 802.4	Token bus	disbanded
IEEE 802.5	Token ring MAC layer	disbanded
IEEE 802.6	MANs (DQDB)	disbanded
IEEE 802.7	Broadband LAN using Coaxial Cable	disbanded
IEEE 802.8	Fiber Optic TAG	disbanded
IEEE 802.9	Integrated Services LAN (ISLAN or isoEthernet)	disbanded
IEEE 802.10	Interoperable LAN Security	disbanded
IEEE 802.11	Wireless LAN (WLAN) & Mesh (Wi-Fi certification)	active
IEEE 802.12	100BaseVG	disbanded
IEEE 802.13	Unused[2]	Reserved for Fast Ethernet development[3]
IEEE 802.14	Cable modems	disbanded
IEEE 802.15	Wireless PAN	active
IEEE 802.15.1	Bluetooth certification	active
IEEE 802.15.2	IEEE 802.15 and IEEE 802.11 coexistence	
IEEE 802.15.3	High-Rate wireless PAN (e.g., UWB, etc.)	
IEEE 802.15.4	Low-Rate wireless PAN (e.g., ZigBee, WirelessHART, MiWi, etc.)	active
IEEE 802.15.5	Mesh networking for WPAN	
IEEE 802.15.6	Body area network	active
IEEE 802.15.7	Visible light communications	
IEEE 802.16	Broadband Wireless Access (WiMAX certification)	
IEEE 802.16.1	Local Multipoint Distribution Service	
IEEE 802.16.2	Coexistence wireless access	
IEEE 802.17	Resilient packet ring	hibernating
IEEE 802.18	Radio Regulatory TAG	
IEEE 802.19	Coexistence TAG	
IEEE 802.20	Mobile Broadband Wireless Access	hibernating
IEEE 802.21	Media Independent Handoff	
IEEE 802.22	Wireless Regional Area Network	
IEEE 802.23	Emergency Services Working Group	
IEEE 802.24	Smart Grid TAG	New (November, 2012)
IEEE 802.25	Omni-Range Area Network	

LAN Protocol: IEEE 802 Reference Model

- IEEE 802 committee
- Physical Layer
  - Encoding/decoding of signals
  - Synchronization
  - Bit transmission/reception
- Physical layer convergence procedure (PLCP)
  - Mapping MAC layer protocol units into framing format suitable for sending
- Physical medium dependent sublayer
  - Defines the characteristics of and method of transmitting and receiving

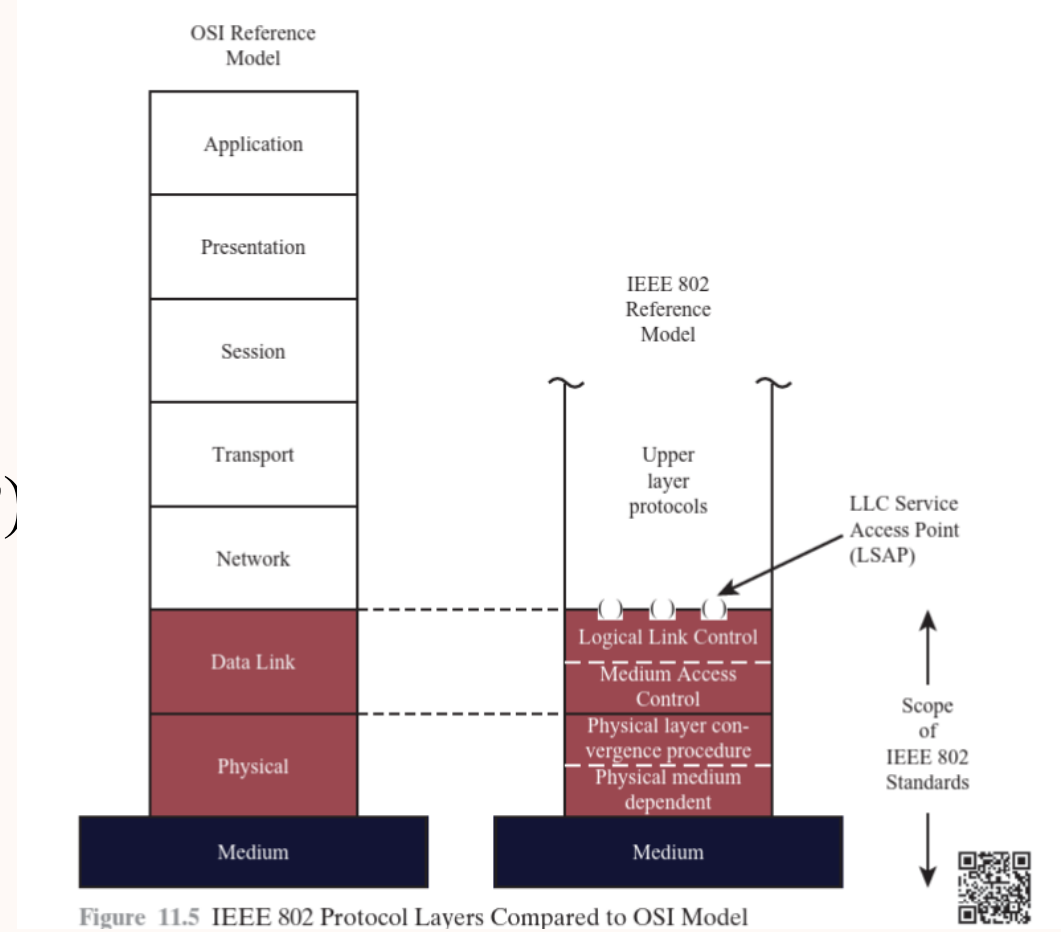


Figure 11.5 IEEE 802 Protocol Layers Compared to OSI Model

LAN Protocol: IEEE 802 Reference Model

- Logical link control (LLC)
  - Provide an interface to higher layers and perform flow and error control
- Medium Access Control
  - On transmission assemble data into a frame with address and error detection fields
  - On reception, disassemble frame and perform address recognition and error detection
  - Govern access to the LAN transmission medium

