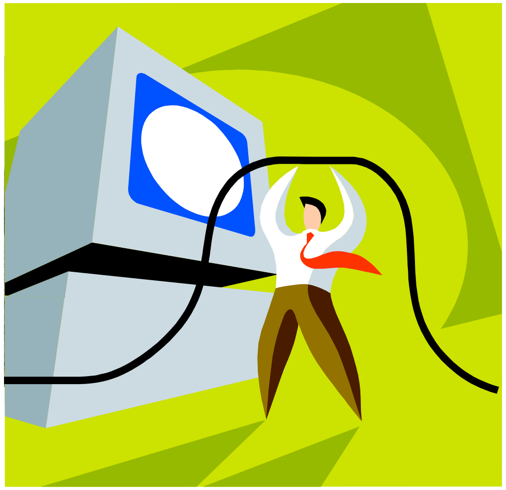
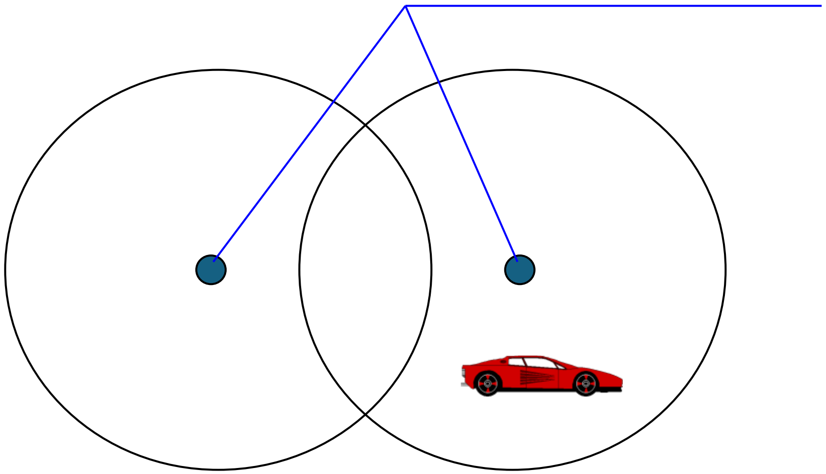
Mobile Networks

Connections and structures



Public cellular network

- Access network with radio link
  - Space is divided in cells with a base station
  - Mobile Node (MN) can work when changing between cells



Cell coverage size is
  - Highly variable
  - Depends on the technology
  - Depends on the number of users

Cells

Advantages:

> capacity

> # users

< power

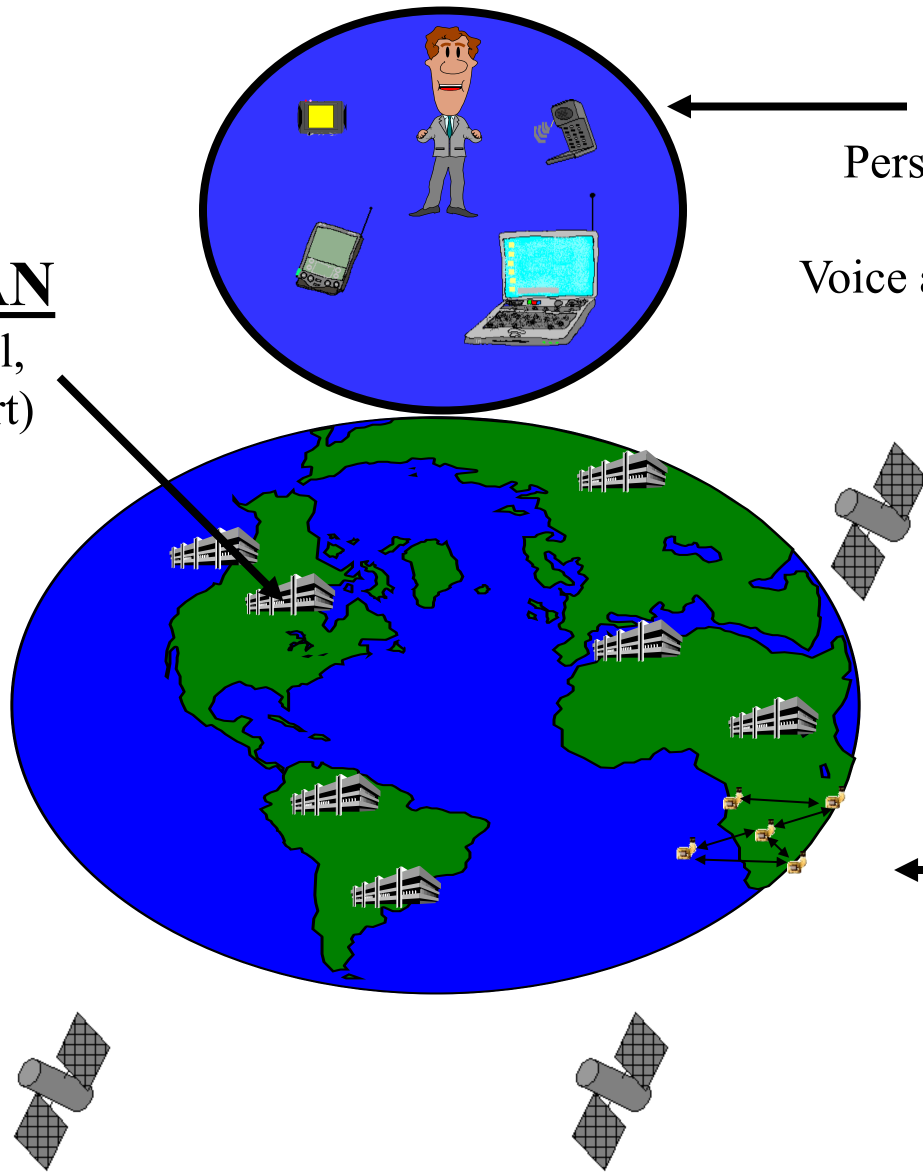
> robustness (distributed system)

Each cell locally takes care of interference, coverage area, etc...

- Disadvantages
  - Uses cabled network between cells
  - Many handovers
  - Interference between cells
- Fundamental:

  Cell dimensioning
    - Length of the cell
    - Frequency re-utilization
    - Channel reservation

Types of Wireless networks



PANs

Personal networks, very limited range

Voice and data with low cost

Wireless LAN

Campus (school, company, airport)

