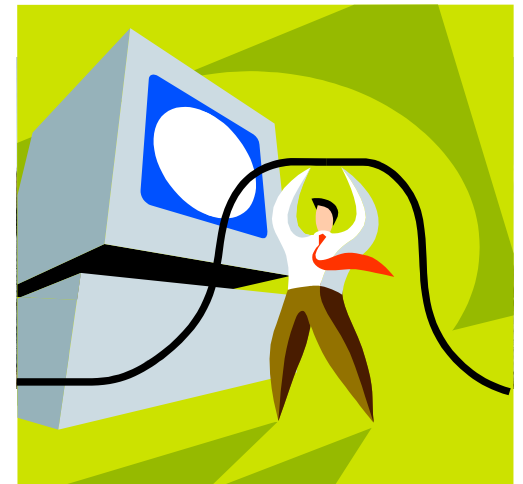




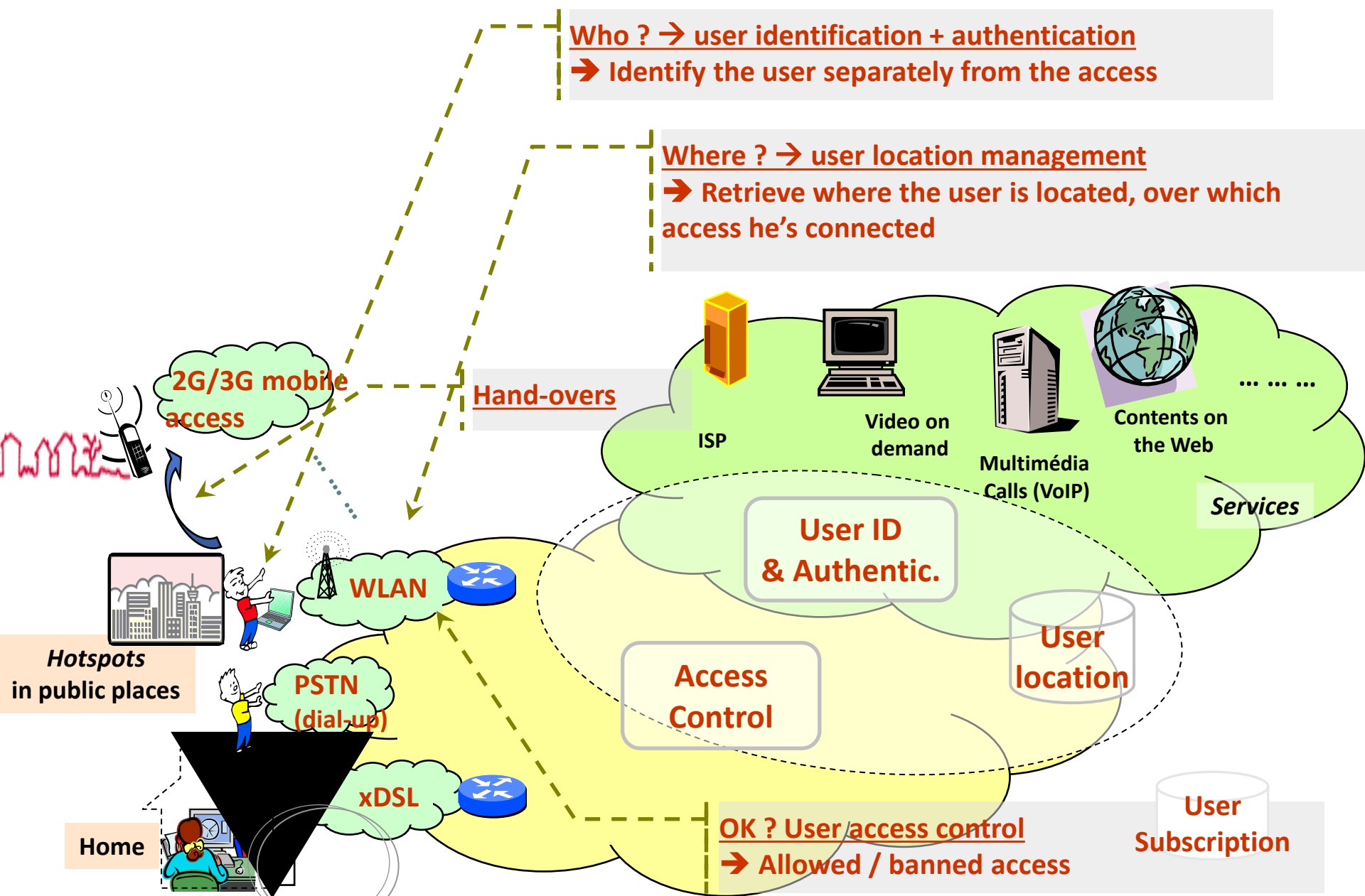
# Mobile Networks

Connections and structures





# Requirements in a mobile network





# Types of connections

- Point-to-point networks
  - Communication points need to be in line of sight (LoS) (e.g. satellite).
- Diffusion networks
  - There is no specific physical relationship between the two communication points (e.g. 802.11)
- Semi-diffusion networks
  - Require some limitations in the relative positioning of the communication points (e.g. Infrared)



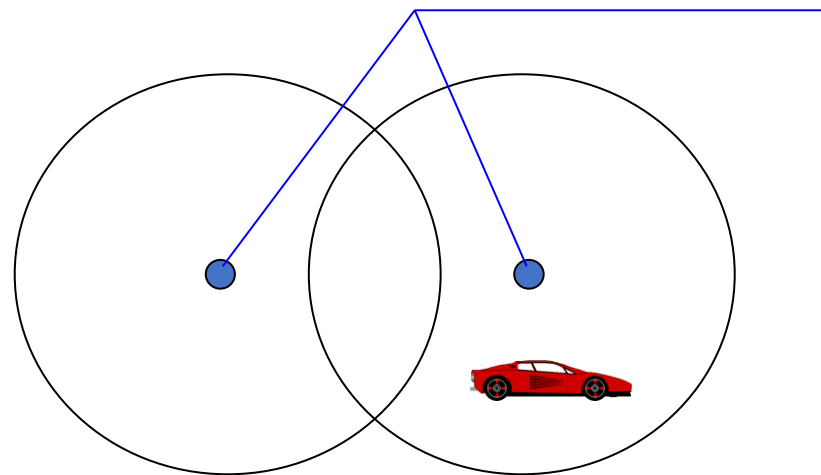
# Cell

- Smallest physical entity that allows the access to mobile entities
- Cell  $\neq$  point-to-point connection
- Associated to the physical mechanism of information transfer (radio technologies or infrared)
- Cell
  - Terminal oriented or
  - Defined by a base station
- There is overlapping of different cells in a wireless network



# 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



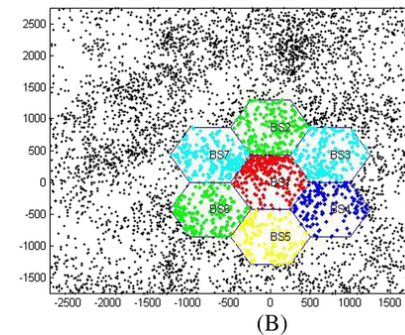
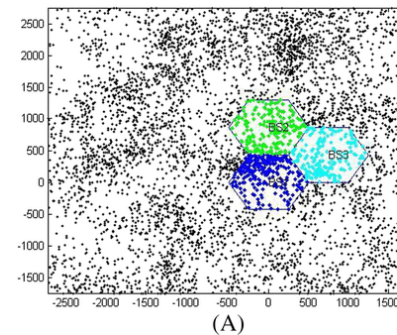
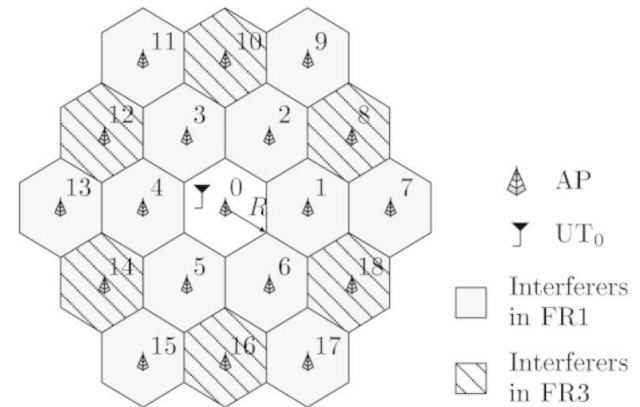
Cell coverage size is

- Highly variable
- Depends on the technology
- Depends on the number of users



# Cells

- Coverage size:
  - 100m to 35 km (GSM)
  - Microcells: closed spaces
  - Hat cell: set of cells
    - Avoid frequent handoffs in critical places
- Format:
  - Teoretically analyzed as a hexagon
  - Reality: it depends on the place
- BS positioning:
  - Cell centrally excited
    - BS in the center of the cell, with omni-directional antenna
  - Cell side excited
    - BSs in the vertices (in three)
    - Directional antennas





# 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



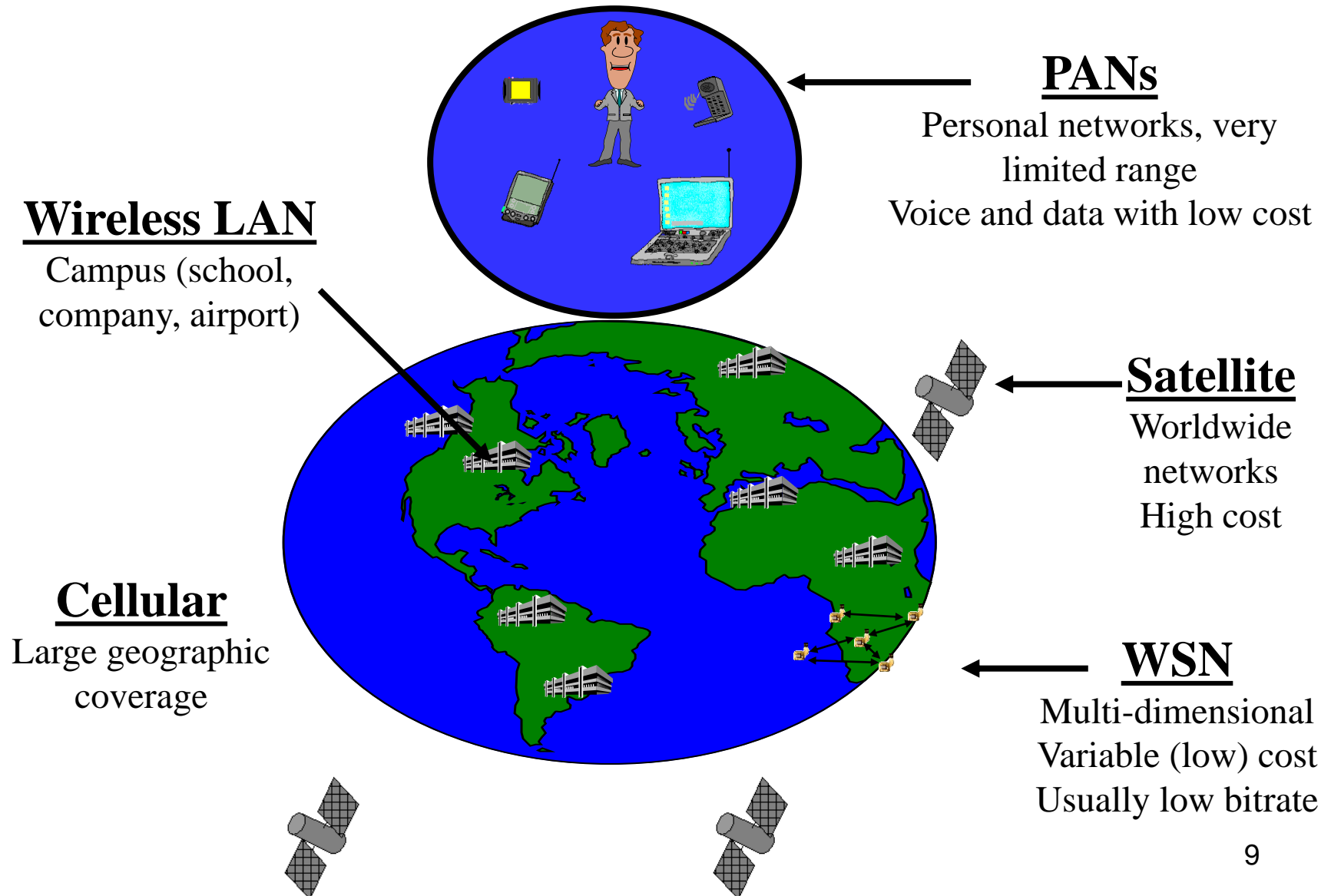
# Wireless networks

- Networks are designed according to the number of users and coverage area
- In wireless networks there are several scales on number of users and coverage area
  - Personal: PANs → Bluetooth
  - Local: LANs → IEEE 802.11
  - Regional: WANs → GSM, UMTS
  - Worldwide : Sattelite → Iridium