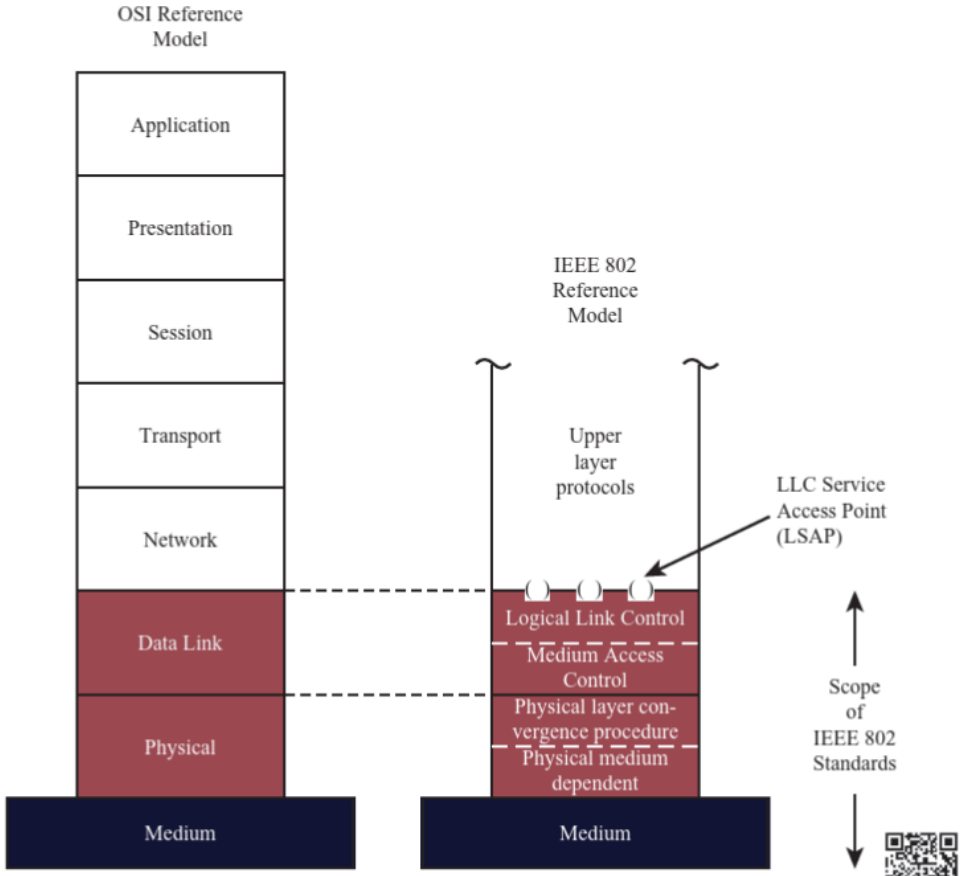


Figure 11.5 IEEE 802 Protocol Layers Compared to OSI Model

IEEE 802 Protocols in Context

managing the transfer between the sender and receiver, e.g. » Error detection and correction to deal with bit errors » Flow control: avoid that the sender outruns the receiver

LLC protocol data unit PDU

MAC Frame

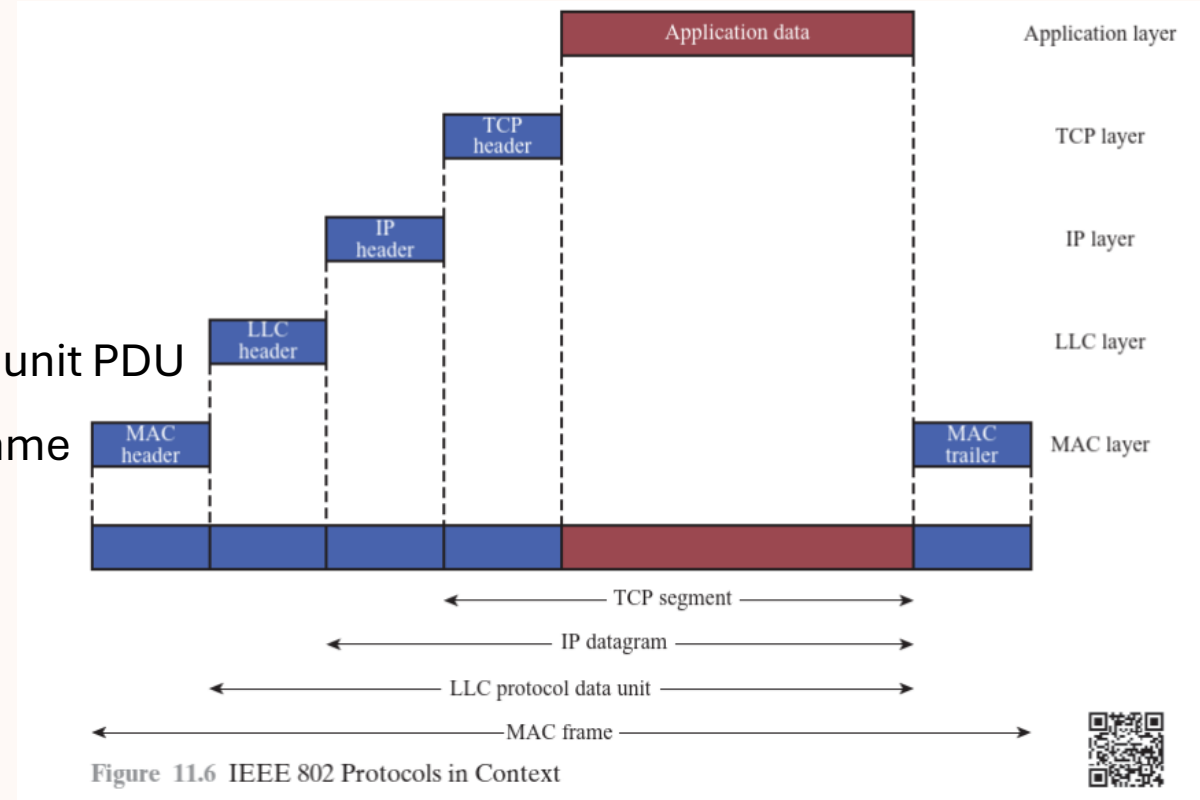


Figure 11.6 IEEE 802 Protocols in Context

controlling which device gets to send a frame next over a link » Easy for point-to-point links; half versus full duplex » Harder for multi-access links: who gets to send?

IEEE 802.11Common 802.11 Amendments

MAC/PHY Standards

Standard	Data rate	Throughput	Technology	Band	Range - Indoor
802.11b	11 Mbps	6-7Mbps	DSSS	2.4Ghz	40m
802.11g	54Mbps	29Mbps	OFDM, DSSS	2.4Ghz	40m
802.11a	54Mbps	29Mbps	OFDM	5Ghz	15m
802.11n	Up to 600Mbps	Up to 420 Mbps	OFDM, MIMO	2.4Ghz/5Ghz	80m
802.11ac	Up to 6.93Gbps	Up to 4.9 Gbps	OFDM, MIMO	5Ghz	35m