Satellite

Worldwide networks

High cost

Cellular

Large geographic coverage

WSN

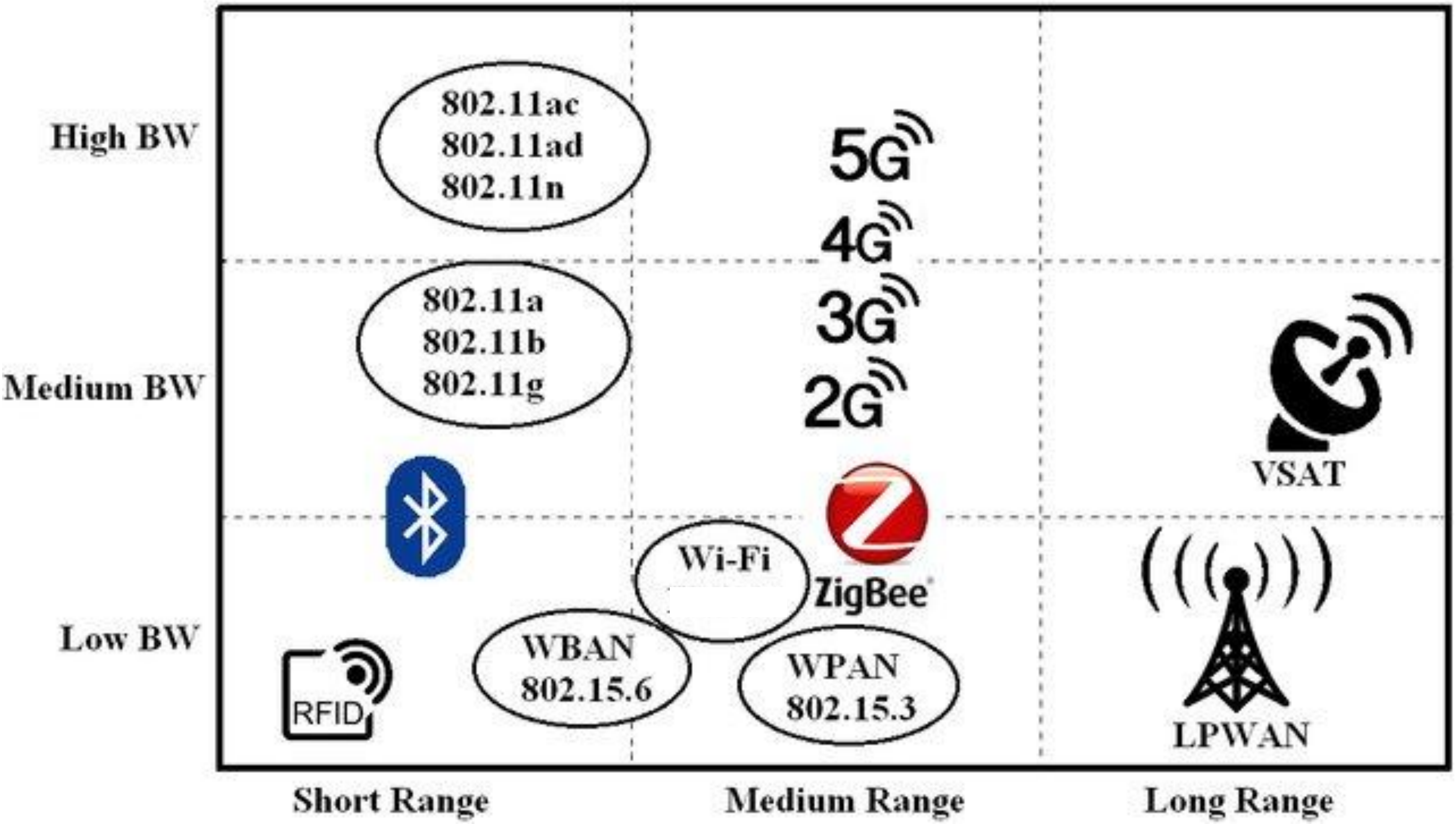
Multi-dimensional

Variable (low) cost

Usually low bitrate

Comparison Between Wireless Technologies

Tradeoff between data rate and range



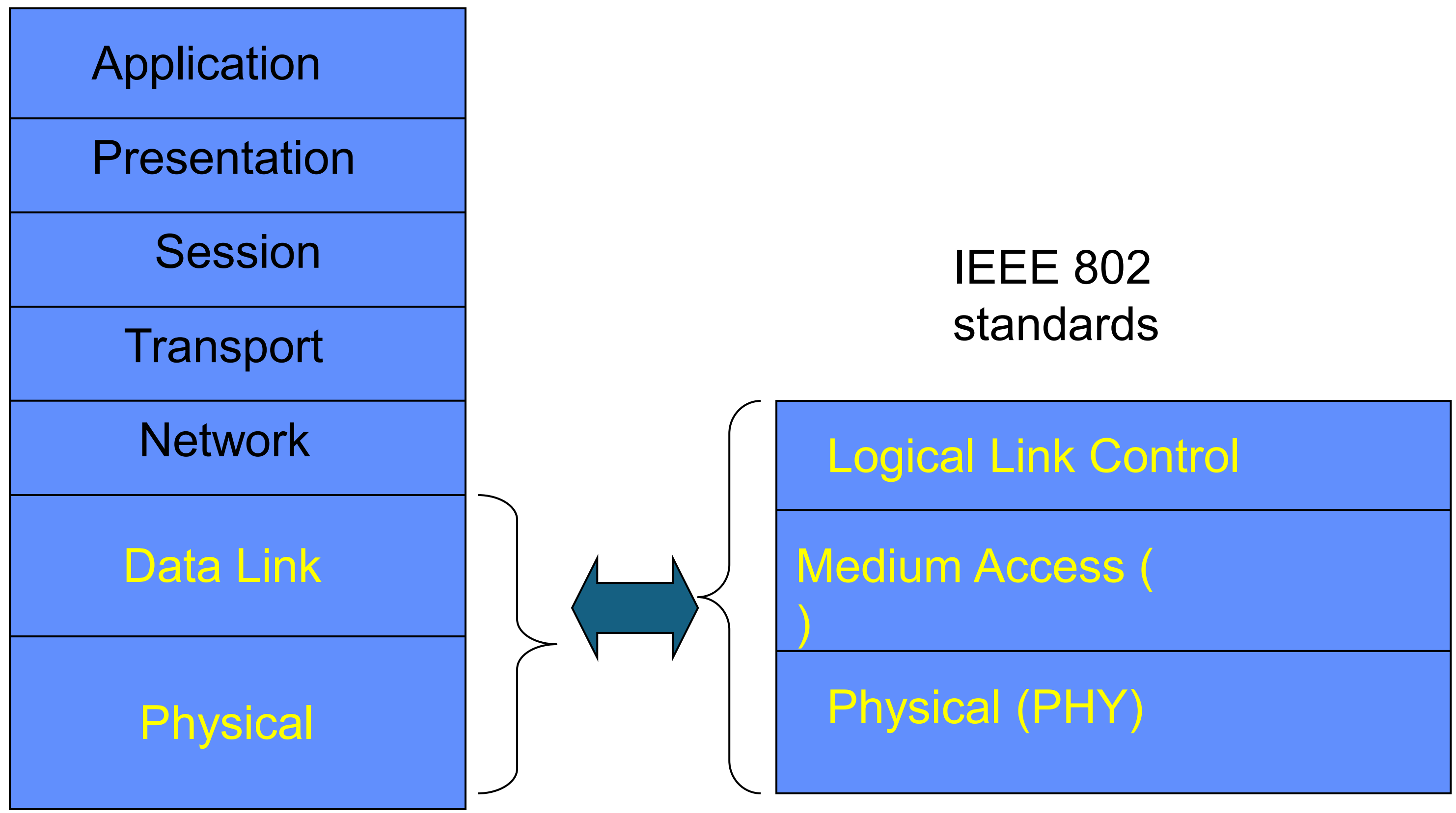
Standardization of Wireless Networks

- Wireless networks are standardized by IEEE.
- Under 802 LAN MAN standards committee.

LAN – Local Area Netework
MAN – Metro Area Network

ISO
OSI
7-layer
model

IEEE 802
standards



802.11

Outline

- 802.11 standard

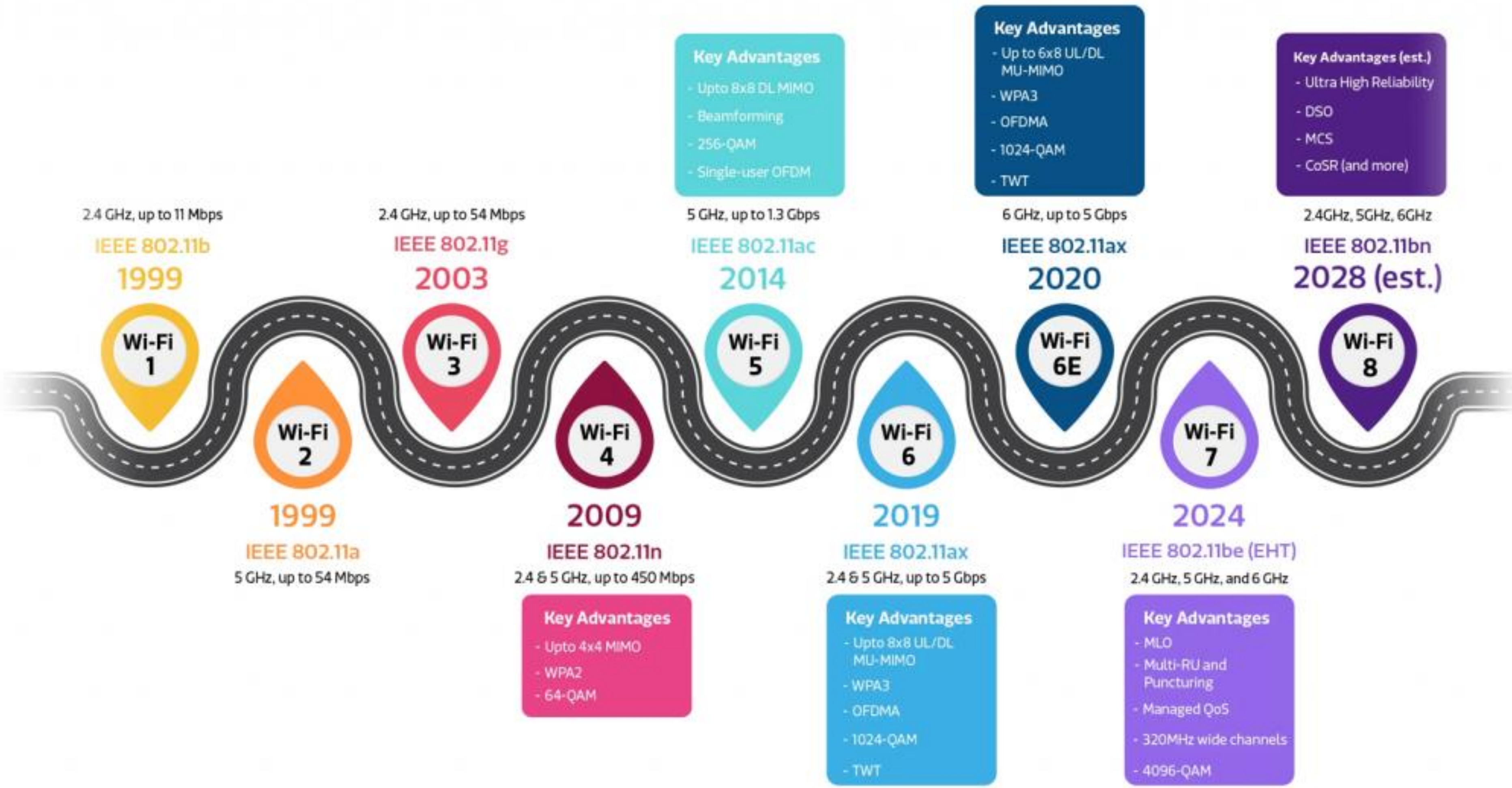
➢Physical layer

- MAC
  - DCF – Distributed Coordination Function
  - PCF – Point Coordination Function
- Advanced MAC functions