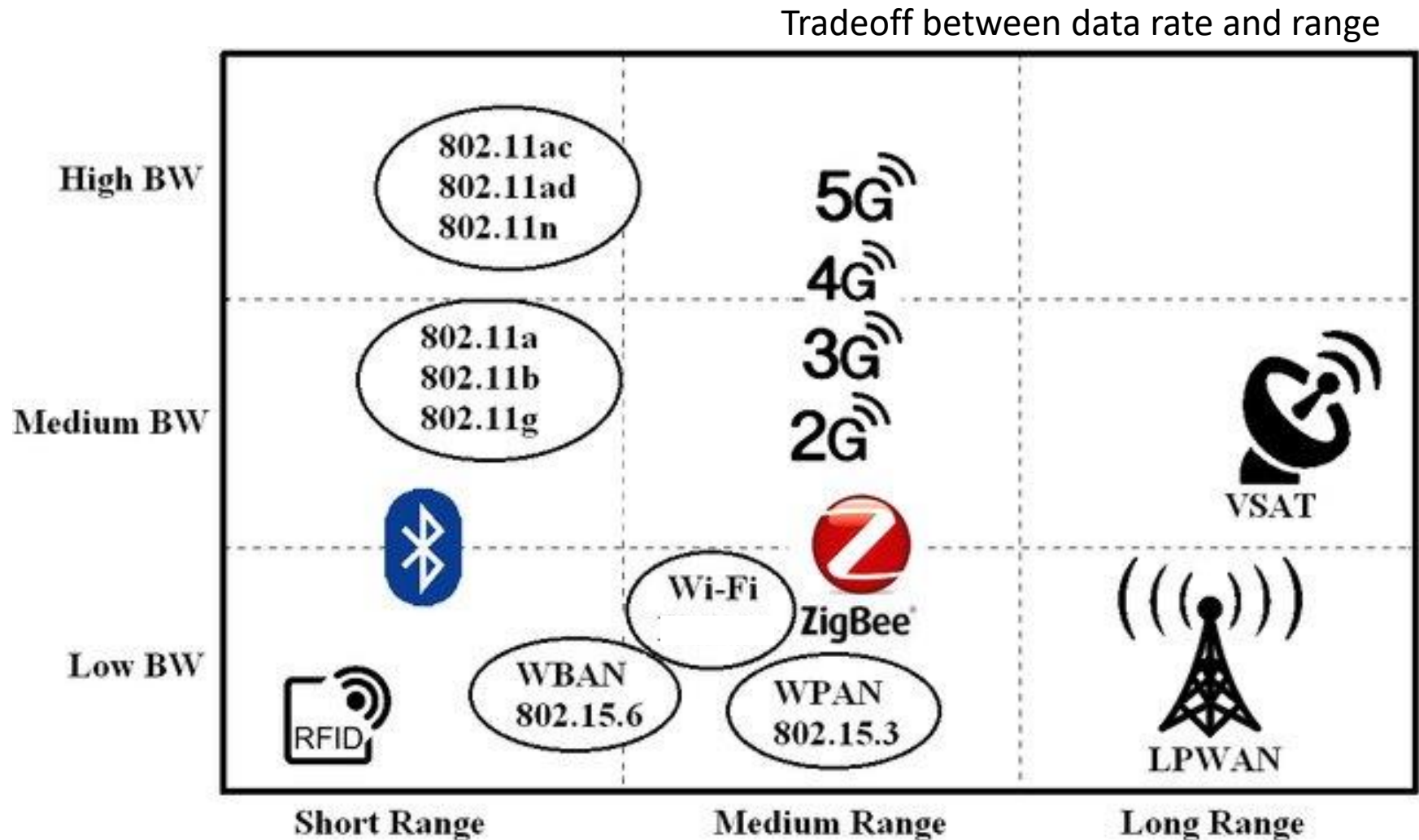


# Types of Wireless networks





# Comparison Between Wireless Technologies





# Wireless Technologies (@~2000)

	<b>PAN</b>	<b>LAN</b>	<b>MAN</b>	<b>MAN</b>
<b><i>Access speed</i></b>	1-2Mb	11Mb	Mbs	>56kb
<b><i>Range</i></b>	10m	100-400m	kms	global
<b><i>Standard</i></b>	IEEE 802.15	IEEE 802.11	IEEE 802.16	GPRS 1xRTT
<b><i>Scalability</i></b>	Low device specific	Medium ethernet	Infra structure	High regional Infrastructure
<b><i>Architecture</i></b>	FHSS	DSSS	cellular	cellular

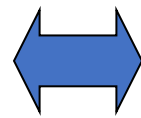


# Standardization of Wireless Networks

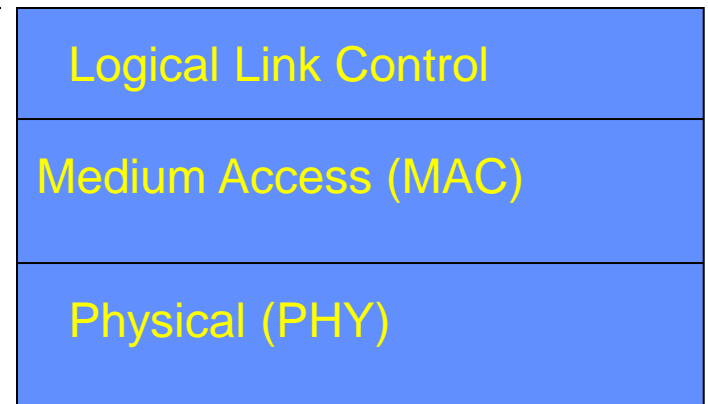
- Wireless networks are standardized by IEEE.
- Under 802 LAN MAN standards committee.

LAN – Local Area Network  
MAN – Metro Area Network

ISO  
OSI  
7-layer  
model



IEEE 802  
standards





# The 802 Class of Standards

- Early list on next slide
- Some standards apply to all 802 technologies
  - E.g. 802.2 is LLC
  - Important for inter operability
- Some standards are for technologies that are outdated
  - Not actively deployed anymore
  - E.g. 802.6

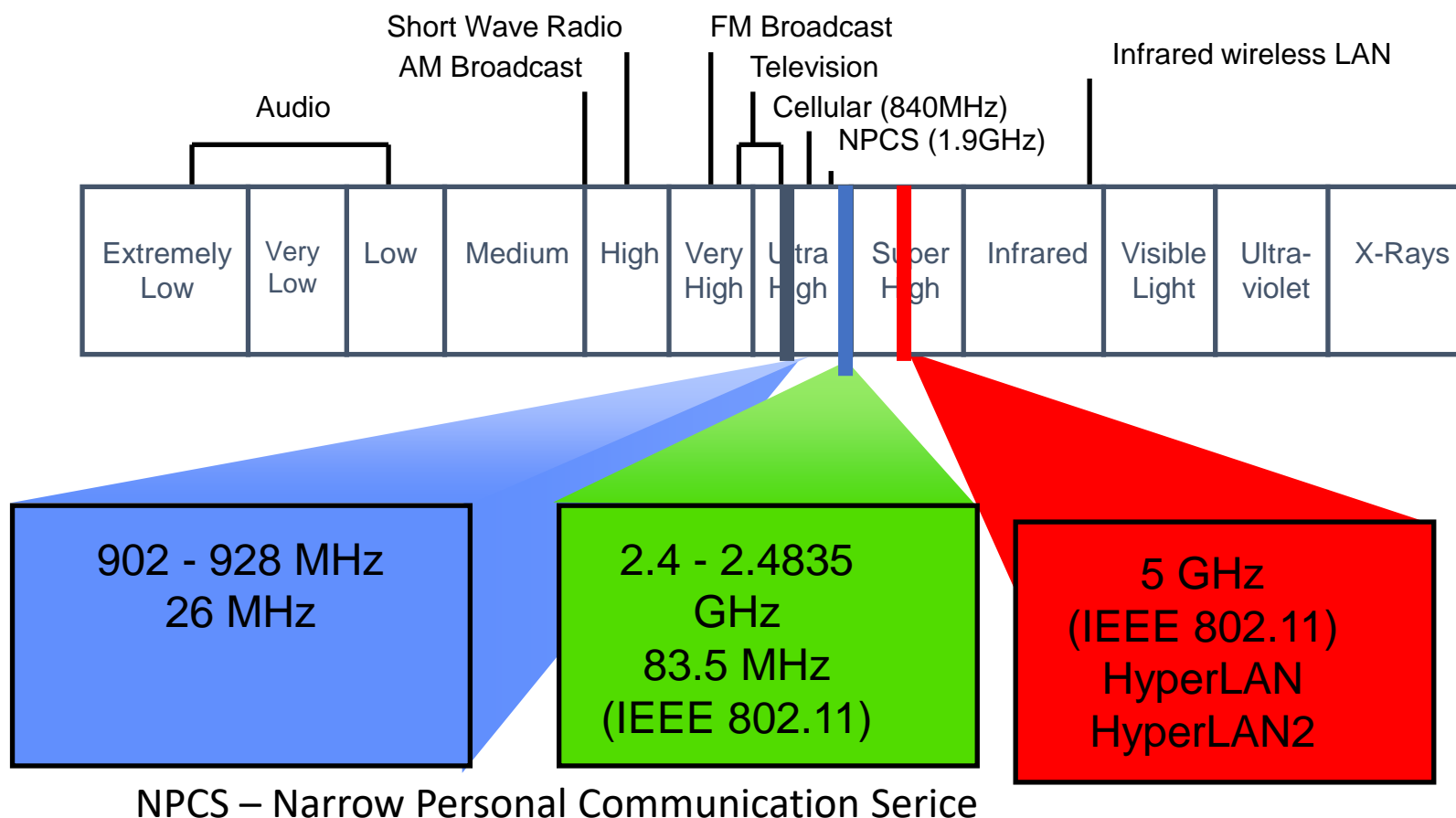


- 802.1 Overview Document Containing the Reference Model, Tutorial, and Glossary
- 802.1 b Specification for LAN Traffic Prioritization
- 802.1 q Virtual Bridged LANs
- 802.2 Logical Link Control
- 802.3 Contention Bus Standard 1 Obase 5 (Thick Net)
  - 802.3a Contention Bus Standard 10base 2 (Thin Net)
  - 802.3b Broadband Contention Bus Standard 10broad 36
  - 802.3d Fiber-Optic InterRepeater Link (FOIRL)
  - 802.3e Contention Bus Standard 1 base 5 (Starlan)
  - 802.3i Twisted-Pair Standard 10base T
  - 802.3j Contention Bus Standard for Fiber Optics 10base F
  - 802.3u 100-Mb/s Contention Bus Standard 100base T
  - 802.3x Full-Duplex Ethernet
  - 802.3z Gigabit Ethernet
  - 802.3ab Gigabit Ethernet over Category 5 UTP
- 802.4 Token Bus Standard
- 802.5 Token Ring Standard
  - 802.5b Token Ring Standard 4 Mb/s over Unshielded Twisted-Pair
  - 802.5f Token Ring Standard 16-Mb/s Operation
- 802.6 Metropolitan Area Network DQDB
- 802.7 Broadband LAN Recommended Practices
- 802.8 Fiber-Optic Contention Network Practices
- 802.9a Integrated Voice and Data LAN
- 802.10 Interoperable LAN Security
- 802.11 Wireless LAN Standard
- 802.12 Contention Bus Standard 1 OOVG AnyLAN
- 802.15 Wireless Personal Area Network
- 802.16 Wireless MAN Standard