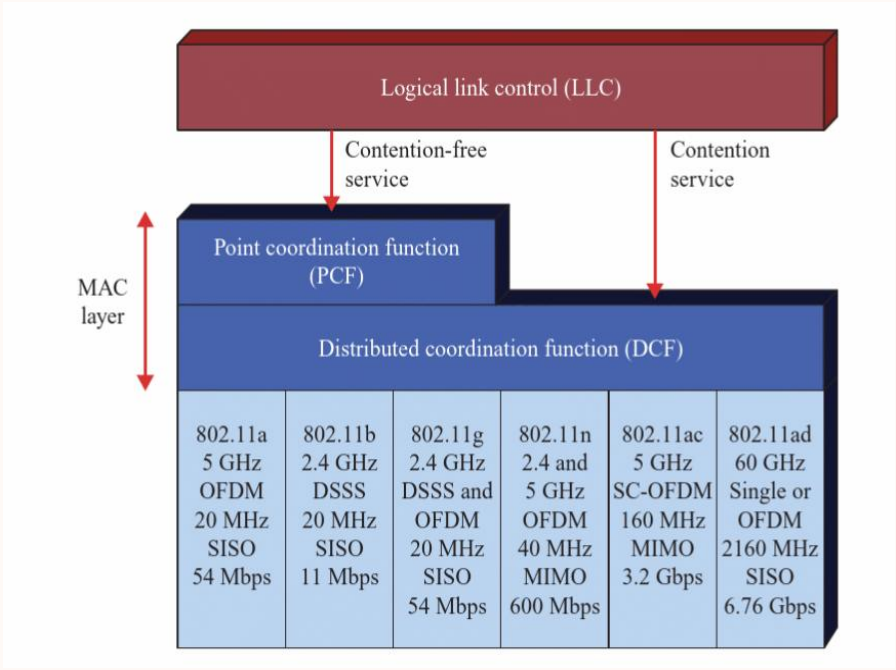
- Other Common Amendments
  - 802.11e – QoS Enhancements to MAC layer
  - 802.11f – Inter access point protocol
  - 802.11s – mesh networking
  - 802.11k – Radio resource management
  - 802.11n/ac—improvements to air interface

IEEE 802.11: Joining a Network

- *Beacon Frames* are used to announce the existence of the network
  - Periodically transmitted by APs (e.g. every 100ms)
  - Lowest data rate, maximum power
  - Provides synchronisation, BSS and Address information
- The user station's behaviour
  - *Passive Scanning*: Scans each available channel looking for beacon frames
  - *Active Scanning*: Does not scan; rather, transmits a probe request – AP will respond with a probe response containing beacon information
  - Active scanning is faster but more intrusive. Active scanning is now more common (allows faster re-connection)
- Association/Authentication: having found an AP to attach to, the user station must register with the AP and perform a basic identity exchange

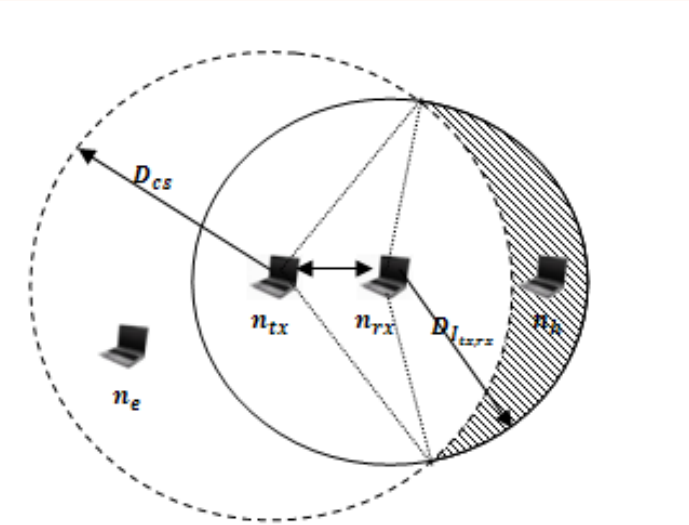
IEEE 802.11: MAC Access Modes

- DCF (Distributed Coordination Function)
  - Contention based medium access
  - Uses CSMA/CA: Listen before send
  - Random back-off
  - Most prevalent MAC access mechanism
- PCF (Point Coordination Function)
  - Contention free
  - Point coordinator (AP) controls medium access
  - *Not widely implemented*
- HCF (Hybrid Coordination Function)
  - Contains contention and contention free access
  - Used as the basis of some QoS mechanisms in WLAN



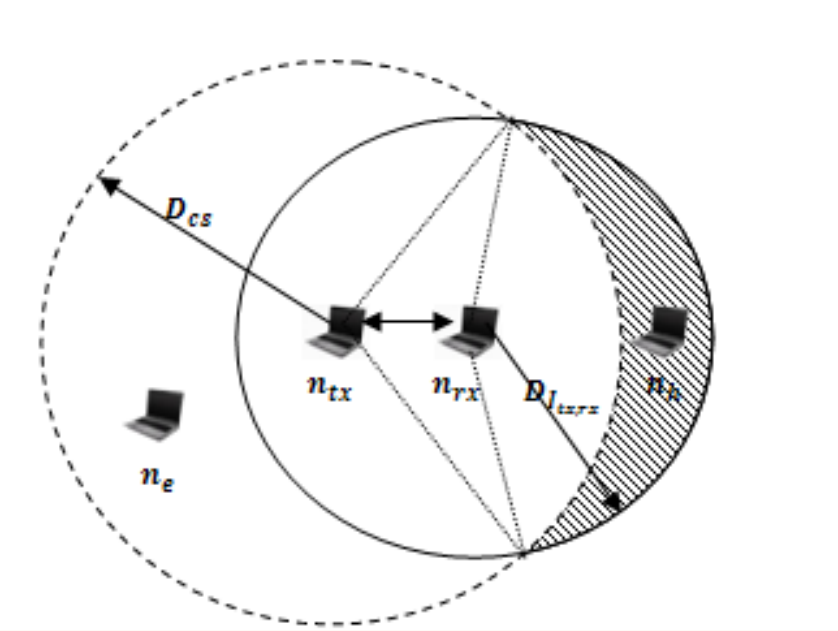
IEEE 802.11: Hidden Node Problem

- **Wireless networks have unclear boundaries**
- Received signal = transmitted signal + interference + noise
  - Hear signal only if received power > carrier sense threshold (CST)
  - Higher power level required for successful packet reception
- Node n_{tx} is transmitting to n_{rx}
- Node n_h is a **hidden node** for this transmission: it may attempt to transmit to node n_{rx} during n_{tx}'s transmission, which will **cause interference** (both transmissions are typically lost)