Historic IEEE 802.11 standard

- Local Wireless Network (WLAN)
- Includes Medium Access Control (MAC)
- Includes(d) five physical layers (PHY)
  - Frequency Hopping Spread Spectrum
  - Direct Sequence Spread Spectrum
  - infrared
  - 11 Mbps - 2.4 GHz
  - 54 Mbps - 5 GHz
  - Early efforts divided in three standards:
    - 802.11
    - 802.11a
    - 802.11b

Wi-Fi Evolution



Historic IEEE 802.11 Family

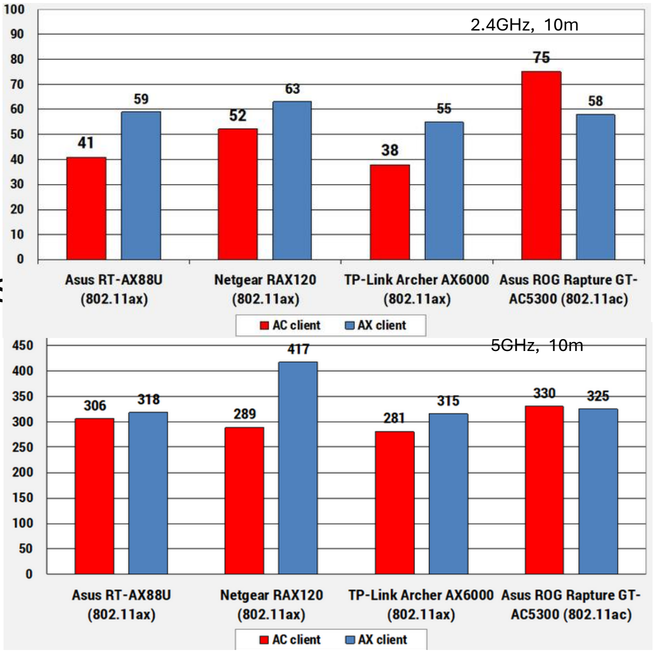
Protocol	Release Data	Freq.	Rate (typical)	Rate (max)	Range (indoor)
Legacy	1997	2.4 GHz	1 Mbps	2Mbps	?
802.11a	1999	5 GHz	25 Mbps	54 Mbps	~30 m
802.11b	1999	2.4 GHz	6.5 Mbps	11 Mbps	~30 m
802.11g	2003	2.4 GHz	25 Mbps	54 Mbps	~30 m
802.11n	2008	2.4/5 GHz	200 Mbps	600 Mbps	~50 m
802.11ac	2014	5 GHz	600Mbps	3.5 Gbps	~35m
802.11ax (Wi-Fi 6)	2021	2.4/5 GHz	130 (2.4 GHz) 400-800Mbps (5GHz)	10 Gbps	~30m
802.11be (Wi-Fi 7)	2024	2.4/5/6 GHz	2-4Gbps (laptop) , 5-18 PC’s	40 Gbps	Similar to Wi-Fi 6
802.11ay	2021	60 GHz	20 Gbps	20-40 Gbps	300-500m
802.11bn	2028?	2.4/5/6 GHz	similar	Similar	similar

New 802.11 Radio technologies

Current recent innovations being deployed:

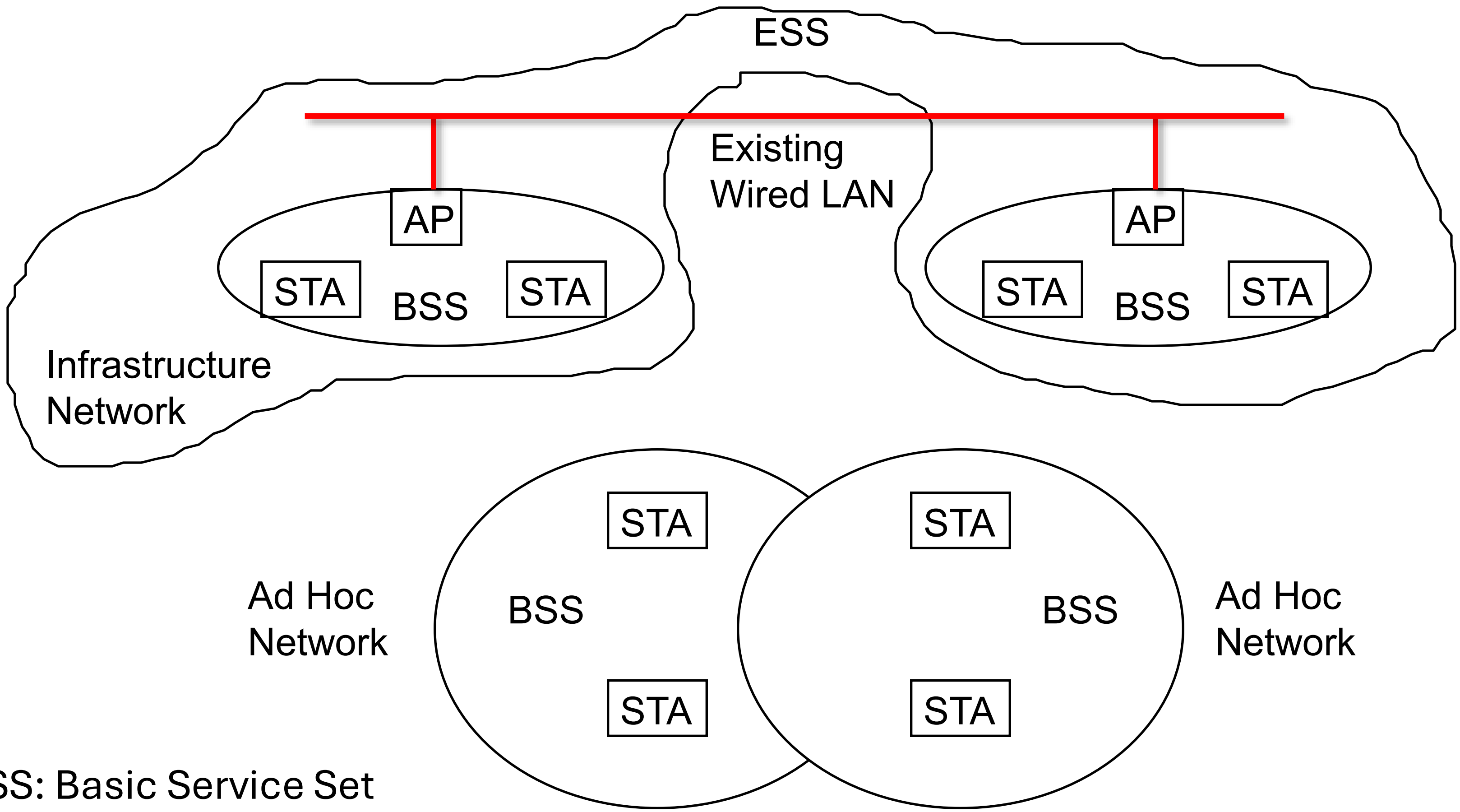
- 802.11ax – Increased throughput in 2.4, 5 (and 6) GHz bands. Increased efficiency.

WiFi6



- 802.11ay – Support for 20 Gbps in 60 GHz band.
- 802.11az – 2nd generation positioning features.
- 802.11ba – Wake up radio. Low power IoT applications
- 802.11bb – Light Communications
- 802.11bc – Enhanced Broadcast Service
- 802.11bd – Enhancements for Next Generation V2X
- 802.11be – Extremely High Throughput
- 802.11bf – WLAN Sensing [pending approval]

802.11 Architecture



BSS: Basic Service Set
ESS: Extended Service Set
DS: Distribution System

Components

- Station (STA) – Mobile Terminal
- Access Point (AP) - STA are connected to Access Points (infrastructured networks)
- Basic Service Set (BSS) – STA and AP with the same coverage and connectivity area create a BSS.
- Extended Service Set (ESS) – Multiple BSSs connected via the APs create an ESS.
- Distribution System (DS) - Contains the entity that interconnects APs

Distribution System (DS)

- The Distribution system interconnects multiple BSSs
- 802.11 standard logically separates the wireless medium from the distribution system – it does not preclude, nor demand, that the multiple media be same or different
- An Access Point (AP) is a STA that provides access to the DS by providing DS services in addition to acting as a STA.
- Data moves between BSS and the DS via an AP
- The DS and BSSs allow 802.11 to create a wireless network of arbitrary size and complexity called the Extended Service Set network (ESS)

Infrastructure vs Ad Hoc Mode

- Infrastructure mode: stations communicate with one or more access points which are connected to the wired infrastructure
  - What is deployed in practice
- Two modes of operation:
  - Distributed Control Functions - DCF
  - Point Control Functions – PCF
  - PCF is rarely used - inefficient
- Alternative is “ad hoc” mode: multi-hop, assumes no infrastructure
  - Rarely used, e.g. military
  - Hot research topic!