# Frequency Bands

- Industrial, Scientific, and Medical (ISM) bands
- Unlicensed, 22 MHz channel bandwidth





802.11





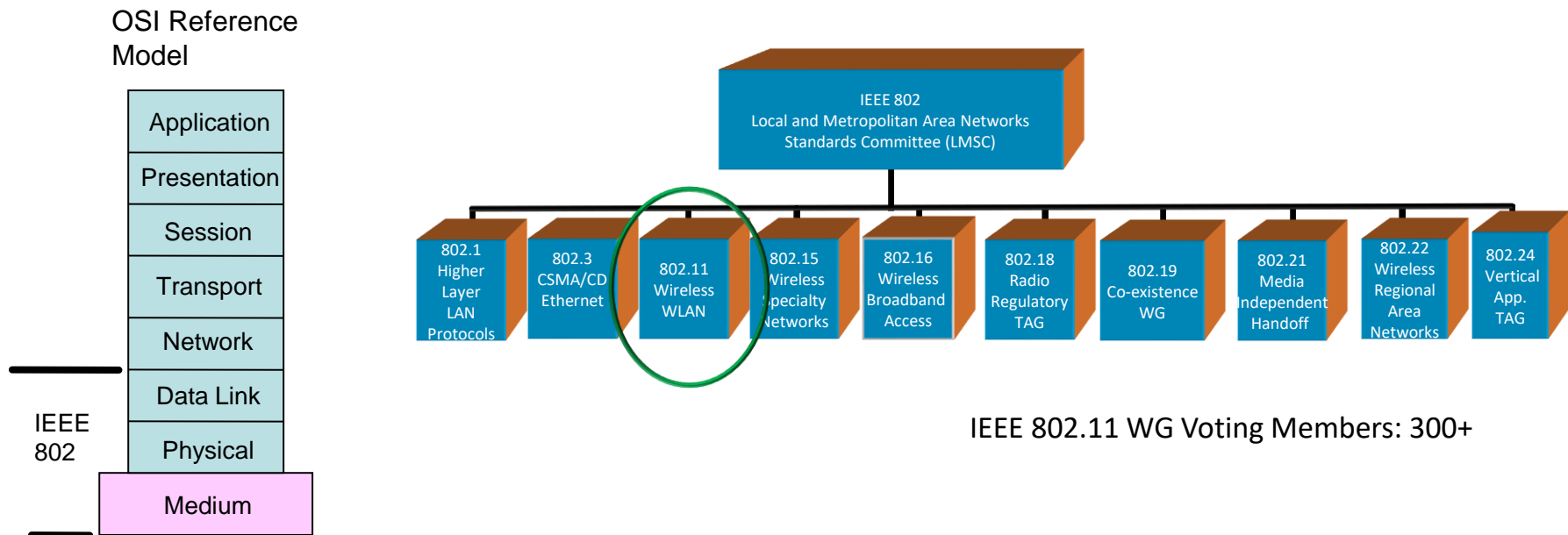
# Outline

- 802.11 standard
  - Physical layer
- MAC
  - DCF – Distributed Coordination Function
  - PCF – Point Coordination Function
- Advanced MAC functions



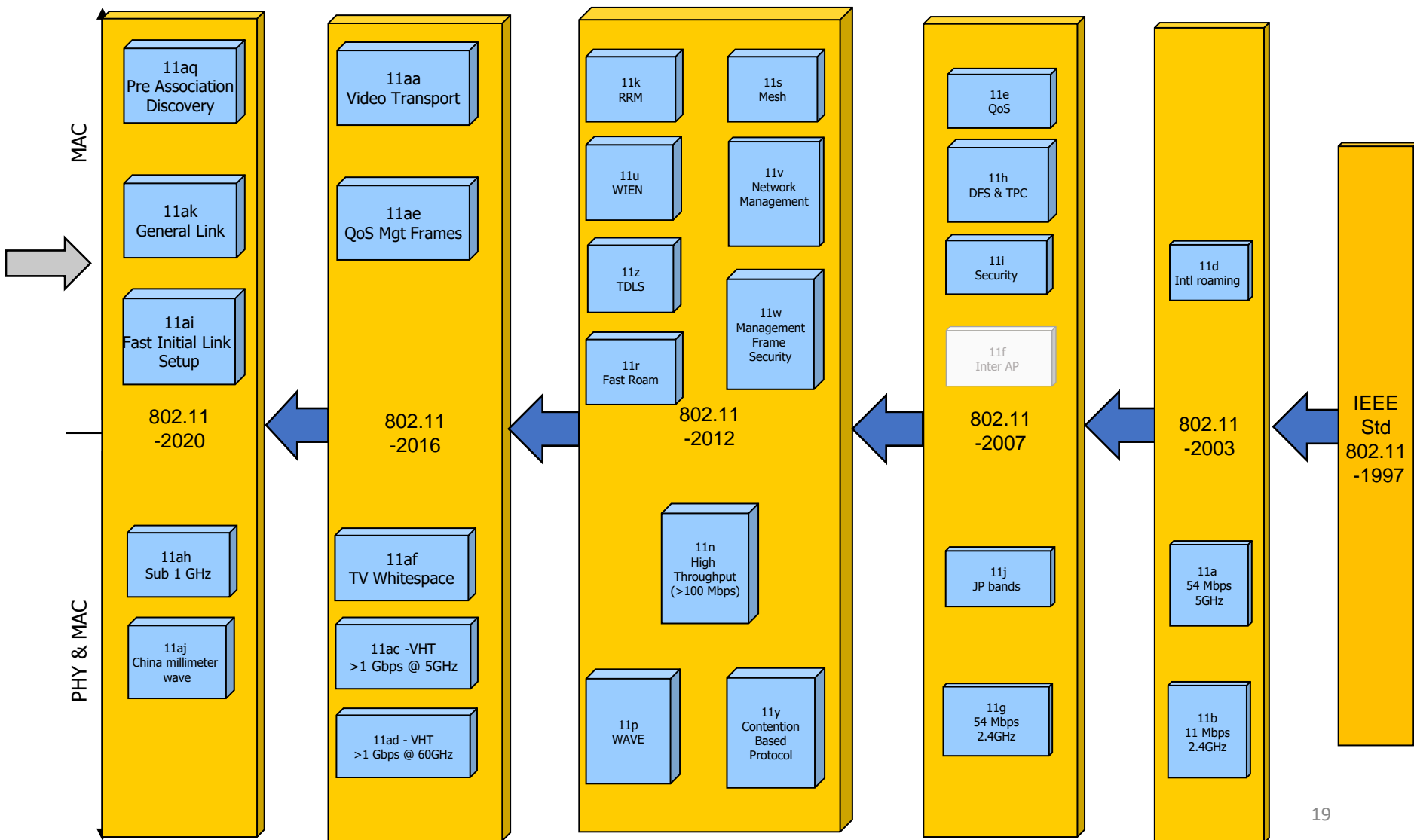
# The IEEE 802.11 Working Group

- Standard: Focus on link and physical layers of the network stack
- Leverage IETF protocols for upper layers





## Development of the IEEE 802.11 Standard is ongoing since 1997



Old versions are being deprecated by new versions, and new features are added as time goes by.



# 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



# 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)	TBD	2.4/5/6 GHz	?	40 Gbps	?
802.11ay	2021	60 GHz	20 Gbps	20-40 Gbps	300-500m



# 802.11 Radio technologies evolution

**802.11az – 2<sup>nd</sup> generation positioning features**

**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**

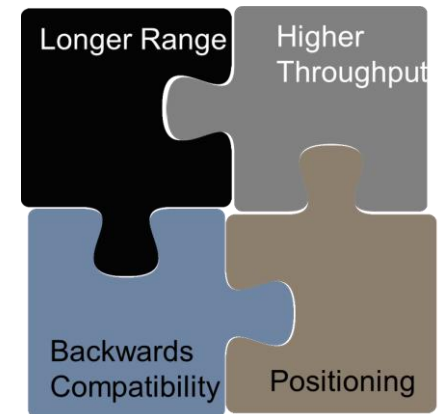
**802.11bi – Randomized MAC Addresses**

**802.11bh – Enhanced Data Privacy**

**Ultra High Reliability Study Group**

**AI/ML Topic Interest Group**

**Ambient Power for IOT Topic Interest Group**



<https://www.ieee802.org/11/IEEE%20802-11-Overview-and-Amendments-Under-Development.pptx>



# IEEE 802.11 innovation

- Market demands and new technology push for new 802.11 standards
- Demand for throughput
  - Continuing exponential demand for throughput ([802.11ax](#) and [802.11ay](#), [802.11be](#))
  - Most (50-80%, depending on the country) of the world's mobile data is carried on 802.11 (Wi-Fi) devices
- New usage models / features
  - Dense deployments ([802.11ax](#)), Indoor Location ([802.11az](#)),
  - Automotive (IEEE Std 802.11p, Next Gen V2X), Internet of Things ([802.11ah](#))
  - Low Power applications ([802.11ba](#))
  - WLAN Sensing ([802.11bf](#) – pending approval)
- Technical capabilities
  - MIMO (IEEE Std 802.11n, 802.11ac, [802.11ay](#)) and OFDMA ([802.11ax](#))
  - 60 GHz radios ([802.11ay](#))
- Changes to regulation
  - TV whitespaces (IEEE Std 802.11af), Radar detection (IEEE Std 802.11h), 6GHz ([802.11ax](#), [802.11be](#))
  - Coexistence and radio performance rules (e.g., ETSI BRAN, ITU-R)



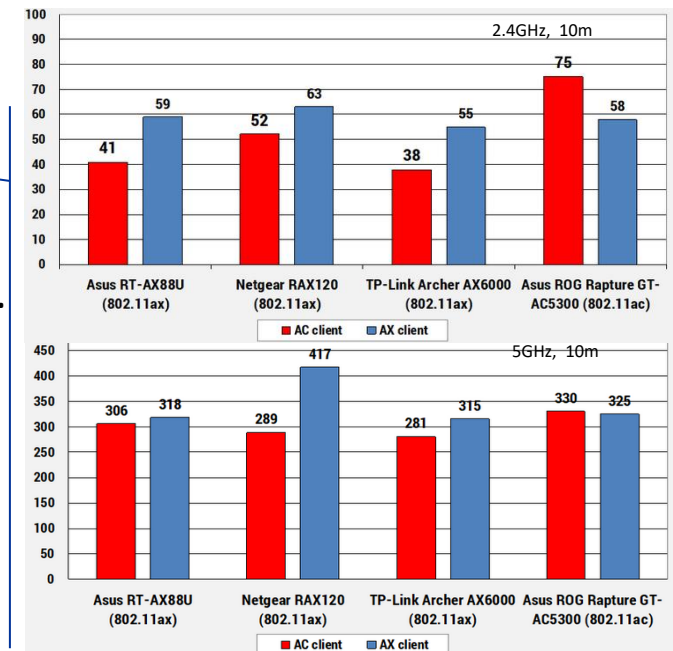
# New 802.11 Radio technologies

Current recent innovations being deployed:

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

## WiFi6

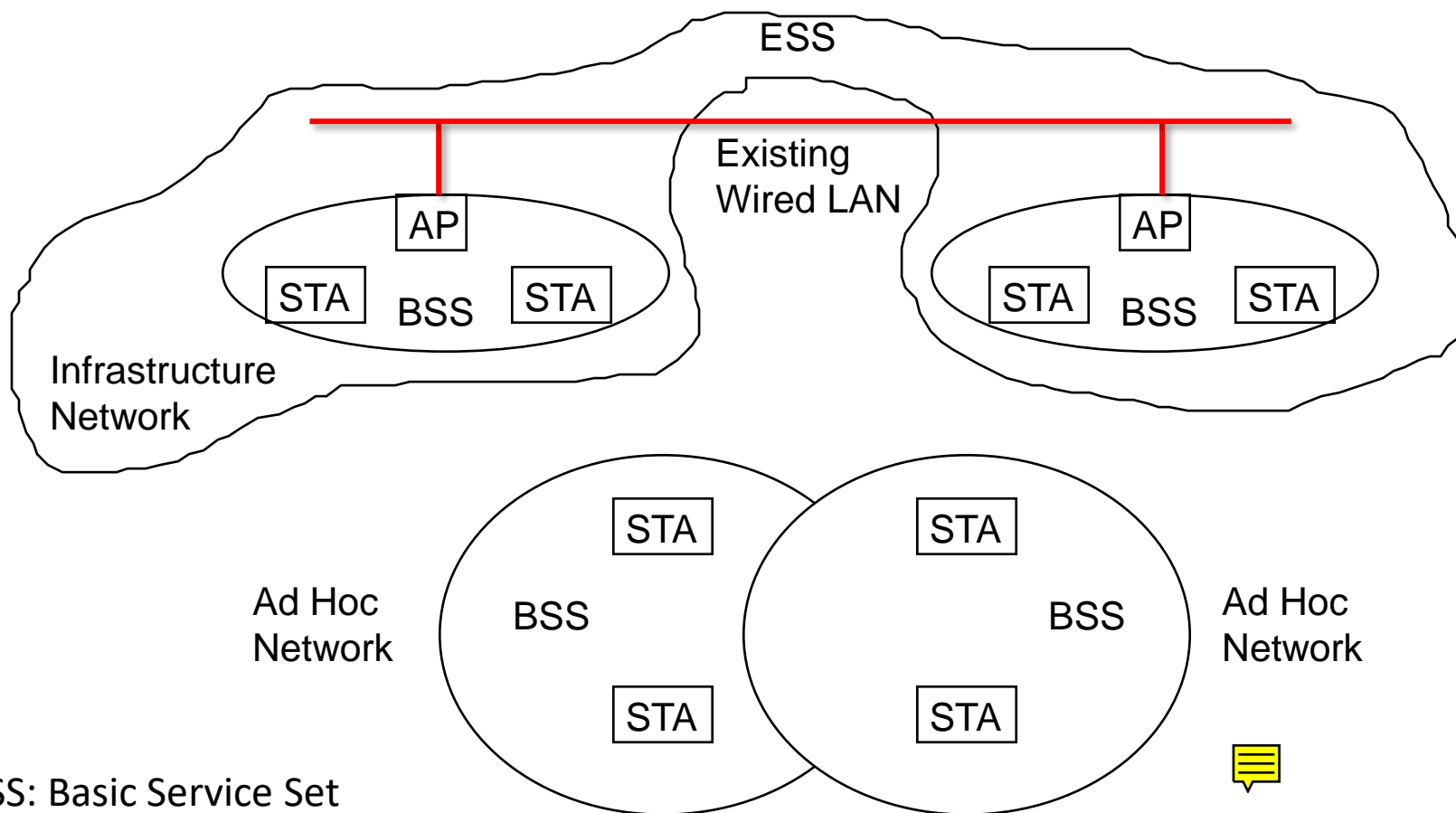
- 802.11ay – Support for 20 Gbps in 60 GHz band.
- 802.11az – 2<sup>nd</sup> generation positioning features.
- 802.11ba – Wake up radio. Low power IoT applications.
- 802.11bb – Light Communications
- 802.11bc – Enhanced Broadcast Service
- 802.11bd – Enhancements for Next Generation V2X
- 802.11be – 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



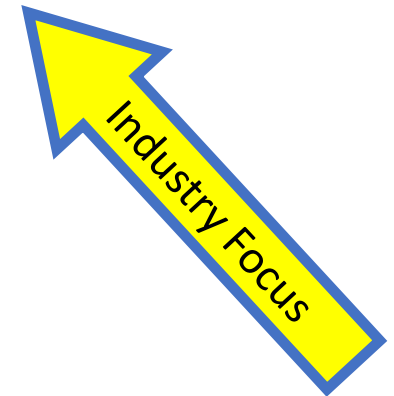
# Distribution System (DS)

- 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!





# 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?




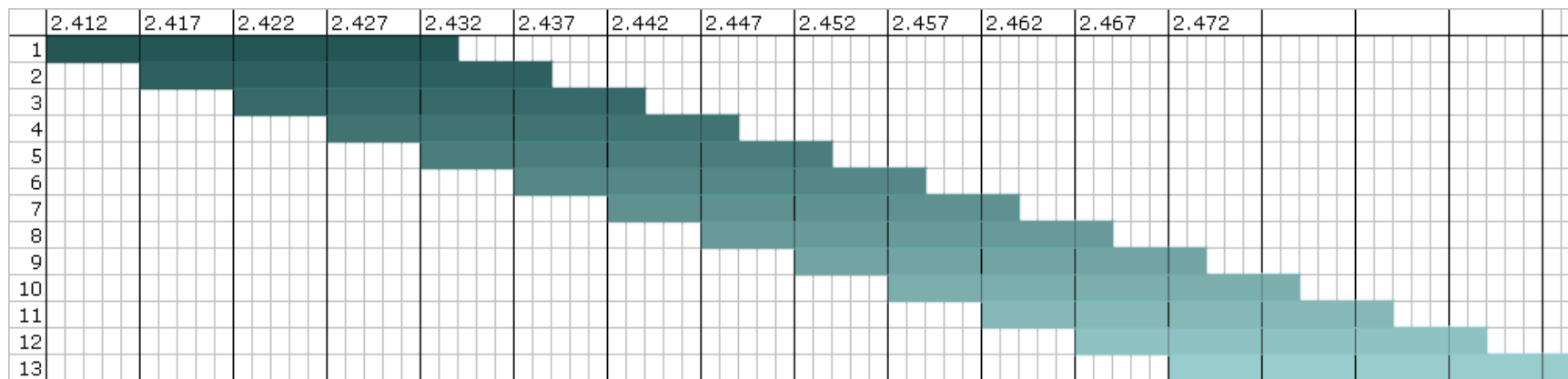
# Outline

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



# 802.11 Channels (2.4GHz)

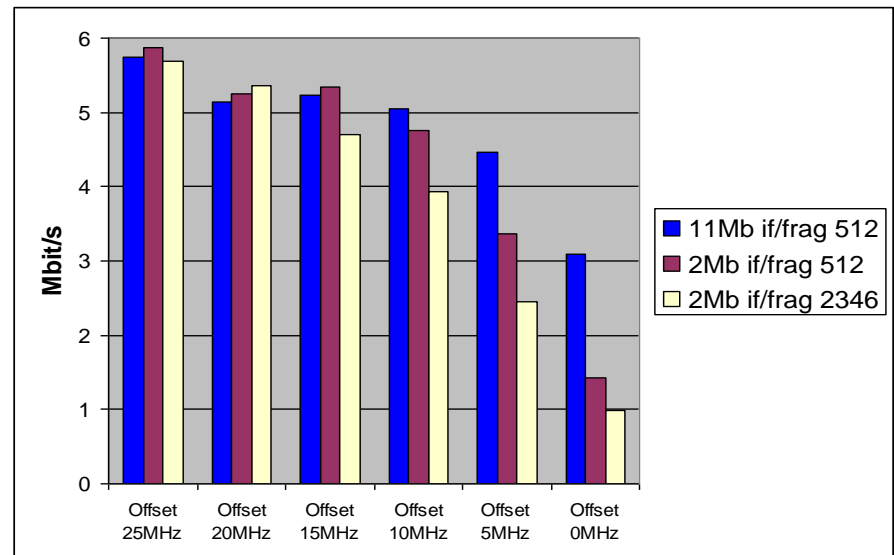
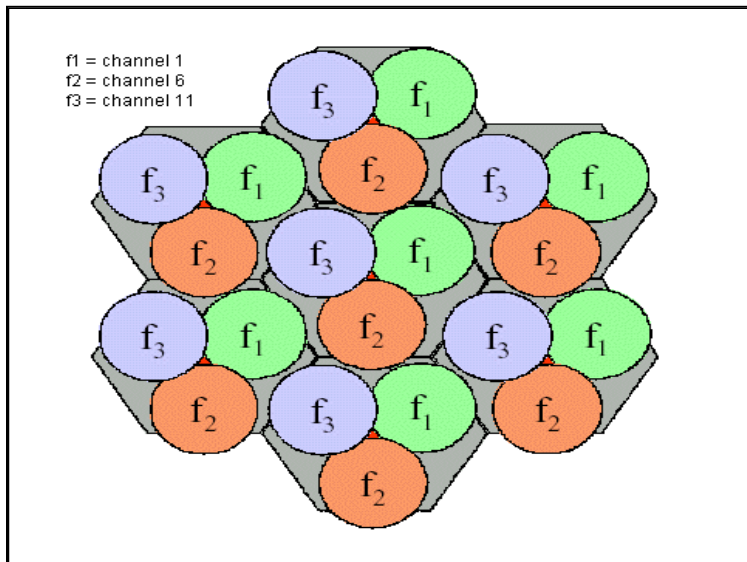
- The frequency is divided in channels
- In the UK and most of EU: 13 channels, 5MHz apart, 2.412 – 2.472 GHz
- In the US: only 11 channels
- Each channel is 22 MHz
- Significant overlap 
- Best channels are 1, 6 and 11





# 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





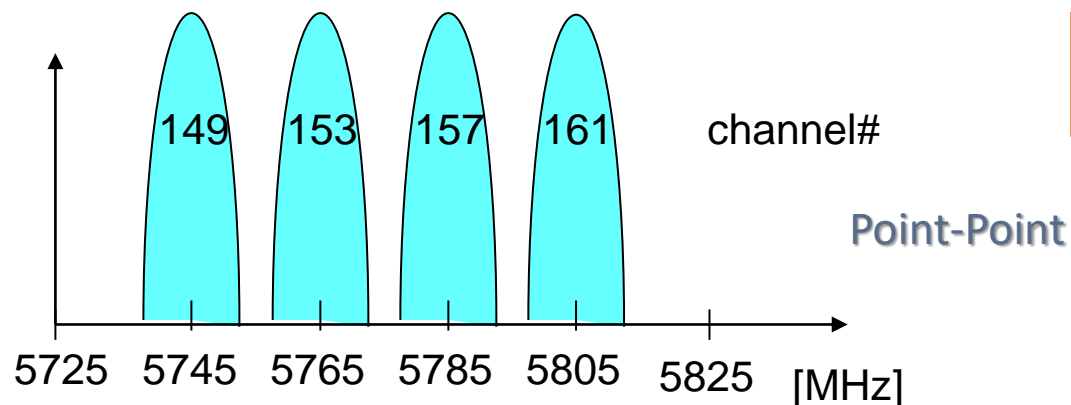
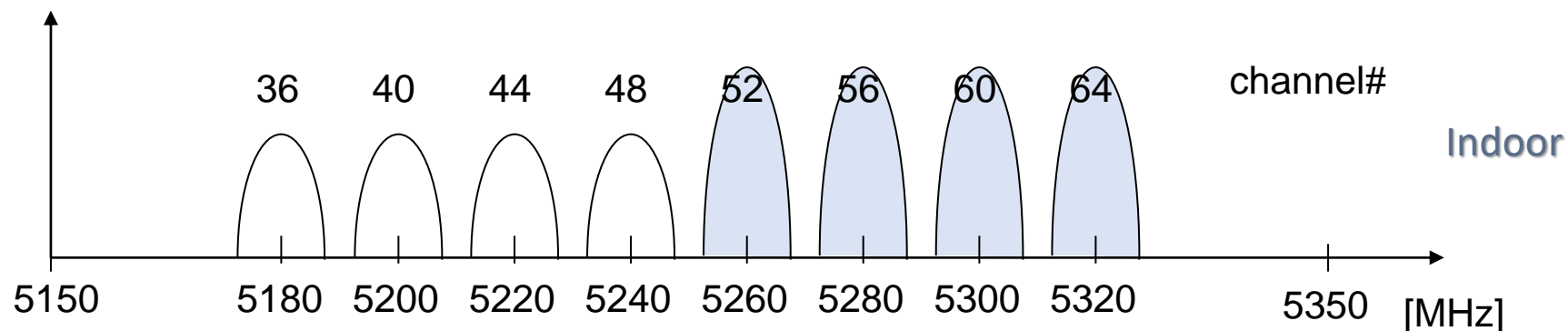