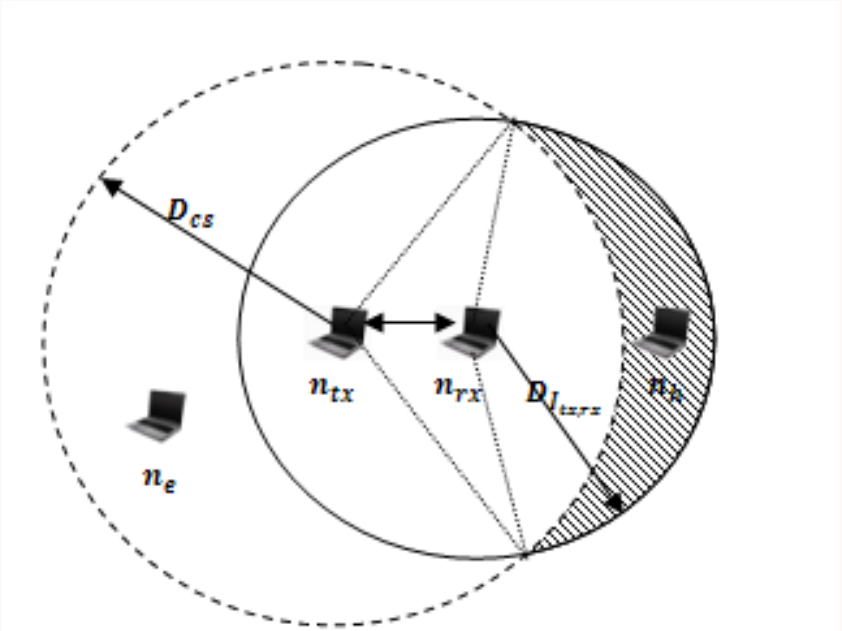
IEEE 802.11: Exposed Node Problem

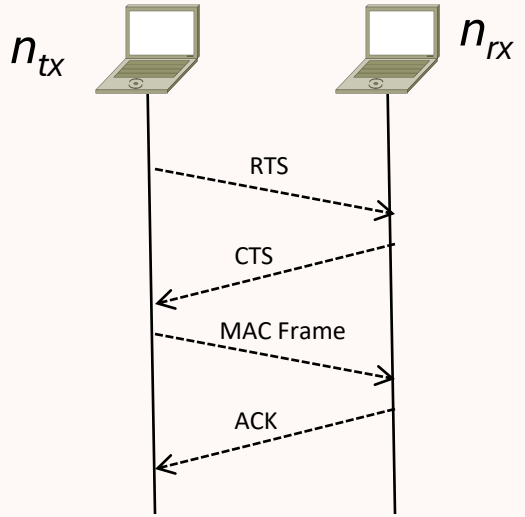
- Node n_{tx} is transmitting to node n_{rx}
- Node n_e is an **exposed node** for this transmission: it should be able to transmit to some other node (not shown), but is prevented from doing so because it can sense n_{tx}'s transmission
- Leads to **reduced throughput**



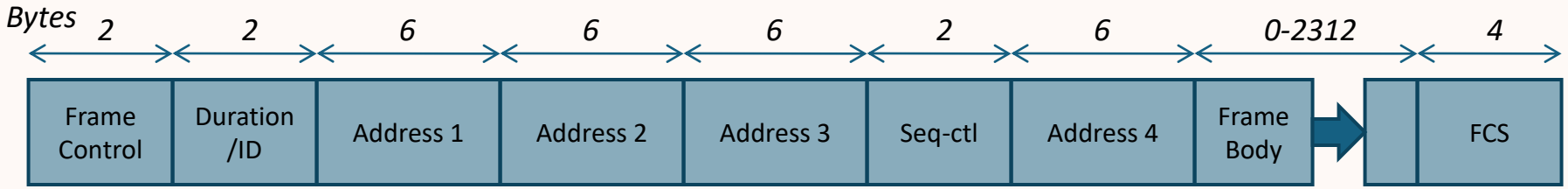
IEEE 802.11:RTS/CTS – Virtual Carrier Sensing

- Request to Send / Clear to Send addresses the hidden node problem
- Each RTS/CTS frame specifies how long the transmission will take
- Hidden node: n_h does not receive the RTS, but will see the CTS and therefore will not transmit.
- Exposed node: n_e will hear the RTS, but will not hear the CTS and thus will know it can transmit.
- Not commonly used due to overhead required
  - Example use case: accept reduced network throughput to improve QoS level.