Industry Focus

What about Ad Hoc?

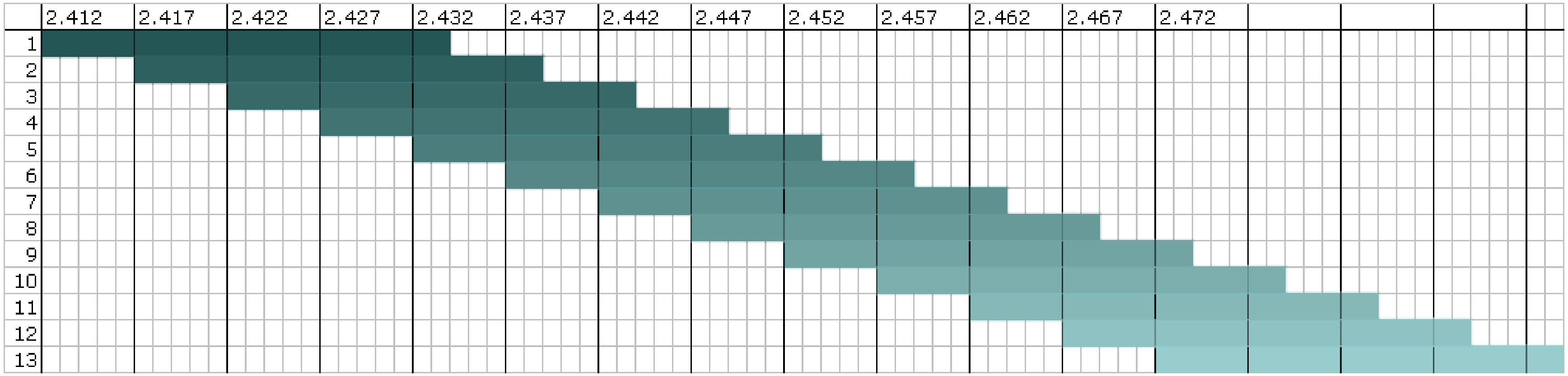
- Ad-hoc mode: no fixed network infrastructure
  - Based on an Independent BSS
  - A wireless endpoint sends and all nodes within range can pick up signal
  - Each packet carries destination and source address
  - Effectively need to implement a “network layer”
    - How do know who is in the network?
    - Routing?
    - Security?

Outline

- 802.11 standard
- ➢Physical layer
- MAC
  - DCF
  - PCF
- Advanced MAC functions

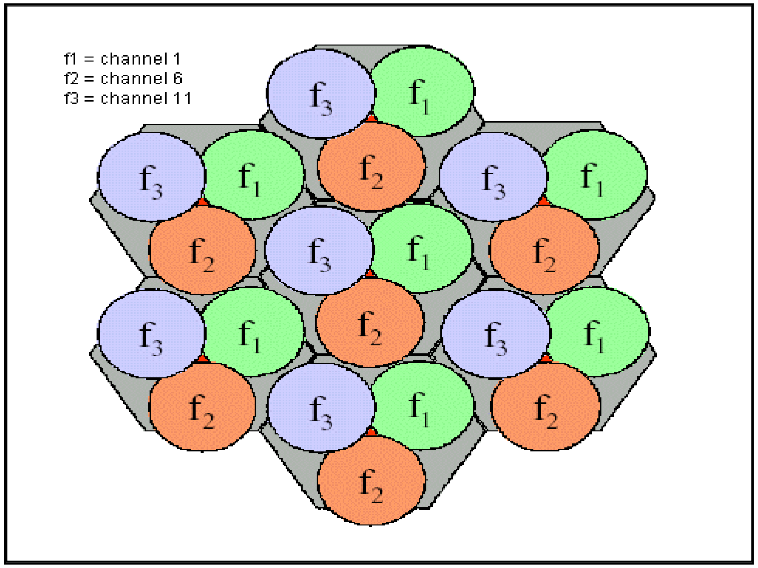
802.11 Channels (2.4GHz)

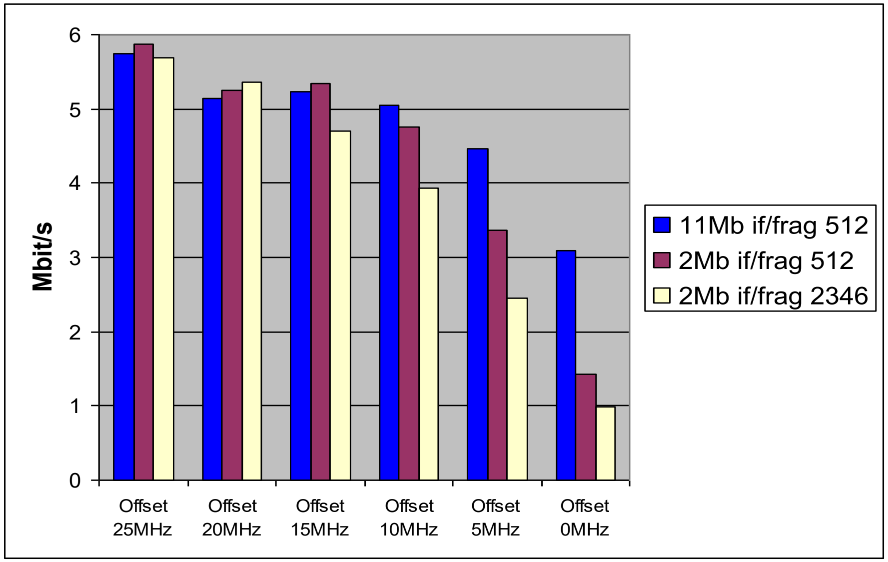
- The frequency is divided in channels
- In the UK and most of EU: 13 channels, 5MHz apart, 2.412 – 2.472 GHz
- In the US: only 11 channels
- Each channel is 22 MHz
- Significant overlap
- Best channels are 1, 6 and 11



Frequency planning

- Interference from other WLAN systems or cells
- IEEE 802.11 operates at uncontrolled ISM band
- 14 channels of 802.11 are overlapping, only 3 channels are disjointed. For example Ch1, 6, 11
- Throughput decreases with less channel spacing
- A example of frequency allocation in multi-cell network

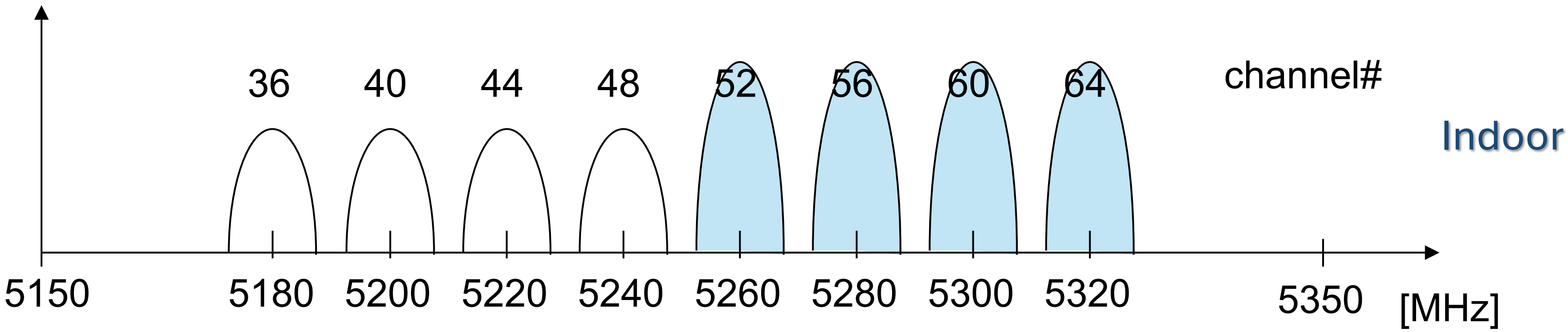




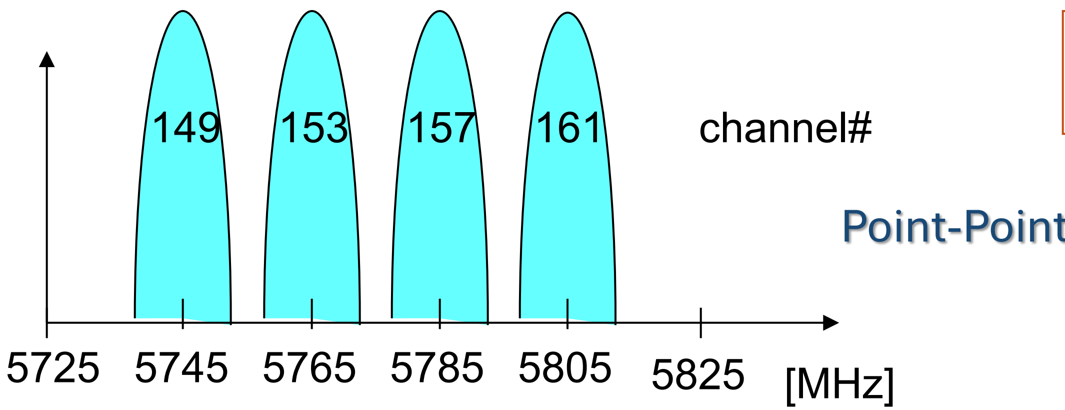
802.11 (5GHz)