## 802.11 (5GHz)

- 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

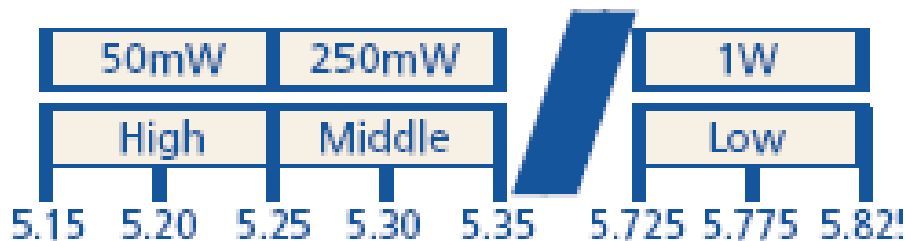


center frequency =  
 $5000 + 5 \times \text{channel number [MHz]}$

Maximum Power Output

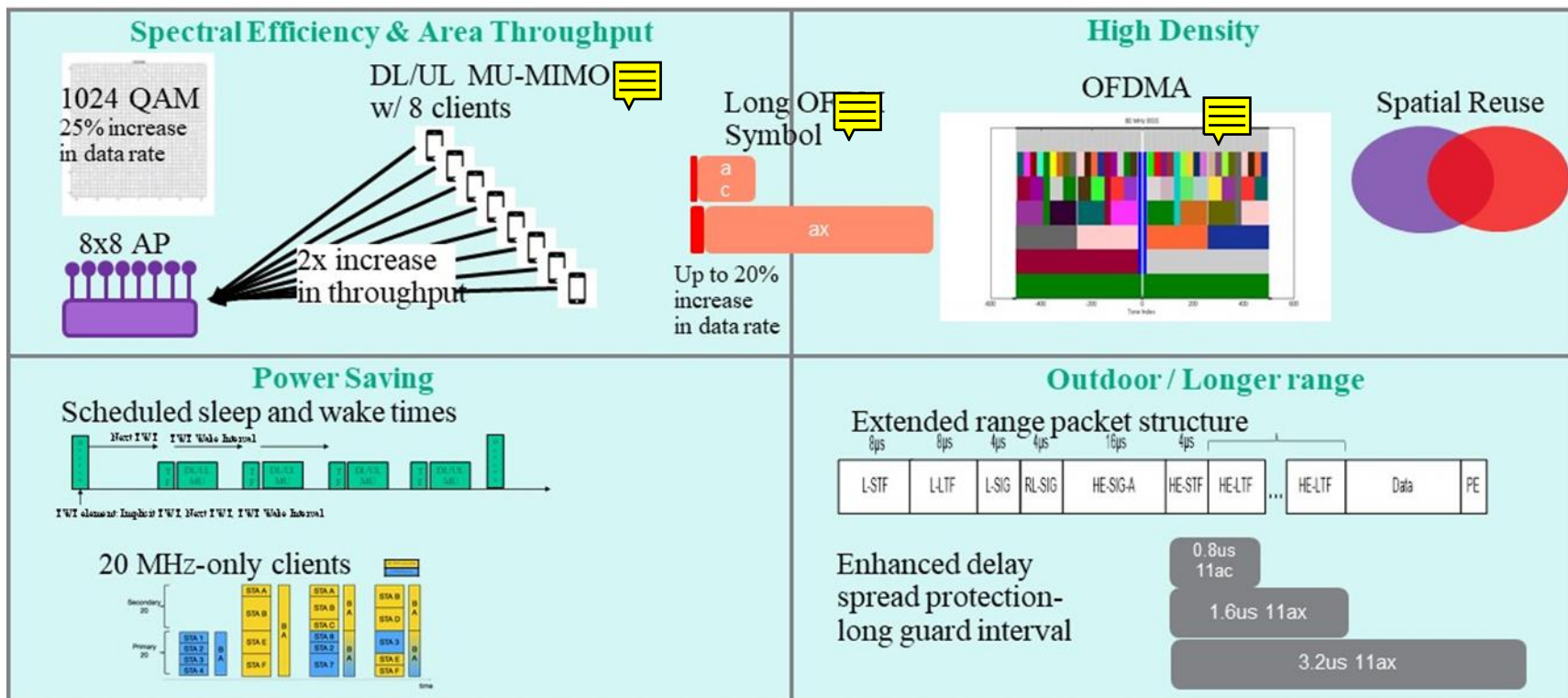
U-NII Band

Frequency (GHz)





# WiFi 6 radio layer enhancements



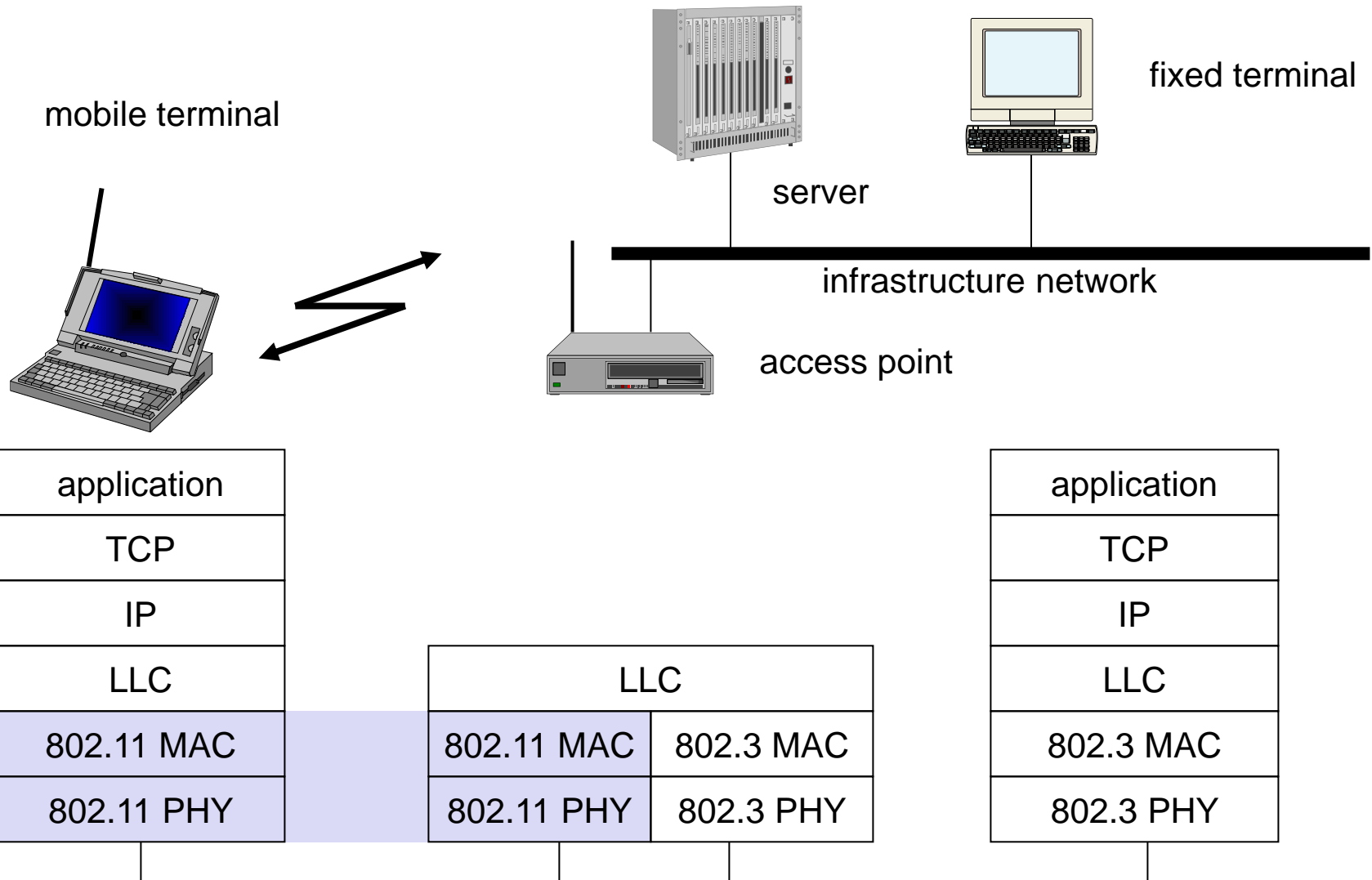


# Outline

- 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

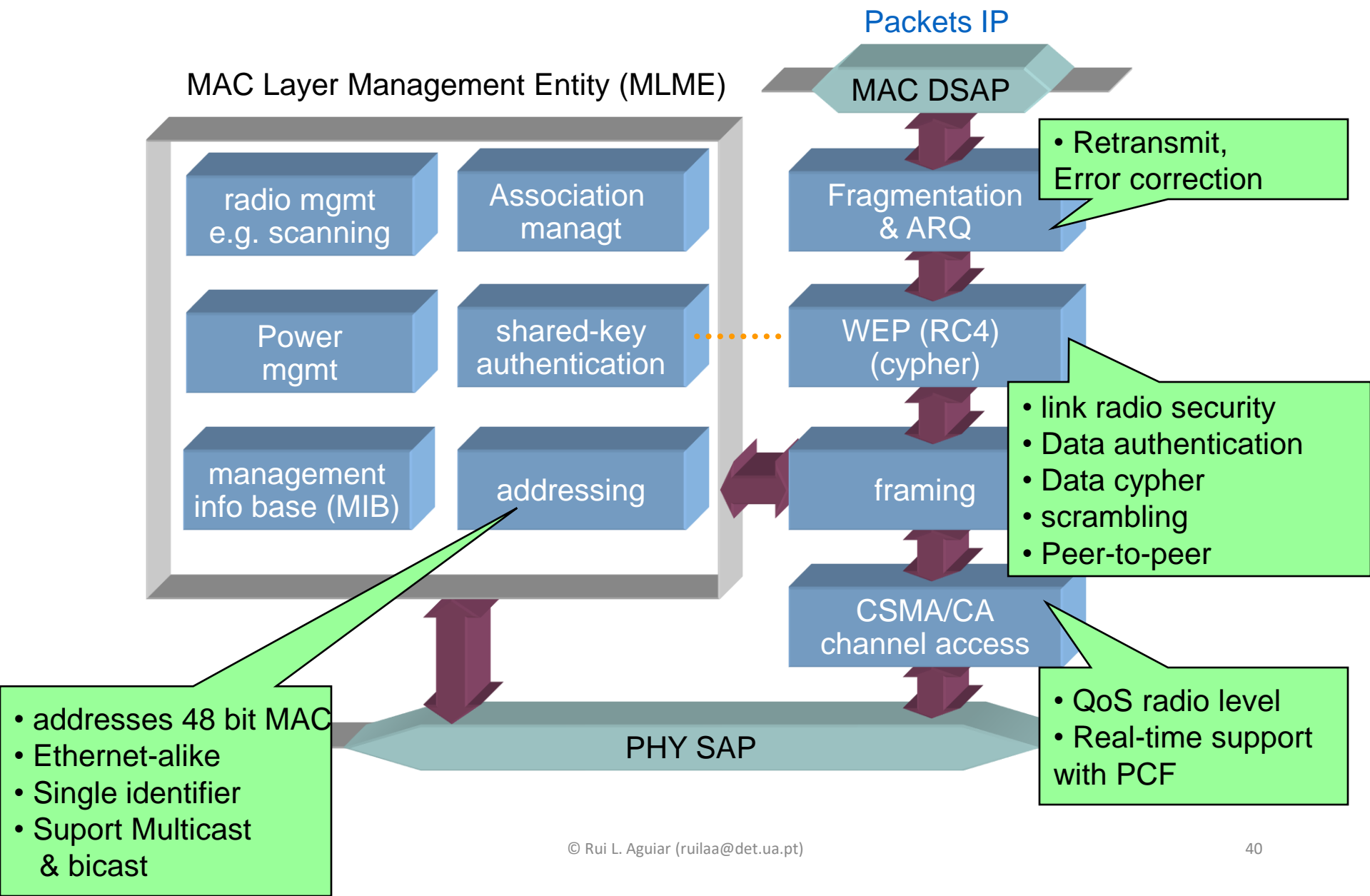


# Features of 802.11 MAC protocol

- 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)