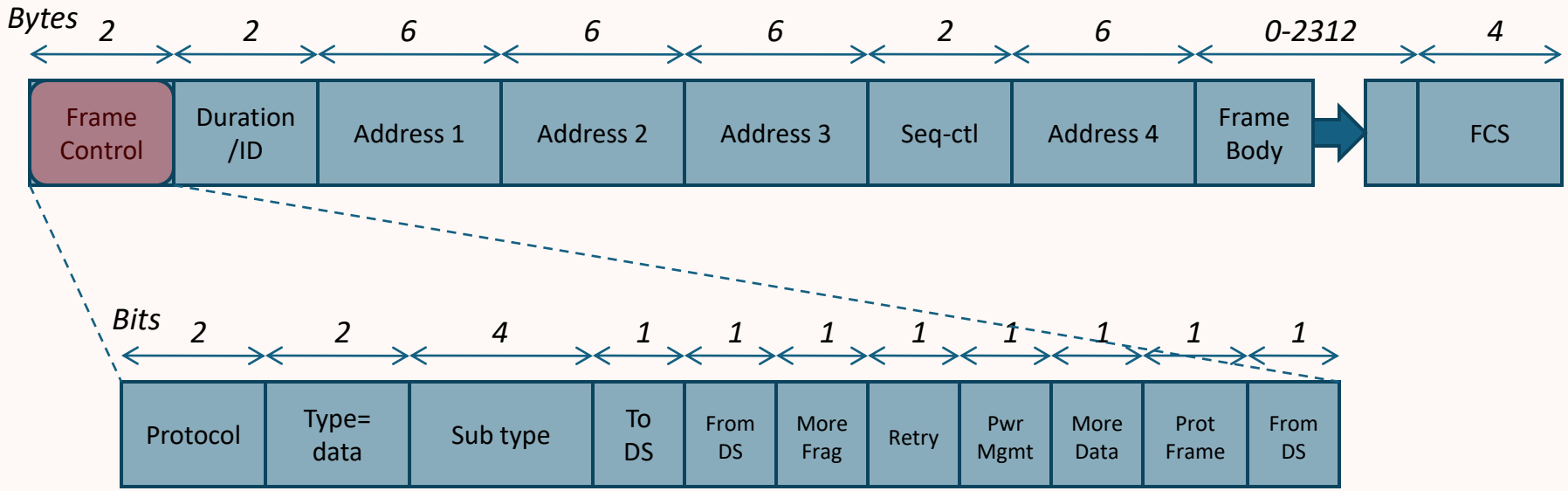


IEEE 802.11: Frame Format



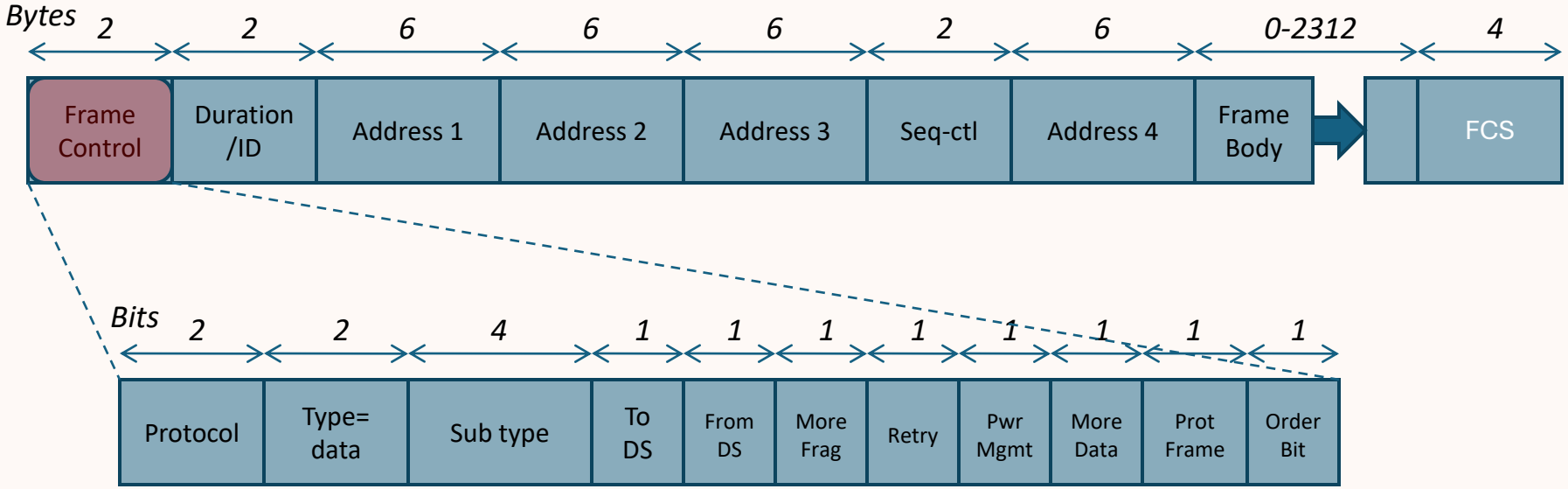
- Generic MAC frame
- The 802.11 MAC uses a different frame structure to Ethernet
  - 4 Address fields
  - Not used all the time
- Overhead of 34 bytes

IEEE 802.11 Frame Control



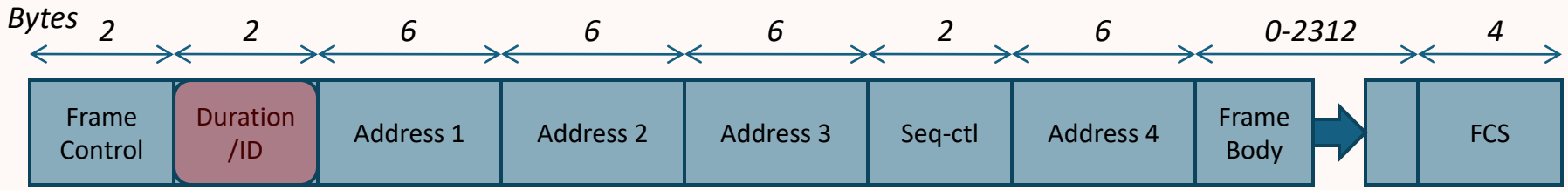
- *Protocol Version:* version of 802.11 MAC
- *Type:* Frame Type (e.g. Management, Data)
- *Sub Type:* Specific Frame Subtype
  - *E.g. 1000 = beacon, 1011=RTS*
- *To DS / From DS:* Specify if frame is destined for the Distribution system (DS) or is coming from the DS

IEEE 802.11 Frame Control



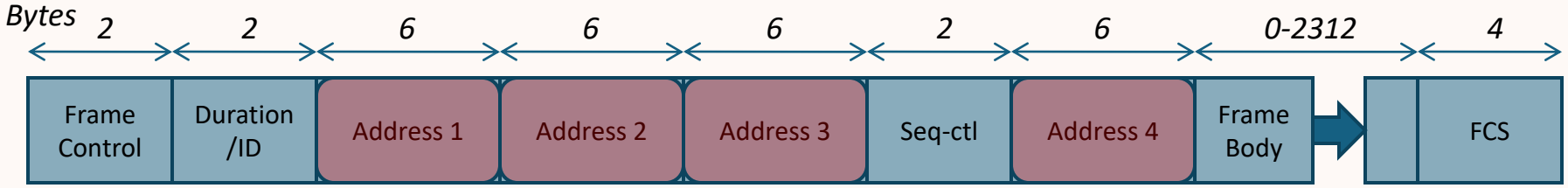
- *More Frag:* Specifies if frame has been fragmented
- *Retry:* Is a retransmission
- *Power Management:* Indicates that sending station will power down after transmission
- *More Data:* Informs a sleeping station that data is available
- *Protected Frame:* Security is being used on Frame
- *Order Bit:* Strict ordering must be used

IEEE 802.11 Duration/ID Field



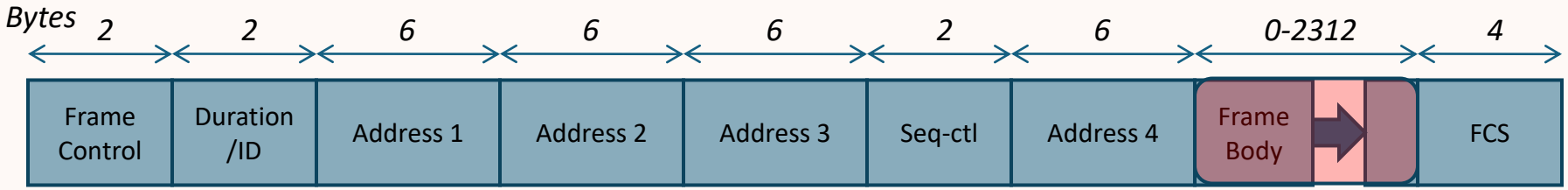
- Duration: Three Purposes
  - Setting the NAV: Defines the amount of time in ms the medium will be busy for
  - CFP Frames: Essentially sets the NAV to the maximum value during contention free periods
  - PS-Poll Frames: Used by stations to inform the AP that they have woken from power saving state