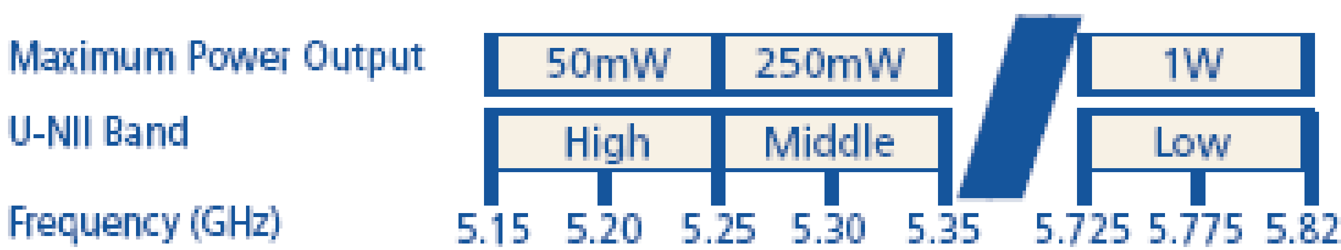
- Uses frequency division in the 5.2 and 5.7 GHz bands
- What are the benefits?
  - Greater bandwidth
  - Less potential interference (5GHz)
  - More non-overlapping channels
- But does not provide interoperability
  - Interoperability at chipset level

Example: 802.11a Physical Channels

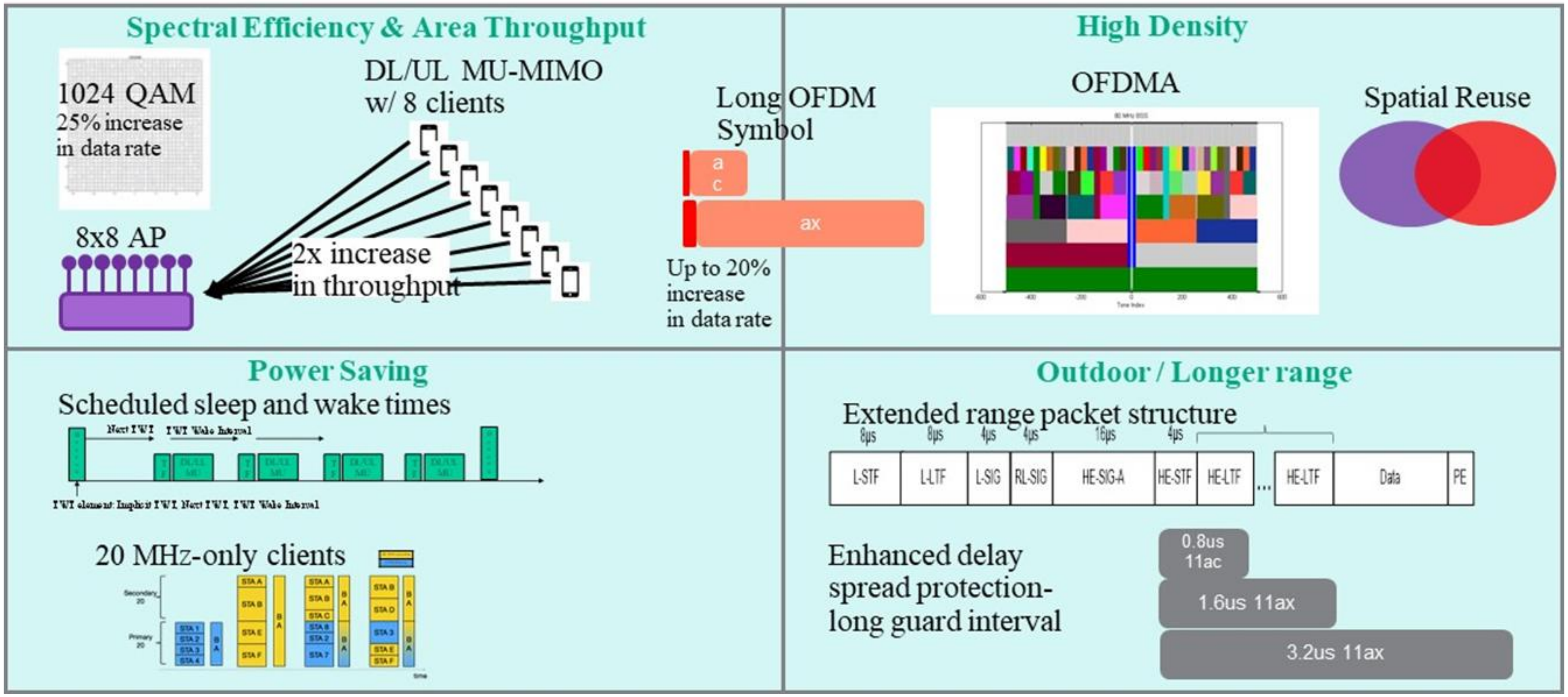


center frequency =
5000 + 5*channel number [MHz]



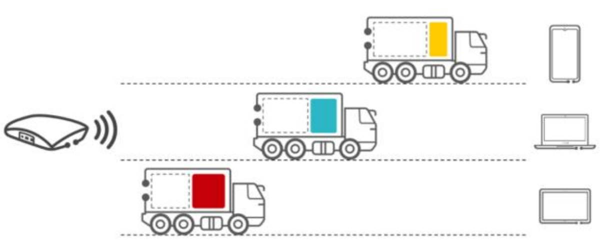


WiFi 6 radio layer enhancements

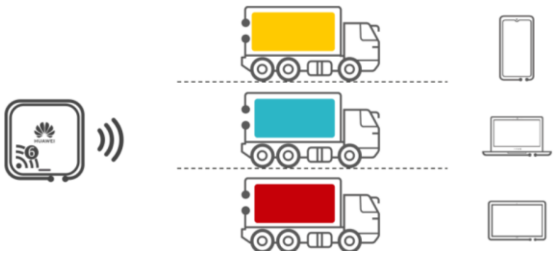


OFDMA – Orthogonal Frequency-division Multiple Access

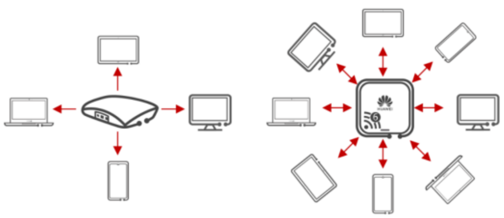
- Multi-user version of OFDM (Orthogonal frequency-division Multiplexing)
- Divides channel resources into multiple Resource Units (RUs)
- Different users are allocated these Rus
- Data of multiple users can be sent on one channel simultaneously
- New in Wi-Fi 6
- So:
  - The AP communicates with multiple users during one transmission period



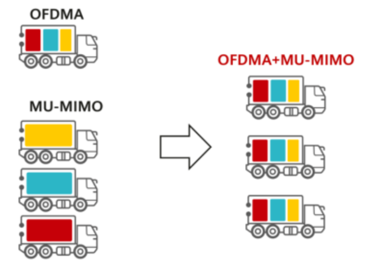
MU-MIMO – Multi-user Multiple-Input and Multiple-Output



- Introduced in Wi-Fi 5
- # antennas in APs is greater than in terminals
  - Unable to make the most out of channel resources
  - E.g.: in 802.11ac, which is only in 5GH<, each spatial stream (1x1 MIMO) has a max PHY rate of 433 Mbps when used with 80 MHz-wide channels
  - Single user transmission
- With MU-MIMO
  - AP communicates with multiple terminals simultaneou
  - Wi-Fi 5: 4x4 DL MU-MIMO (4 * 433 in downlink only)
  - Wi-Fi 6: 8x8 UL/DL MU-MIMO (8 * 433 in uplink/downlink)
- MU-MIMO



OFDMA + MU-MIMO



- MU-MIMO
  - Physically divides network resources to increase capacity and efficiency in high-bandwidth applications (i.e., video streaming and download)
  - Increases spatial stream utilization and effective bandwidth while also lowering latency
  - Prone to impact from terminals
- OFDMA
  - Supports multi-channel transmission in the frequency domain
  - Ideal for low-bandwidth, small-packet applications (e.g., web browsing, IM)
  - Increases spatial stream utilization and queueing time.
  - Stable and resilient to impact from terminals
- MU-MIMO + OFDMA = Complementary operation
  - Optimal resource allocation based on services, via joint scheduling

Wi-Fi 7

- 6 GHz band!
  - In reality, Wi-Fi 6E also had…
  - Maximum channel bandwidth: 320MHz
    - Wi-fi 6: 160MHz
    - Analogy: highways with more lanes
- Quadrature Amplitude Modulation (QAM)
  - Data is represented by combinations of amplitudes, phases or frequencies
  - The encoding scheme determines the number of bits that can be carried in a symbol
  - Wi-Fi 6 uses 1024-QAM (10 bits) … Wi-Fi 7 used 4096-AQM (12 bits→1.2x +)
- Multi-link Operation (MLO): 2.4GHz + 5GHz+ 6 GHz
- Peak transmission rate:
  - Wi-fi 6: 9.6Gbps
  - Wi-Fi 7: 23.06Gbps (x2.4 times!)