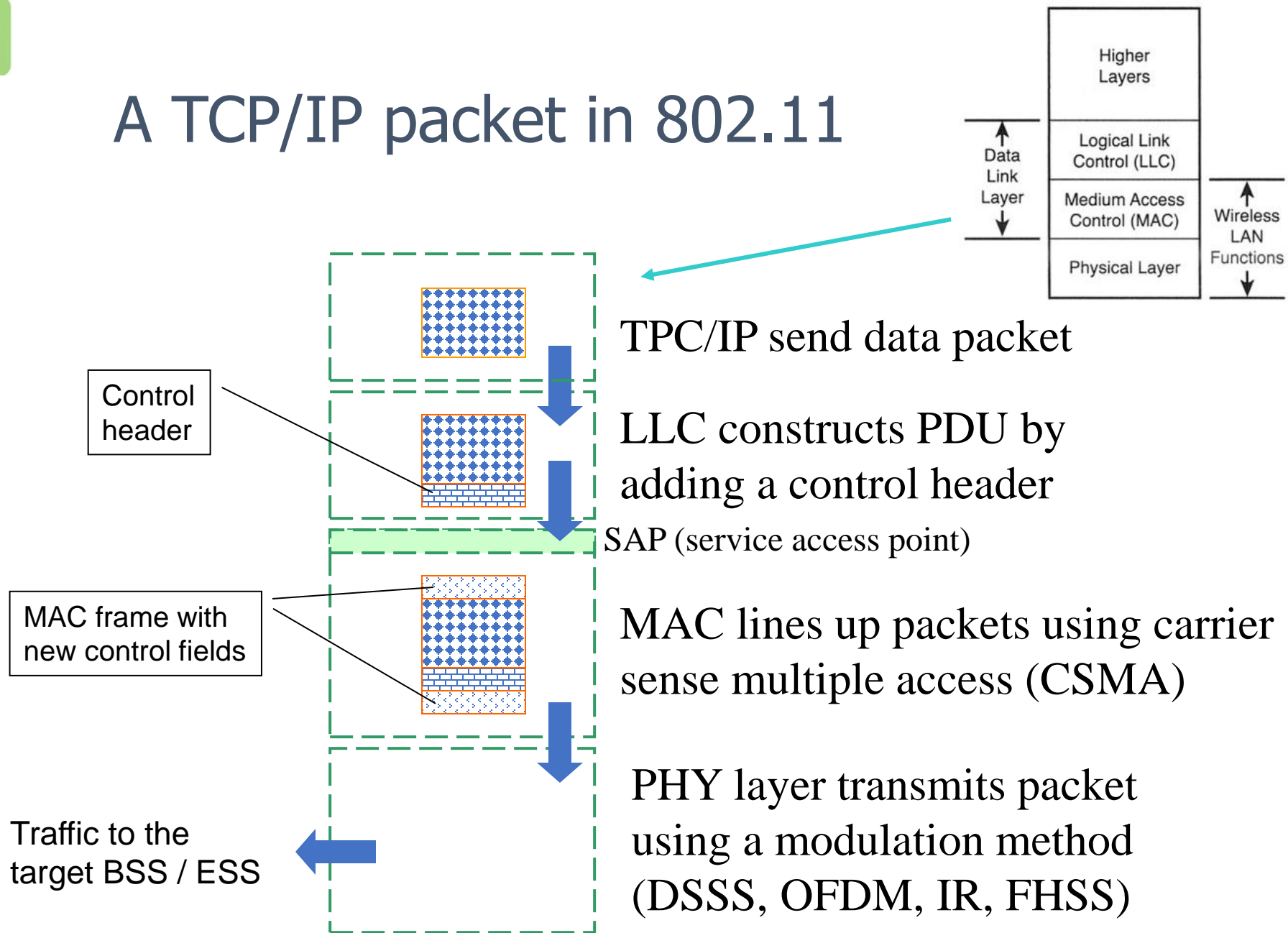
# MAC IEEE802.11







# A TCP/IP packet in 802.11

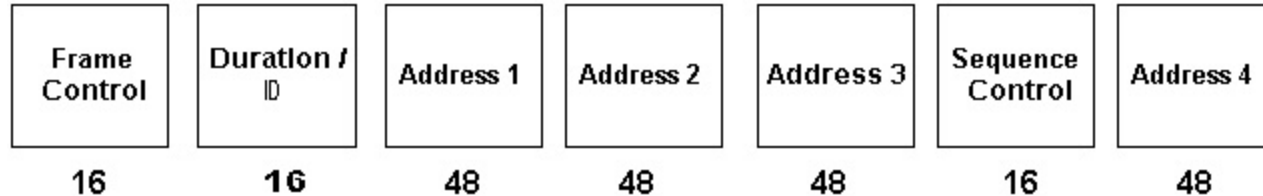


*\*BDU: protocol data unit*

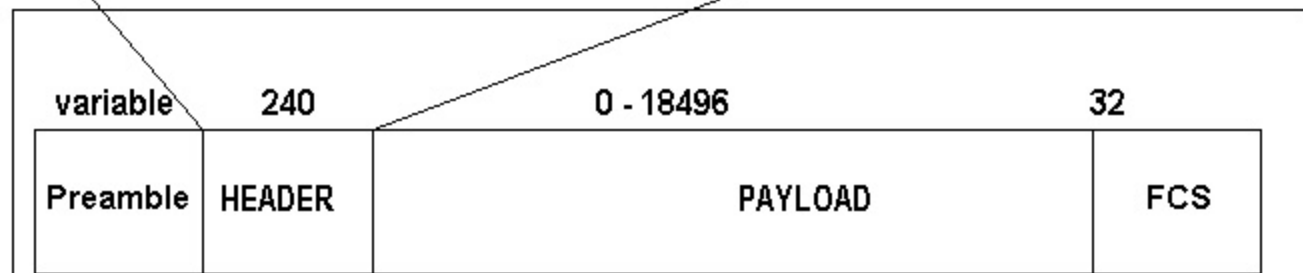


# 802.11 Frames

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

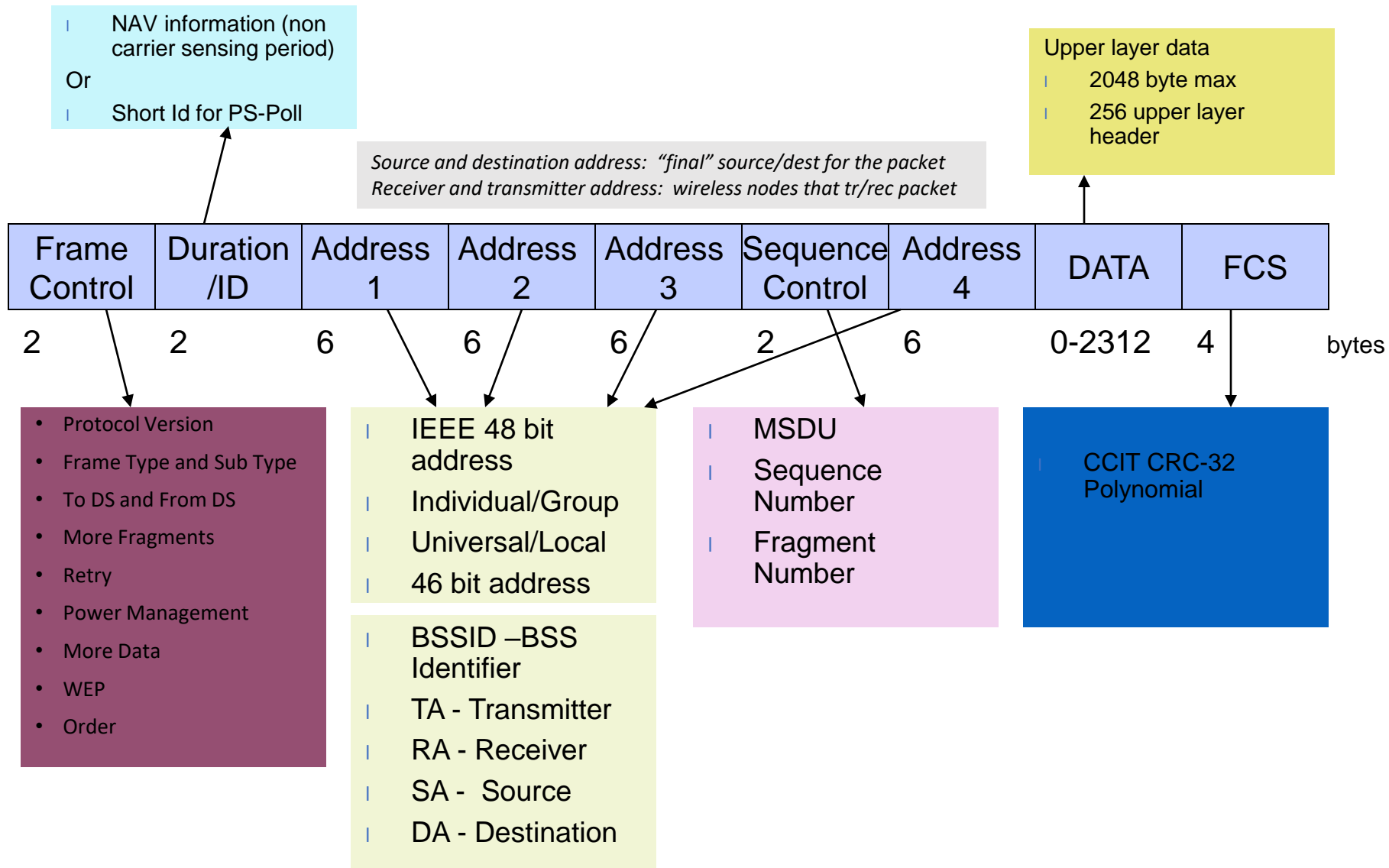


The 240 bit header may be truncated, based on specific frame type





# 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

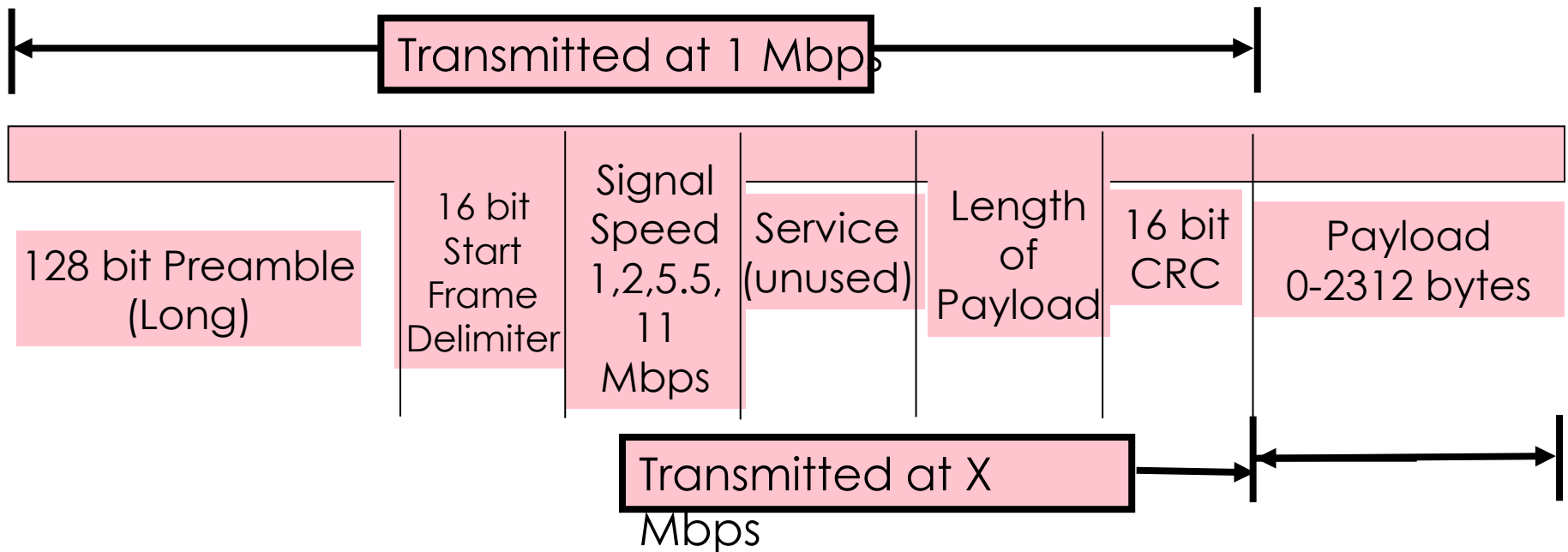
- 802.11 allows for multiple bit rates
  - Allows for adaptation to channel conditions
  - Specific rates dependent on the version
- Algorithm for selecting the rate is not defined by the standard – left to vendors
- Packets have multi-rate format
  - Different parts of the packet are sent at different 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