IEEE 802.11Address Fields



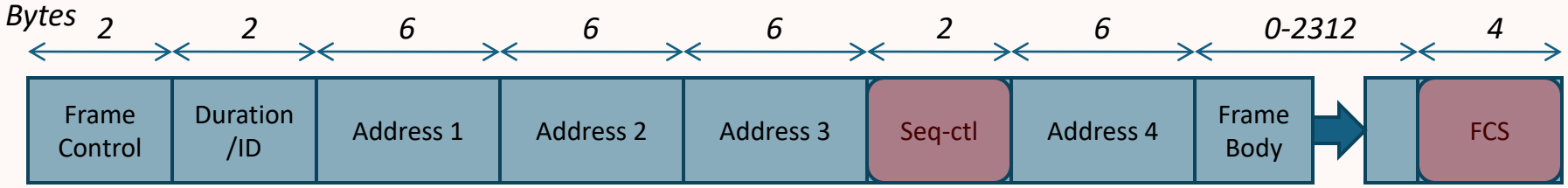
- All addresses are 48 bit IEEE MACs
  - Destination: Identifies the final recipient
  - Source: Identifies the original source
  - Receiver: Identifies the receiver which should process the frame (Intermediate node)
  - Transmitter: Identifies the transmitter of the frame (Intermediate node)

IEEE 802.11 Frame Body



- Also called the "Data Field"
- Contains the higher layer payload
- 802.11 supports up to 2312 bytes of data
  - RFC 1191 (Path MTU Discovery) allows max size of 1500 bytes

IEEE 802.11 Seq-Ctl & FCS



- Sequence Control – Used for detecting and discarding of duplicate frames
- Frame Check Sequence – Often called the CRC, used to check frame integrity

802.11: Frames types

- Three types of frames
  - Control
    - signalling to manage transmission of data
  - Data
    - carry higher layer data
  - Management
    - enable stations to establish and maintain communications.
    - establish connection with the network

802.11: Control Frames

- Power Save-Poll: request AP send frames buffered while station in power-saving mode.
- RTS
- CTS
- Ack
- Contention-Free(CF)-End: for PCF announce end of contention free period.
- CF-End+CF-Ack: acnowledges the CF-end.

802.11: Data Frames

- 8 frame types
  - 4 carry upper level data from source station to destination station.
    - Data
    - Data+CF-Ack
      - Ack piggybacked, only send during CF period.
    - Data+CF-Poll
      - Used by PCF to deliver data and request data from station.
    - Data+CF-Ack+CF-Poll
      - Combine above.
  - 4 used for control
    - Null Function data frame
      - Power management bit used to indicate station changing to low-power state.
    - CF-Ack, CF-Poll, CF-Ack+CF-Poll as above, but with no data.

802.11 Management Frames

- Management Frames
  - Manage communication between stations and AP
    - Association request—join BSS
    - Association response
    - Reassociation request—move from one BSS to another.
      - APs coordinate to forward frames
    - Reassociation response
    - Probe request—used to locate BSS
    - Probe response
    - Beacon—allow mobile stations to locate and identify BSS.
    - Announcement traffic indication message—alert low-power mode station to waiting traffic.
    - Dissociation
    - Authenticaton
    - Deauthentcation

IEEE 802.11 Why do I get lower throughput?

e.g. 54Mbps connection but user only sees a throughput of 29Mbps

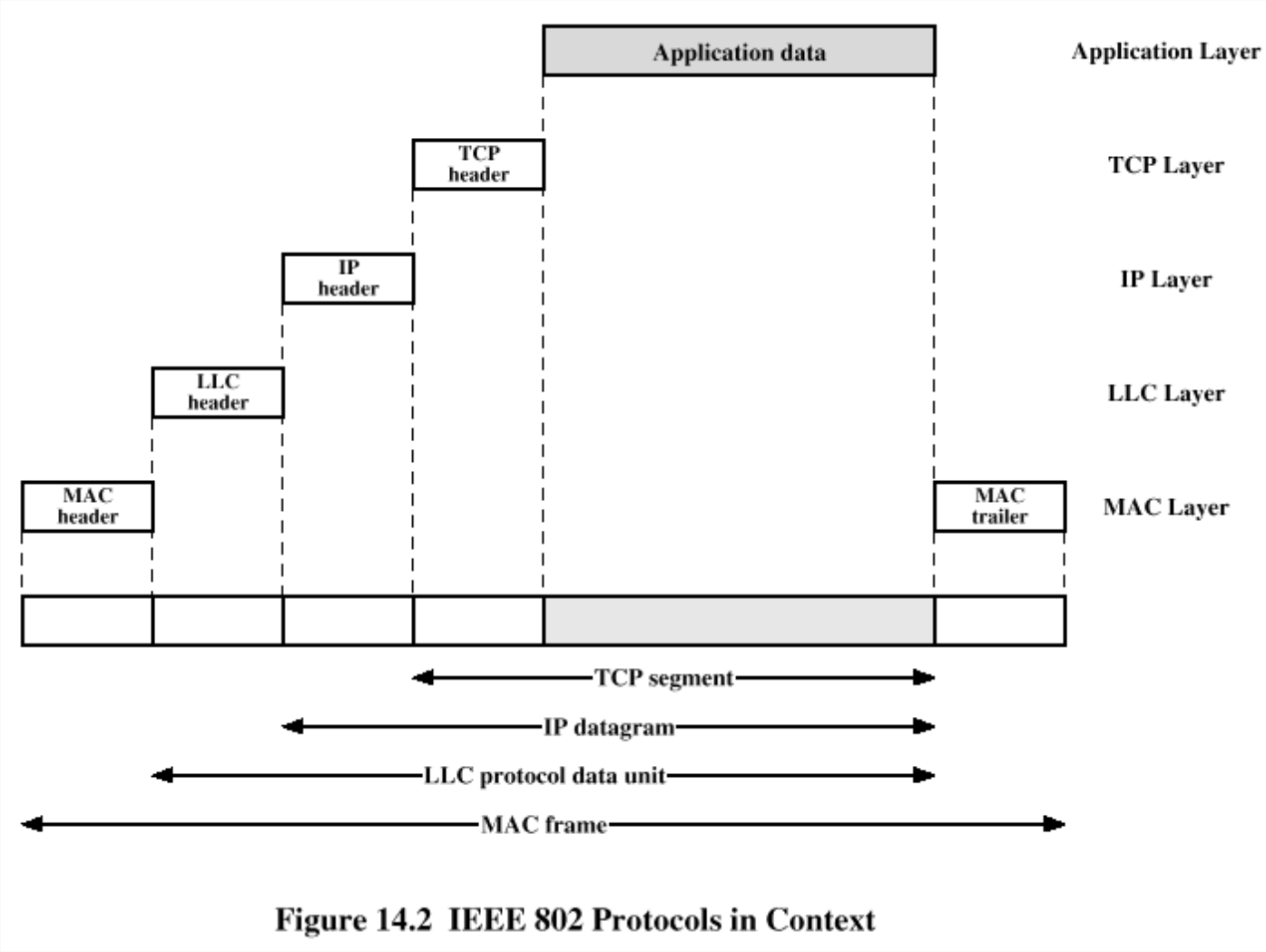
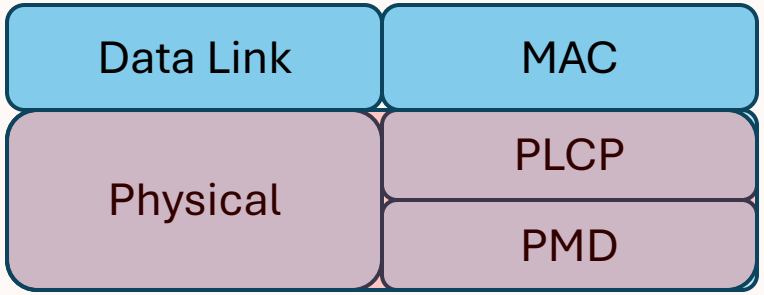