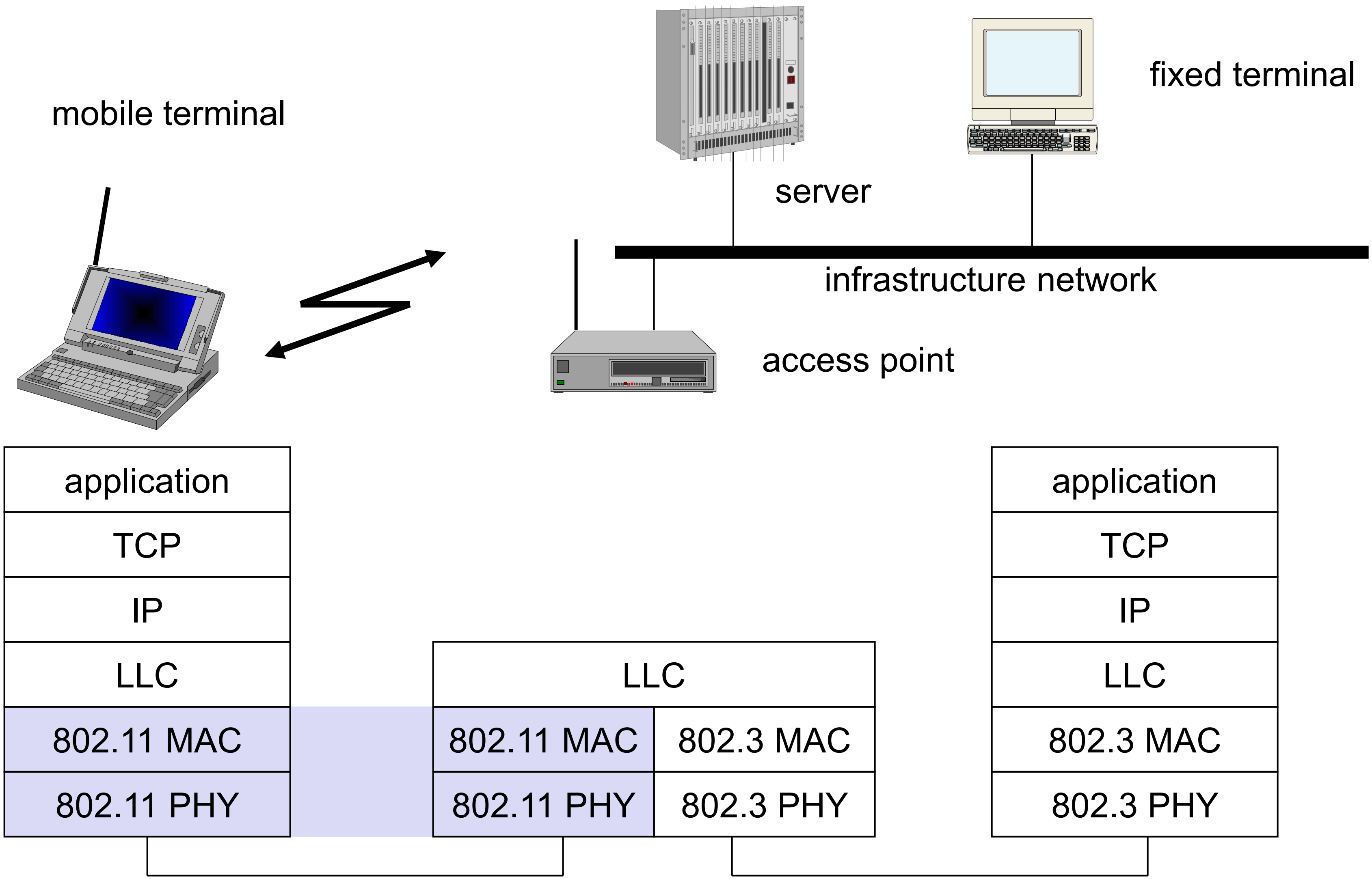
Wi-Fi 8

- Multi-AP Coordination
- Channel BW 320 MHz (and more)
- 8192 QAM Modulation (higher quantity of signals modulated)
- mmWave spectrum
- Distributed Multi-Link Operation

Outline

- 802.11 standard
- Physical layer
- ➢MAC
  - DCF
  - PCF
- Advanced MAC functions

802.11- in the TCP/IP stack



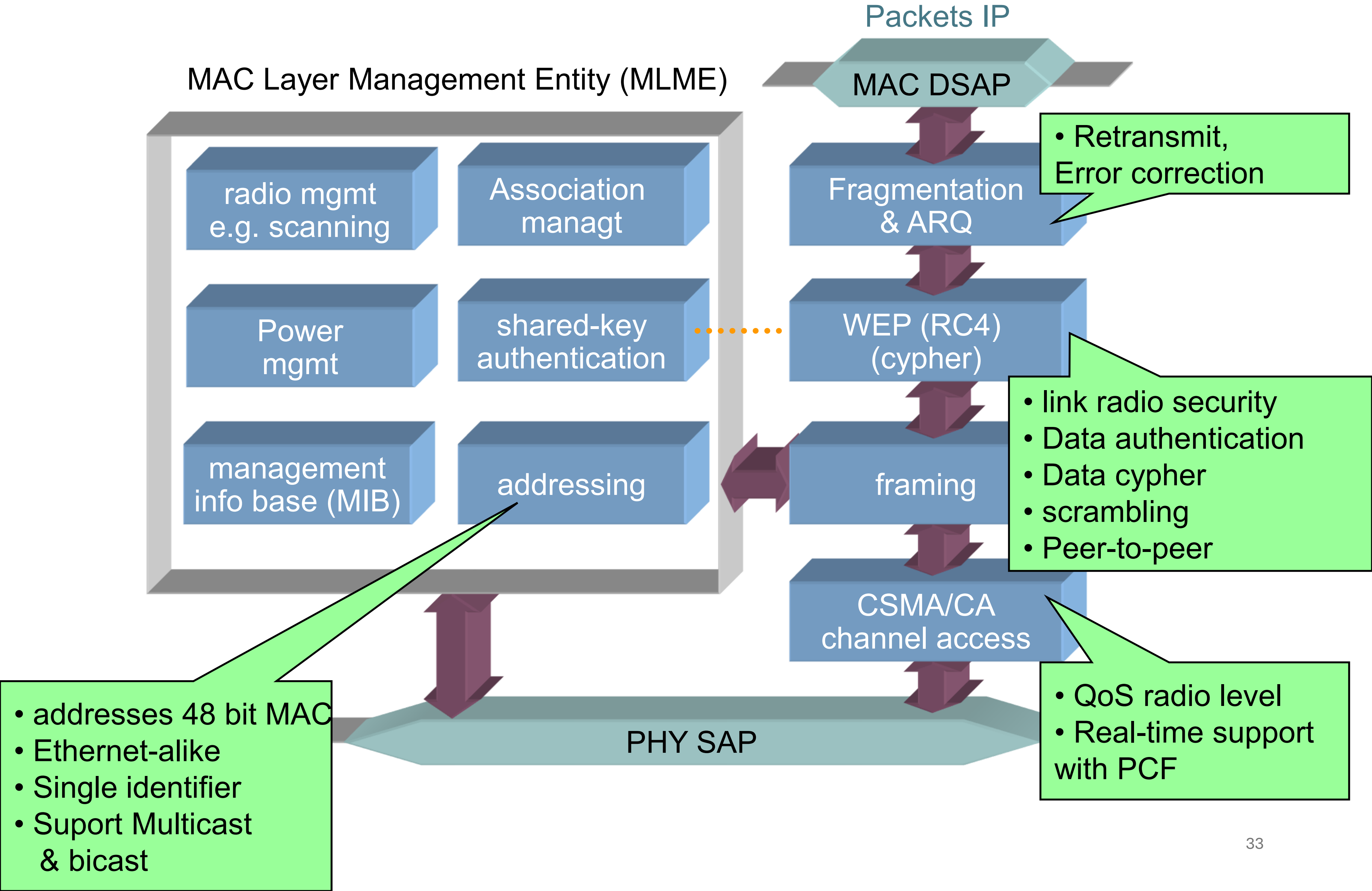
802.11 MAC Overview

- Uses variant of Carrier Sense Multiple Access with Collision Avoidance (CS/MACA)
  - RTS/CTS used for addressing hidden-nodes
- Automatic Repeat Request (ARQ)
  - Error control method for reliability
  - All frames have to be properly ACK, or timeout occurs
- Two operating modes:
  - Infra-structured network (Access point)
  - Ad-Hoc networks (without access point)
- Power saving support
- Wired Equivalent Privacy (WEP)
- MAC management
- Independent of the physical layer or of operating mode