# 802.11b: Long Preamble

Long Preamble = 144 bits

- Interoperable with older 802.11 devices
- Entire Preamble and 48 bit PLCP Header sent at *1 Mbps*

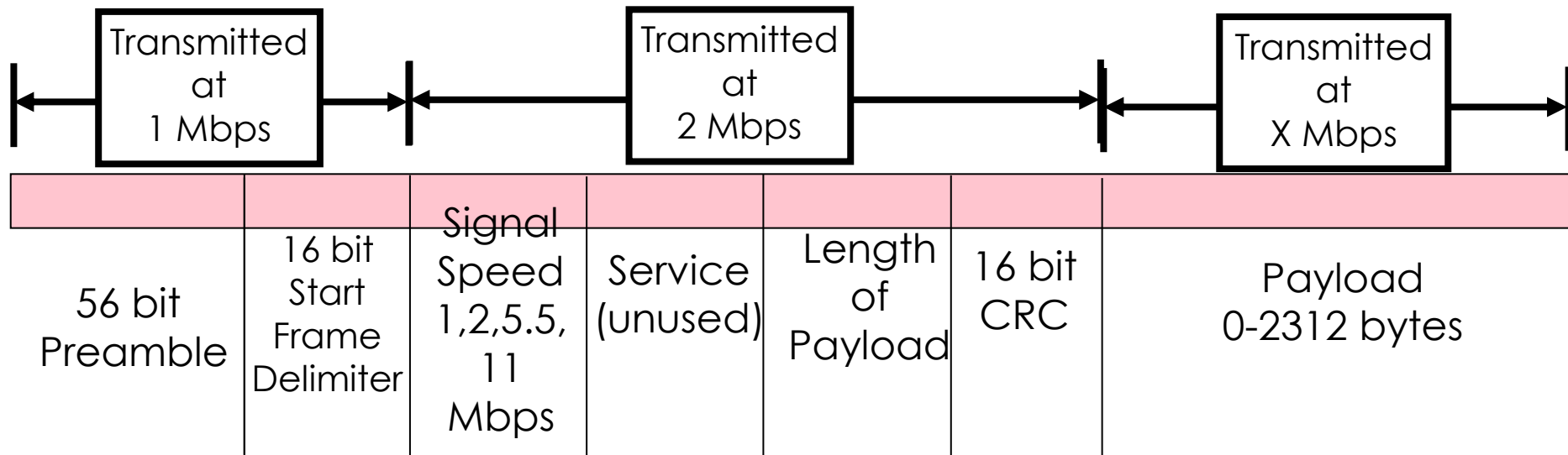




# 802.11b: Short Preamble

Short Preamble = 72 bits

- Preamble transmitted at 1 Mbps
- PLCP Header transmitted at 2 Mbps
- more efficient than long preamble







# 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

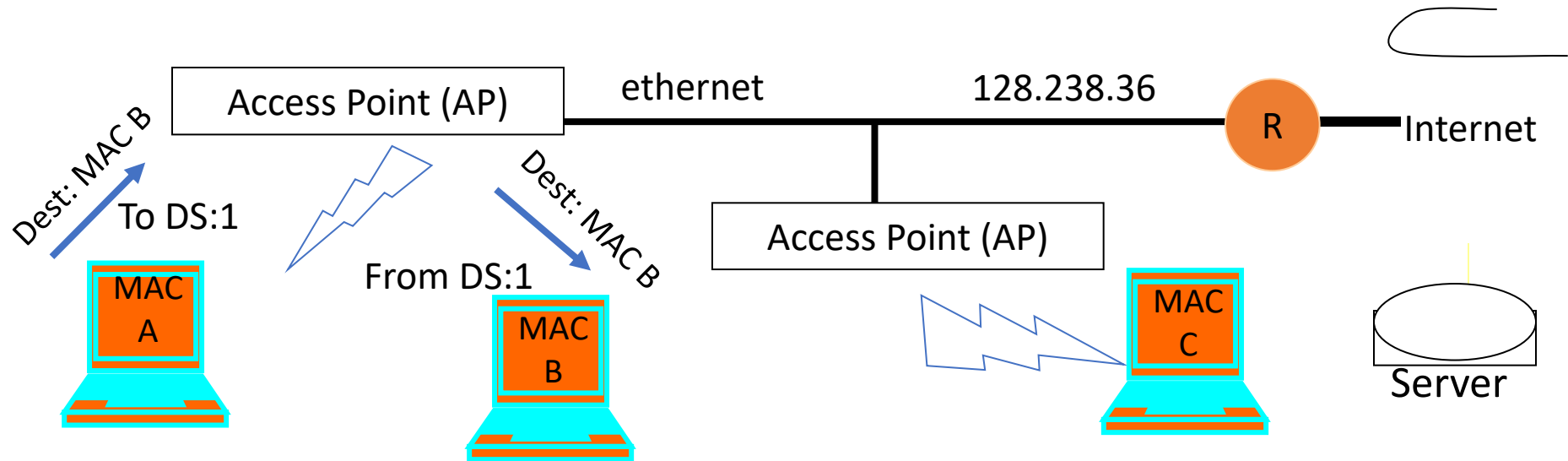


# Data Flow Examples

- 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



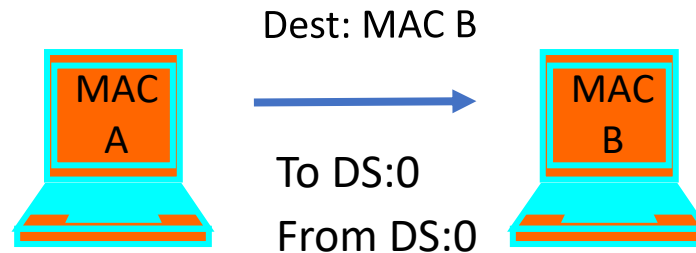
# Case 1: Communication Inside BSS



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



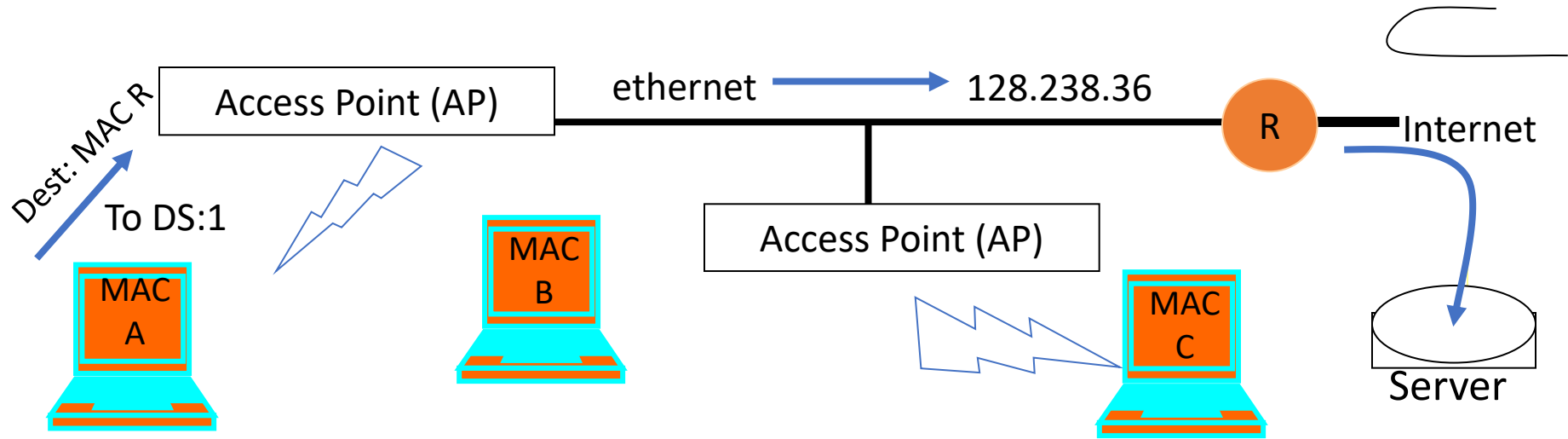
## Case 2: Ad Hoc



- 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



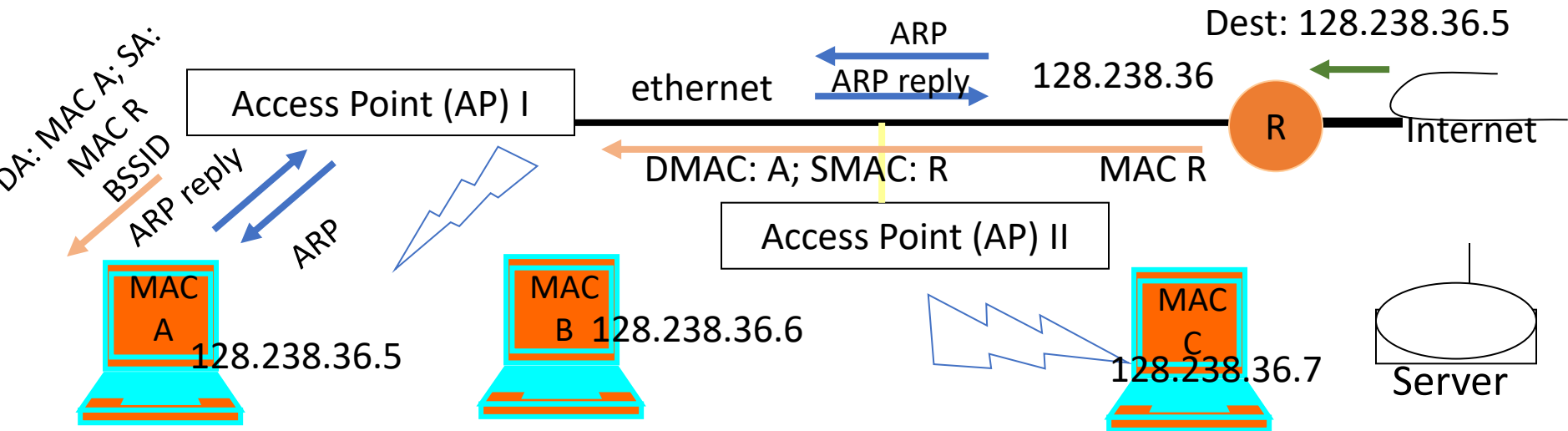
## Case 3: To the Internet



- 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



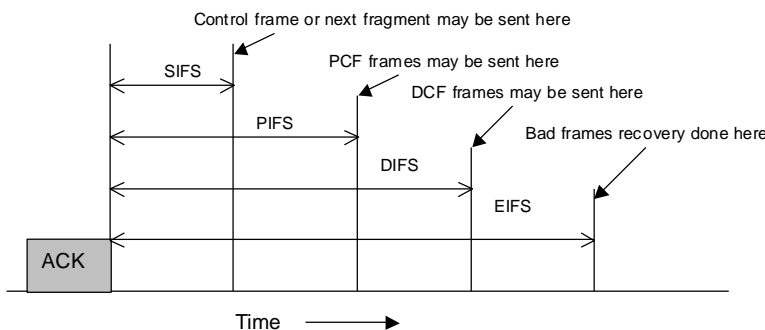
# Outline

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



# MAC Layer

- Asynchronous Data Service (DCF)
  - CSMA/CA
  - RTS/CTS
- Timing-controlled service (PCF)
  - Polling
- Inter-frame spacing (IFS)
  - DIFS (distributed), for the node to start transmitting
  - PIFS (point), used by PCF for network access
  - SIFS (short), between packets of the same flow