Figure 14.2 IEEE 802 Protocols in Context

IEEE 802.11

Physical Layer



- Divided into two layers:
  - Physical Layer Convergence Procedure (PLCP)
    - Intermediate layer between MAC and actual transmission
    - Adds its own header specific to each physical layer
  - Physical Medium Dependent (PMD)
    - Responsible for transmitting bits
    - Specific to each physical layer

IEEE 802.11

Physical Layer

Radio Link

- A number of Physical layers defined:
  - Frequency Hopping Spread Spectrum (FHSS)
  - Direct Sequence Spread Spectrum (DSSS)
  - Infrared Light (IR)
    - Not used due to low data rates and interference
    - No products were created
  - Orthogonal Frequency Division Multiplexing (OFDM)
  - High Rate Direct Sequence (HR/DS)
  - Extended Rate Phy (ERP)

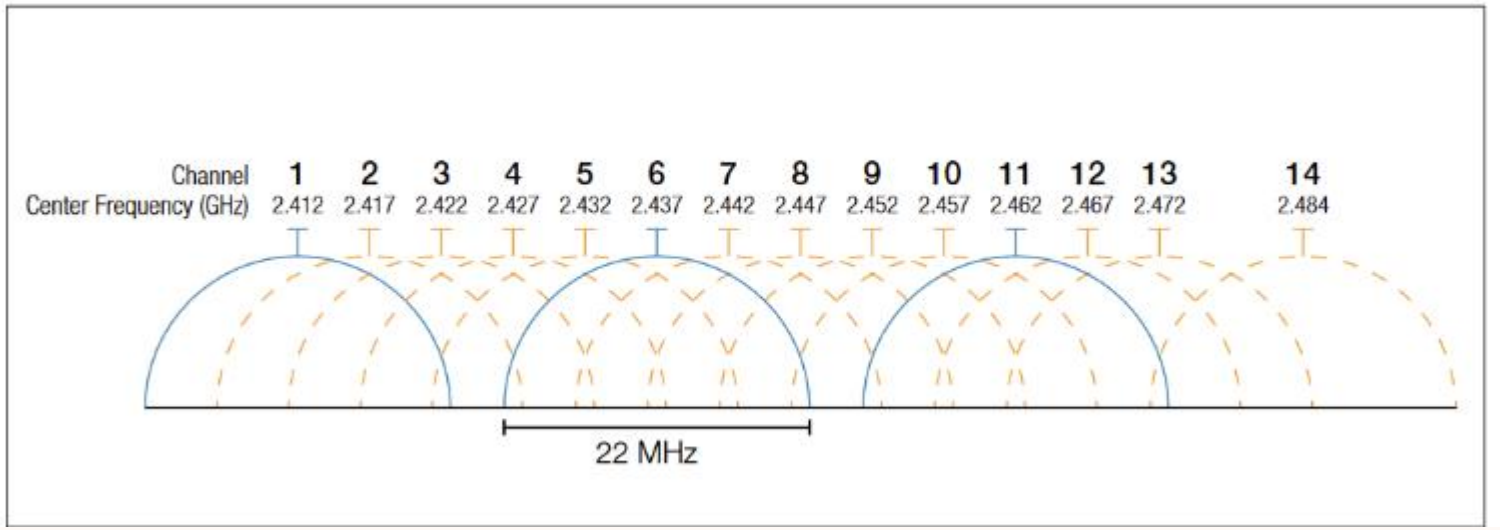
IEEE 802.11: Physical Layer
Radio Link

- The 802.11b, 802.11g, and the low-frequency part of the 802.11n standards utilize the 2.400 – 2.500 GHz spectrum located in the ISM band.
- The 802.11a, 802.11n and 802.11ac standards use the more heavily regulated 4.915 – 5.825 GHz band.
- These are often referred to as the "2.4 GHz and 5 GHz frequency bands". Each of these spectrums are sub-divided into channels with a center frequency and bandwidth, similar to the way commercial spectrums are sub-divided.