Features of 802.11 MAC protocol

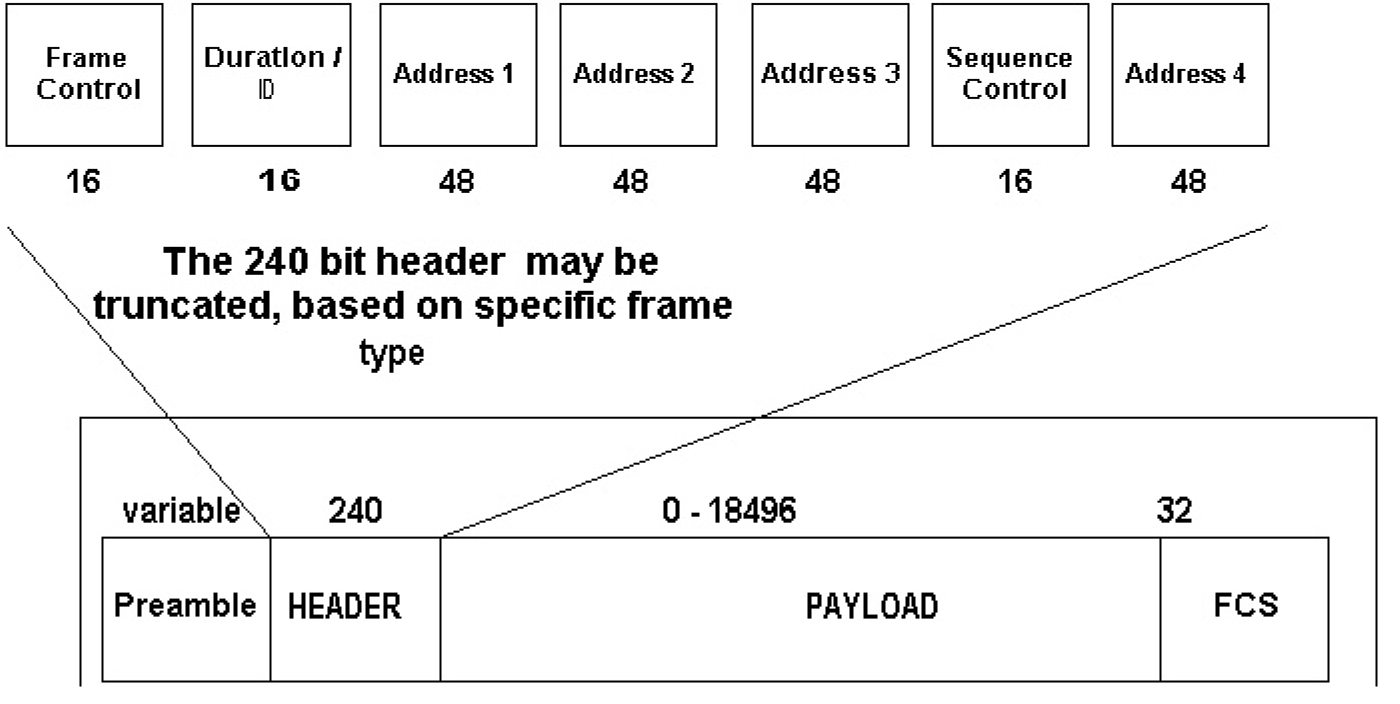
- Fair control access
  - Supports Media Access Control functionalities
    - Addressing
    - CSMA/CA
- Protection of data
  - Error detection (FCS – Frame Check Sequence)
    - Compares number with received values
  - Error correction (ACK frame)
- Reliable data delivery
  - Fragmentation
  - Flow control: stop-and-wait (the next frame is only sent after an ACK from the previous one is received)

MAC IEEE802.11

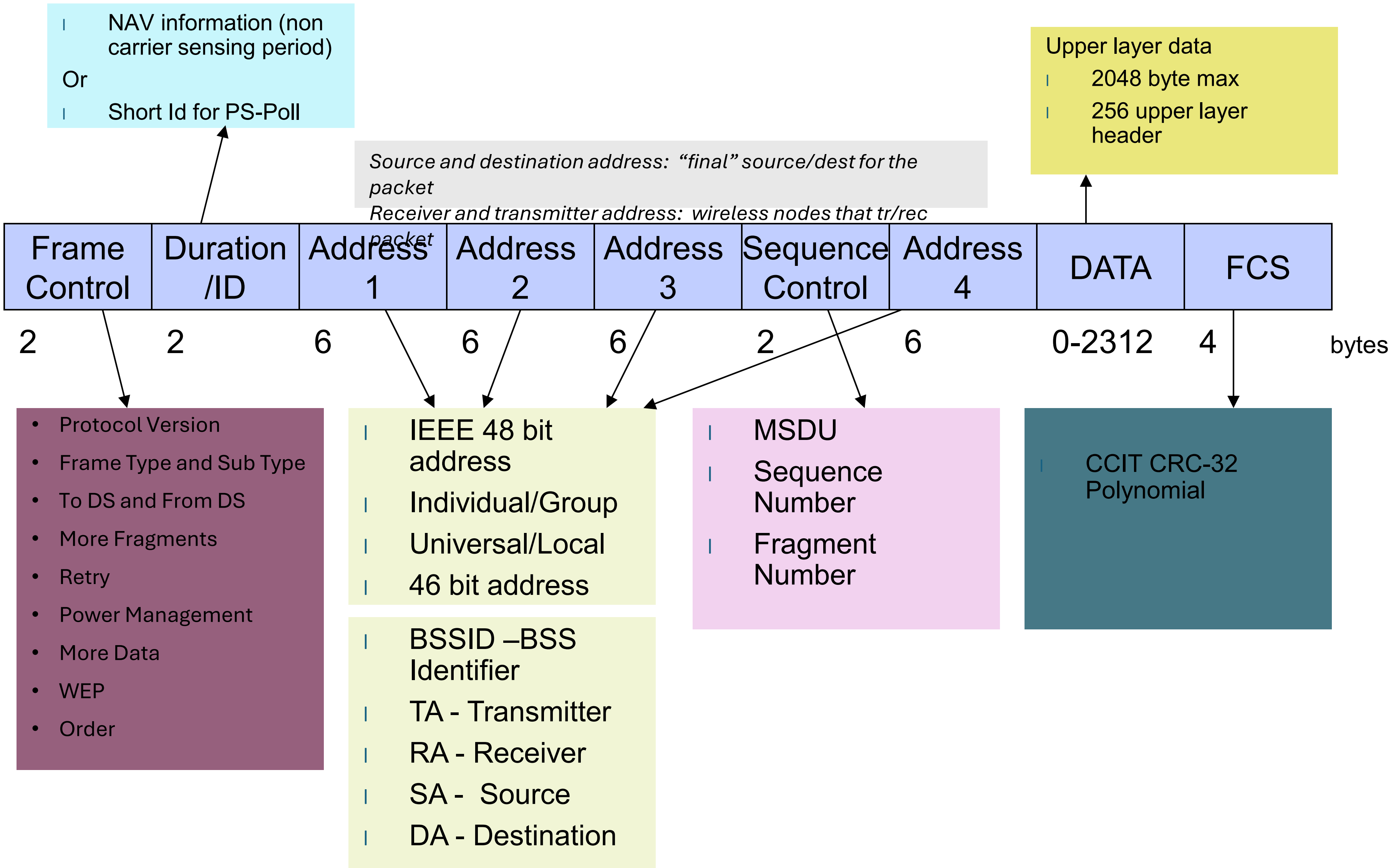


802.11 Frames

- Three types of frames
  - control: RTS, CTS, ACK
  - Management
  - Data
- Header depends on the frame type



Frame Format



Packet Types

- Type/sub-type field is used to indicate the type of the frame
- Management:
  - Association/Authentication/Beacon
- Control
  - RTS, CTS, CF-end, ACK
- Data
  - Data only, or Data + CF-ACK, or Data + CF-Poll or Data + CF-Poll + CF-ACK

CF → Contention Free

Some More Fields

- Duration/ID: Duration in DCF mode/ID is used in PCF mode
- More Frag: 802.11 supports fragmentation of data
- More Data: In polling mode, station indicates it has more data to send when replying to CF-POLL
- RETRY is 1 if frame is a retransmission;
- WEP (Wired Equivalent Privacy) is 1 if frame is WEP coded
- Power Mgmt is 1 if in Power Save Mode;
- Order = 1 for strictly ordered service

Multi-bit Rate

- 802.11 allows for multiple bit rates
  - Allows for adaptation to channel conditions
  - Specific rates dependent on the version
- Algorithm for selecting the rate is not defined by the standard – left to vendors
- Packets have multi-rate format
  - Different parts of the packet are sent at different rates
- Short vs Long preamble
  - Preamble allows the receiver to synchronize with the transmitter
  - Additional data is added to the header to help check for transmission errors
  - Long
    - Older, requires more data to help check for transmission errors (does it better)
  - Short
    - Less data = faster