IEEE 802.11

Physical Layer

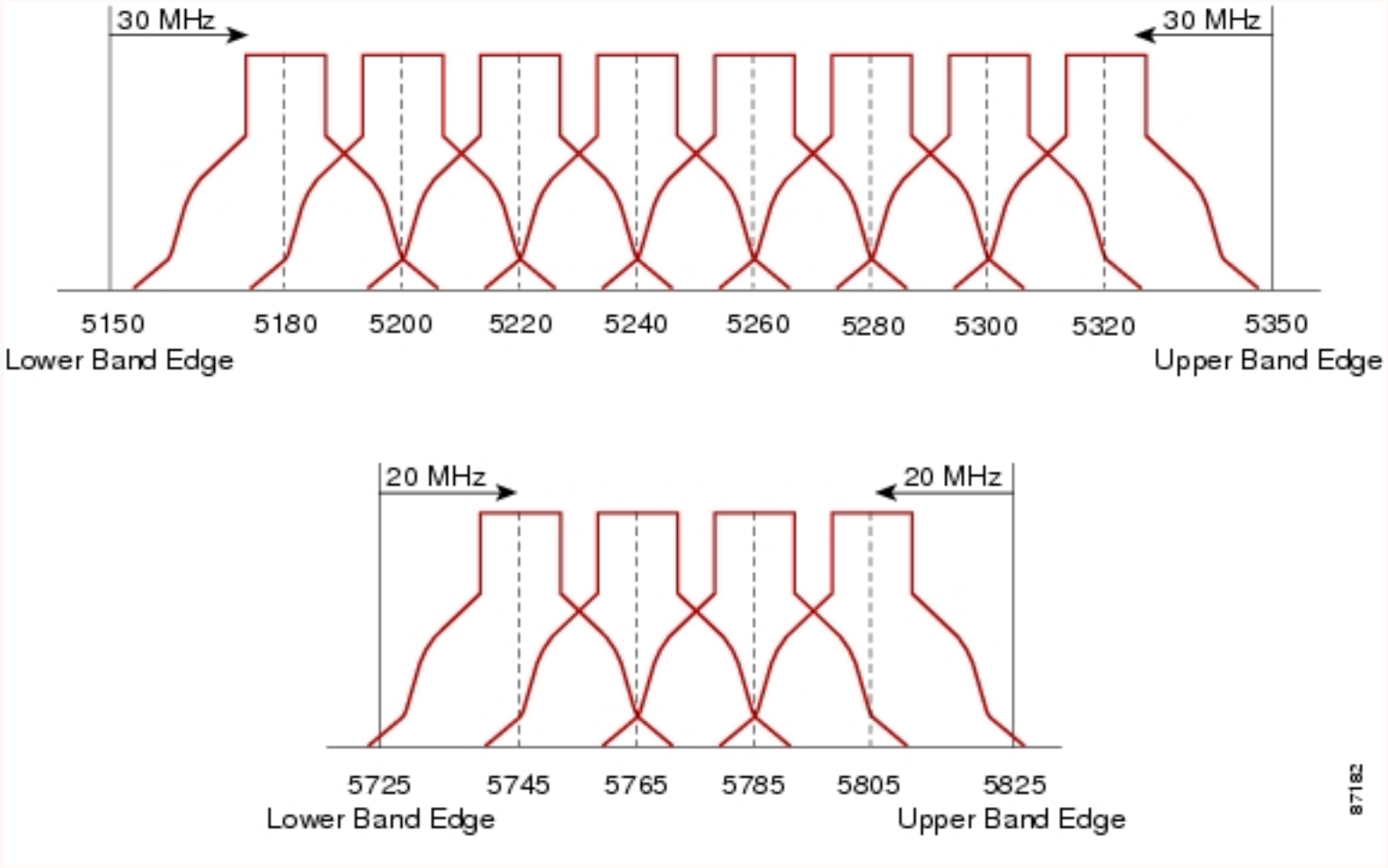
ISM Band – 802.11b/g 2.4Ghz



- 20Mhz channels with 1MHz guard bands
- Selecting different channels does not mean you will not interfere
- Only 3 non-overlapping channels available
  - 1, 6, 11

https://www.tek.com/en/documents/primer/wi-fi-overview-80211-physical-layer-and-transmitter-measurements

IEEE 802.11: Physical Layer ISM Band – 802.11a/n/ac 5Ghz



IEEE 802.11: 802.11n

- Goal is to improve network throughput
- Adds a number of new features - most significantly:
  - Increased channel BW
    - Normally 802.11 channels are 20Mhz wide
    - 802.11n allows a doubling of this channel width to occupy two channels (40Mhz)
      - Allows for slightly more that double the bit rate.
  - Multiple Input Multiple Output (MIMO)
    - Multiple antennas can be used simultaneously
    - Helps with multipath problems.

IEEE 802.11

802.11n

Modulation Coding Scheme

- Modulation and Coding Scheme (MCS) is used to categorise the factors affecting data rates for transmission.
  - Modulation scheme
    - Up to 64 QSM
  - Coding rate
    - k/n = for every k bits of data, n bits transmitted.
  - Guard interval
  - Channel bandwidth
  - Number of spatial streams

IEEE 802.11

802.11n

Modulation Coding Scheme

- 78 permutations of the factors affecting data rates are defined
  - MCS values 0-31 fix modulation type and coding scheme.
  - MCS values 32-77 allow different spatial streams to use different modulation types and coding schemes.
  - Aps must support MCS values 0-15
  - Stations must support 0-7

MCS index	Spatial streams	Modulation type	Coding rate	Data rate (Mbit/s)			
				20 MHz channel		40 MHz channel	
				800 ns GI	400 ns GI	800 ns GI	400 ns GI
0	1	BPSK	1/2	6.50	7.20	13.50	15.00
1	1	QPSK	1/2	13.00	14.40	27.00	30.00
2	1	QPSK	3/4	19.50	21.70	40.50	45.00
3	1	16-QAM	1/2	26.00	28.90	54.00	60.00
4	1	16-QAM	3/4	39.00	43.30	81.00	90.00
5	1	64-QAM	2/3	52.00	57.80	108.00	120.00
6	1	64-QAM	3/4	58.50	65.00	121.50	135.00
7	1	64-QAM	5/6	65.00	72.20	135.00	150.00
8	2	BPSK	1/2	13.00	14.40	27.00	30.00
9	2	QPSK	1/2	26.00	28.90	54.00	60.00
10	2	QPSK	3/4	39.00	43.30	81.00	90.00
11	2	16-QAM	1/2	52.00	57.80	108.00	120.00
12	2	16-QAM	3/4	78.00	86.70	162.00	180.00
13	2	64-QAM	2/3	104.00	115.60	216.00	240.00
14	2	64-QAM	3/4	117.00	130.00	243.00	270.00
15	2	64-QAM	5/6	130.00	144.40	270.00	300.00
16	3	BPSK	1/2	19.50	21.70	40.50	45.00
17	3	QPSK	1/2	39.00	43.30	81.00	90.00
18	3	QPSK	3/4	58.50	65.00	121.50	135.00
19	3	16-QAM	1/2	78.00	86.70	162.00	180.00
20	3	16-QAM	3/4	117.00	130.70	243.00	270.00
21	3	64-QAM	2/3	156.00	173.30	324.00	360.00
22	3	64-QAM	3/4	175.50	195.00	364.50	405.00
23	3	64-QAM	5/6	195.00	216.70	405.00	450.00
...	4	...	...	...	...	...	...
31	4	64-QAM	5/6	260.00	288.90	540.00	600.00

Wi-Fi Generations					
	Wi-Fi 4	Wi-Fi 5	Wi-Fi 6	Wi-Fi 6E	**Wi-Fi 7**
Launch date	2007	2013	2019	2021	2024
IEEE std.	802.11n	802.11ac	802.11ax		802.11be
Latency/Resiliency					MLO
Max data rate	1.2 Gbps	3.5 Gbps	9.6 Gbps		46 Gbps
Bands	2.4/5 GHz	2.4/5 GHz	2.4/5 GHz	2.4/5/6 GHz	2.4/5/6 GHz
Security	WPA 2	WPA 2	WPA 3		WPA 3
Channel width	20,40 MHz	20,40,80,80+80, 160 MHz	20,40,80,80+80,160 MHz		Up to 320 MHz
Modulation	64-QAM, OFDM	256-QAM, OFDM	1024-QAM, OFDMA		4096-QAM, OFDMA
MIMO	4x4 MIMO	4x4 MIMO, DL MU-MIMO	8x8 UL/DL MU-MIMO		16x16 MU-MIMO
Power Saving			TWT		RTWT