Addressing Fields

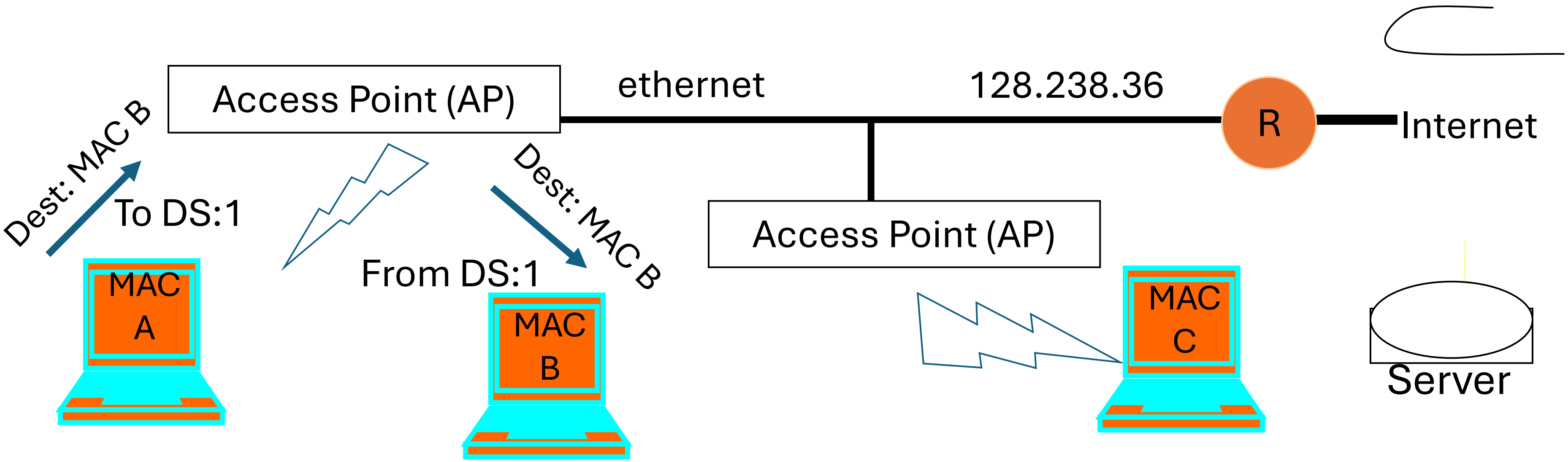
To DS	From DS	Message	Address 1	Address 2	Address 3	Address 4
0	0	station-to-station frames in an IBSS; all mgmt/control frames	DA	SA	BSSID	N/A
0	1	From AP to station	DA	BSSID	SA	N/A
1	0	From station to AP	BSSID	SA	DA	N/A
1	1	From one AP to another in same DS	RA	TA	DA	SA

RA: Receiver Address TA: Transmitter Address
DA: Destination Address SA: Source Address
BSSID: MAC address of AP in an infrastructure BSS

Data Flow Examples

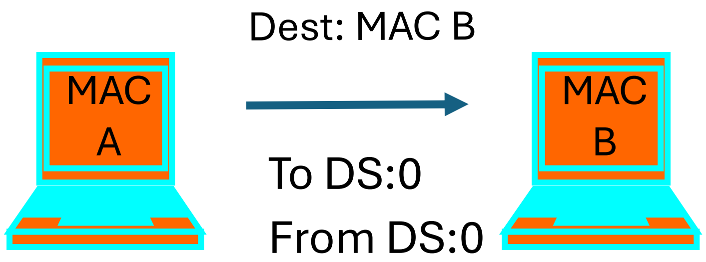
- Case 1: Packet from a station under one AP to another in same AP's coverage area
- Case 2: Packet between stations in an IBSS
- Case 3: Packet from an 802.11 station to a wired server on the Internet
- Case 4: Packet from an Internet server to an 802.11 station

Case 1: Communication Inside BSS



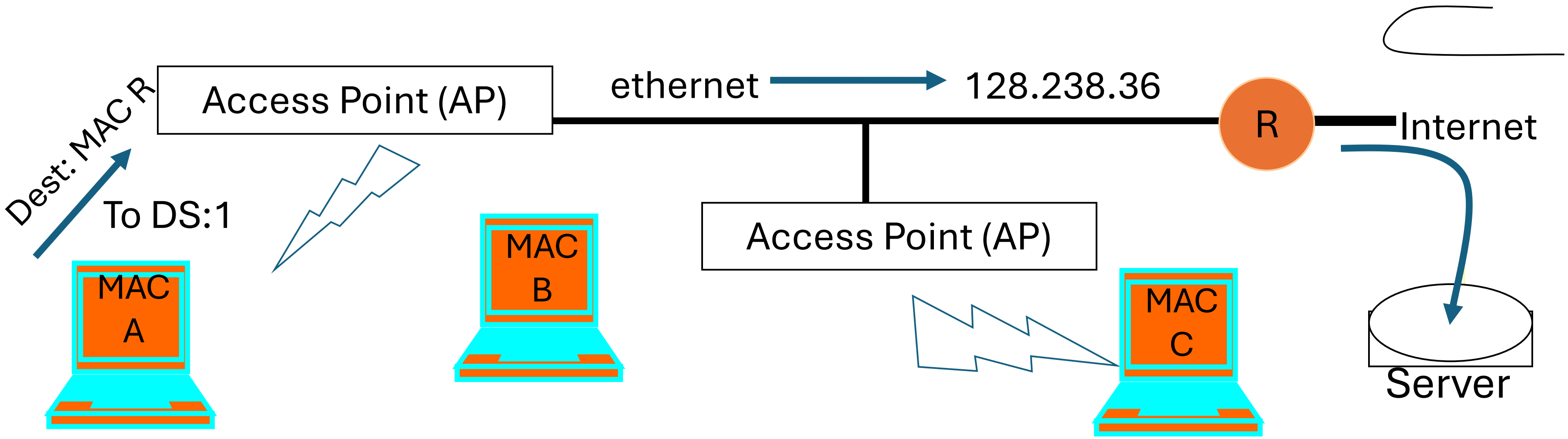
- AP knows which stations are registered with it so it knows when it can send frame directly to the destination

Case 2: Ad Hoc



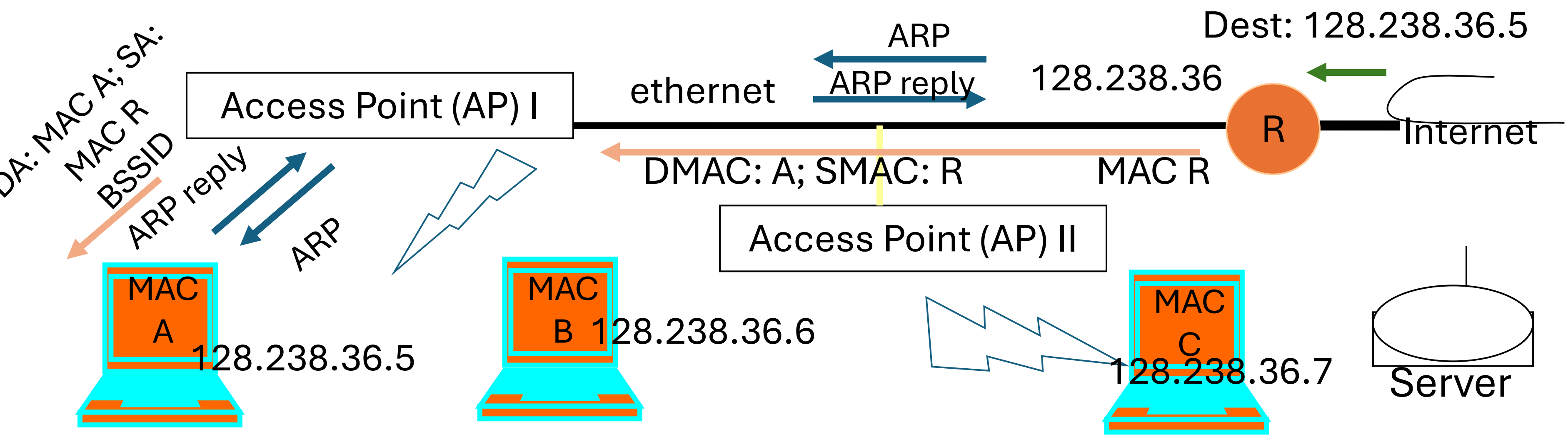
- Direct transmit only in IBSS (Independent BSS), i.e., without AP
- Note:
  - in infrastructure mode (i.e., when AP is present), even if B can hear A, A sends the frame to the AP, and AP relays it to B

Case 3: To the Internet



- MAC A determines IP address of the server (using DNS)
- From the IP address, it determines that server is in a different subnet
- Hence it sets MAC R as DA;
  - Address 1: BSSID, Address 2: MAC A; Address 3: DA
- AP will look at the DA address and send it on the ethernet
  - AP is an 802.11 to ethernet bridge
- Router R will relay it to server

Case 4: From Internet to Station



- Packet arrives at router R – uses ARP to resolve destination IP address
  - AP knows nothing about IP addresses, so it will simply broadcast ARP on its wireless link
  - DA = all ones – broadcast address on the ARP
- MAC A host replies with its MAC address (ARP reply)
  - AP passes on reply to router
- Router sends data packet, which the AP simply forwards because it knows that MAC A is registered

Let’s stop here!
Next: Practical Work!