**DCF: Distribution Coordination Function**

**PCF: Point Coordination Function**

**DIFS: DCF Inter Frame Spacing**

**PIFS: PCF Inter Frame Spacing**

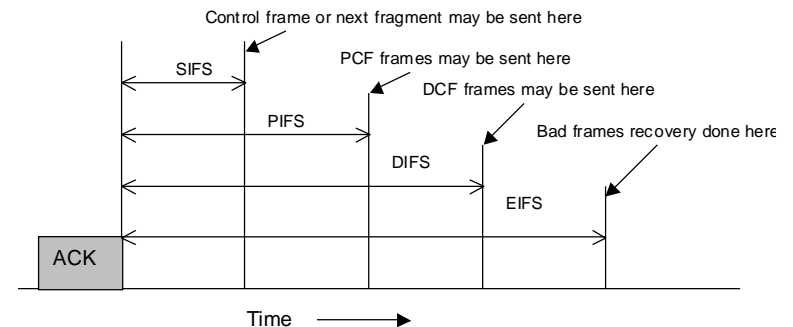
**SIFS: Short Interframe Spacing**





# Carrier Sense Multiple Access

- Before transmitting a packet, sense carrier
- If it is idle, send
  - After waiting for one DCF inter frame spacing (DIFS)
- If it is busy, then
  - Wait for medium to be idle for a DIFS (DCF IFS) period
  - Go through exponential backoff, then send
    - Want to avoid that several stations waiting to transmit automatically collide
- Wait for ACK
  - If there is one, you are done
  - If there isn't one, assume there was a collision, retransmit using exponential backoff



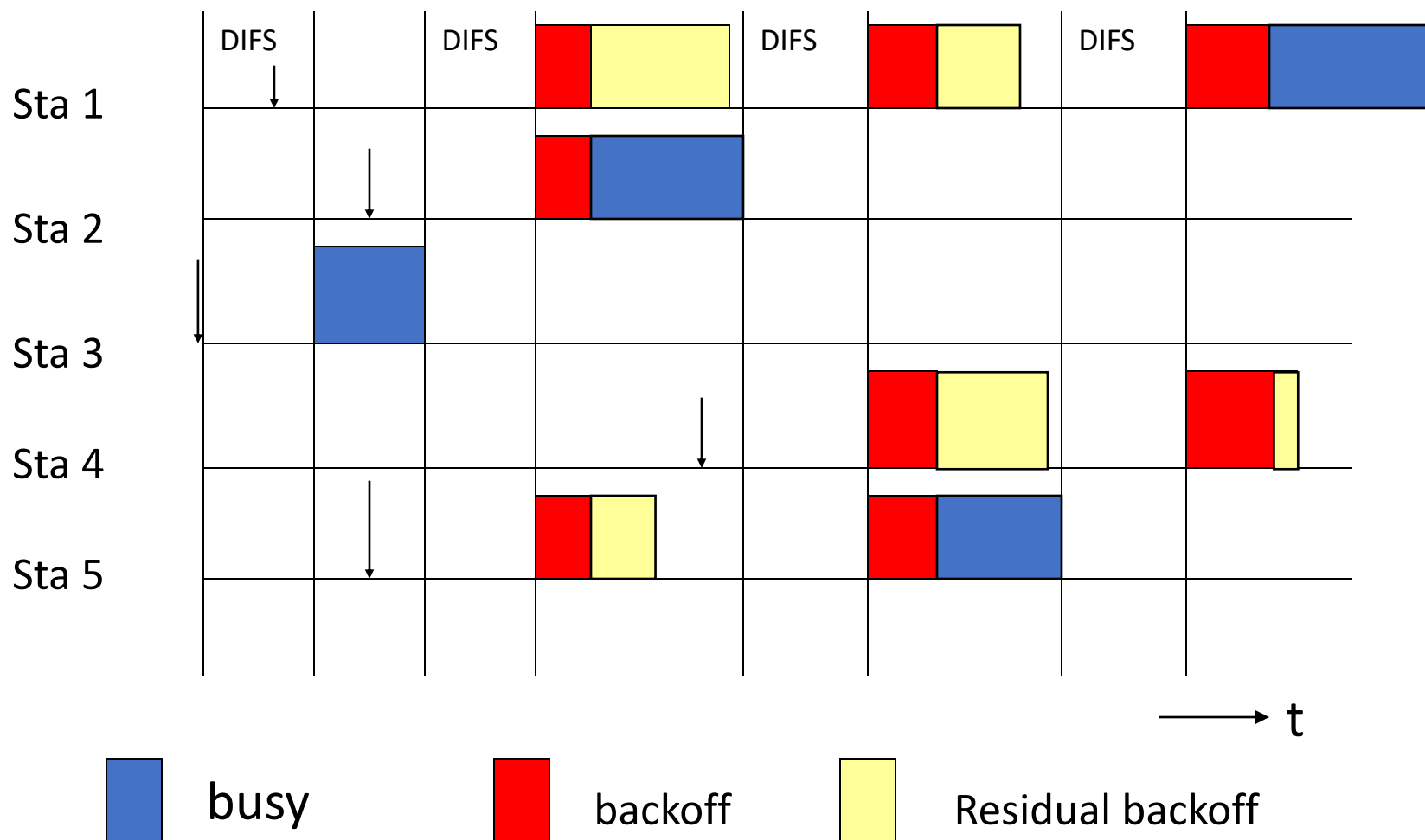


# Exponential Backoff

- Force stations to wait for random amount of time to reduce the chance of collision
  - Backoff period increases exponential after each collision
  - Similar to Ethernet
- If the medium is sensed busy:
  - Wait for medium to be idle for a DIFS (DCF IFS) period
  - Pick random number in contention window (CW) = backoff counter
  - Decrement backoff timer until it reaches 0
    - But freeze counter whenever medium becomes busy
  - When counter reaches 0, transmit frame
  - If two stations have their timers reach 0; collision will occur;
- After every failed retransmission attempt:
  - increase the contention window exponentially
  - $2^i - 1$  starting with  $CW_{\min}$  up to  $CW_{\max}$  e.g., 7, 15, 31, ...



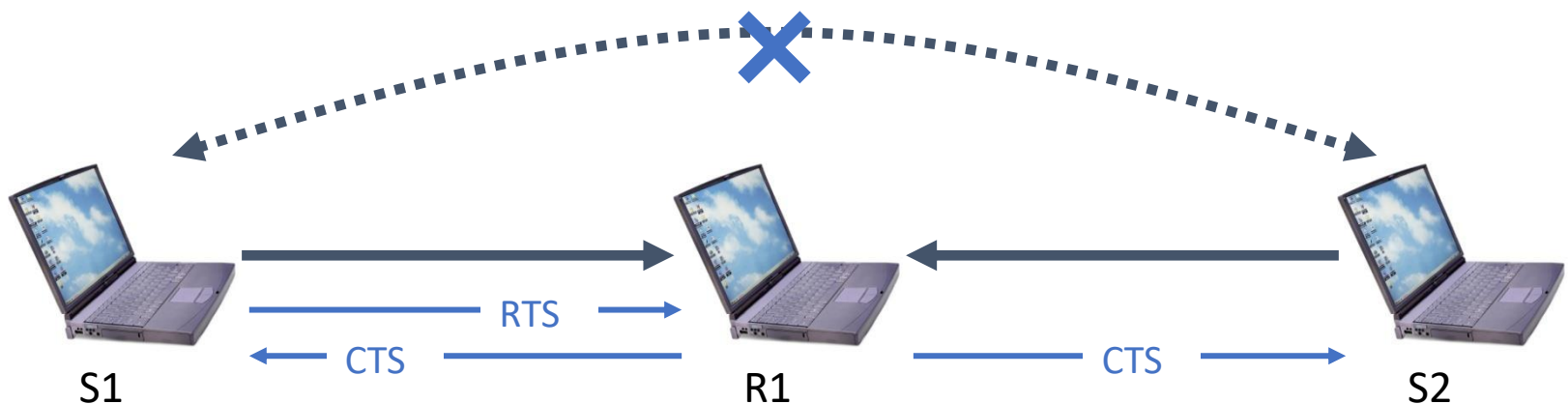
# CSMA/CA





# Collision Avoidance

- Difficult to detect collisions in a radio environment
  - While transmitting, a station cannot distinguish incoming weak signals from noise – its own signal is too strong
- Why do collisions happen?
  - Near simultaneous transmissions
    - Period of vulnerability: propagation delay
  - Hidden node situation: two transmitters cannot hear each other and their transmission overlap at a receiver





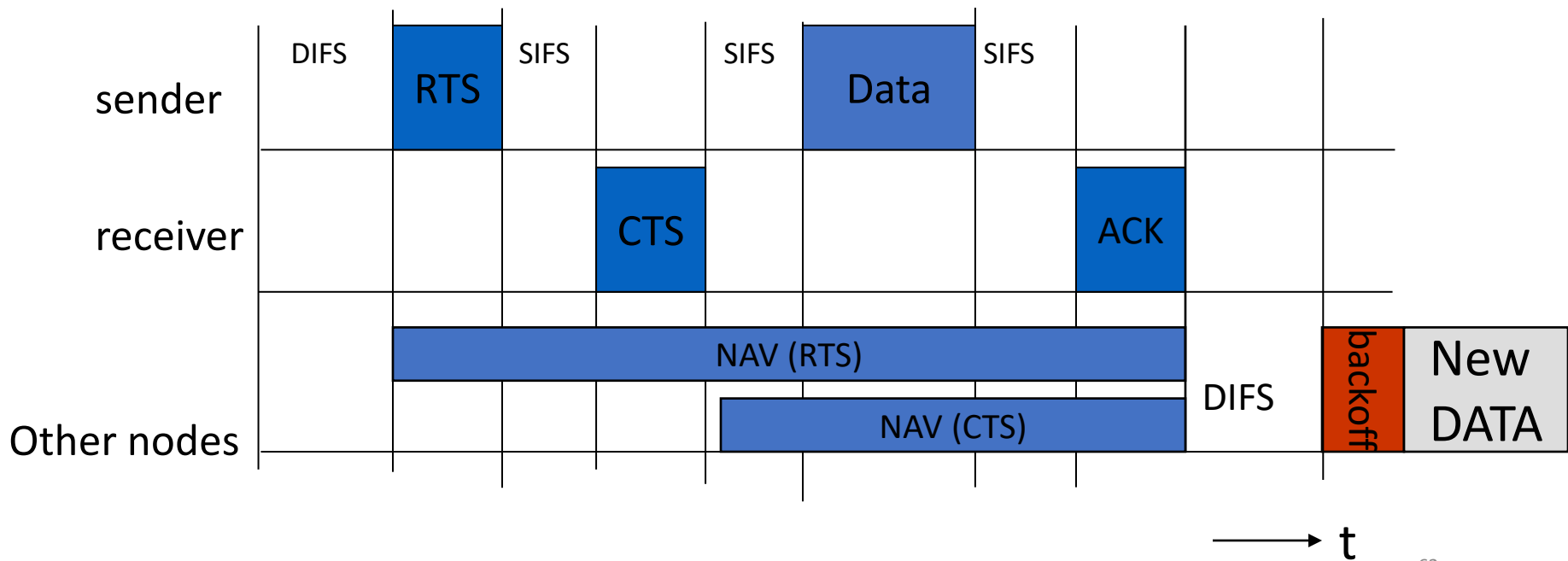
# Request-to-Send and Clear-to-Send

- Before sending a packet, a station first sends a RTS.
- The receiving station responds with a CTS.
  - RTS and CTS are smaller than data packets
  - RTS and CTS use shorter IFS to guarantee access
- Stations that hear either the RTS or the CTS “remember” that the medium will be busy for the duration of the transmission
  - Based on a Duration ID in the RTS and CTS
- Virtual Carrier Sensing: stations maintain Network Allocation Vector (NAV)
  - Time that must elapse before a station can sample channel for idle status



# RTS/CTS: NAV

- NAV: Network Allocation Vector
- NAV acts as a distributed (in each node) resource allocation register
- RTS/CTS
  - Not a “major” concer





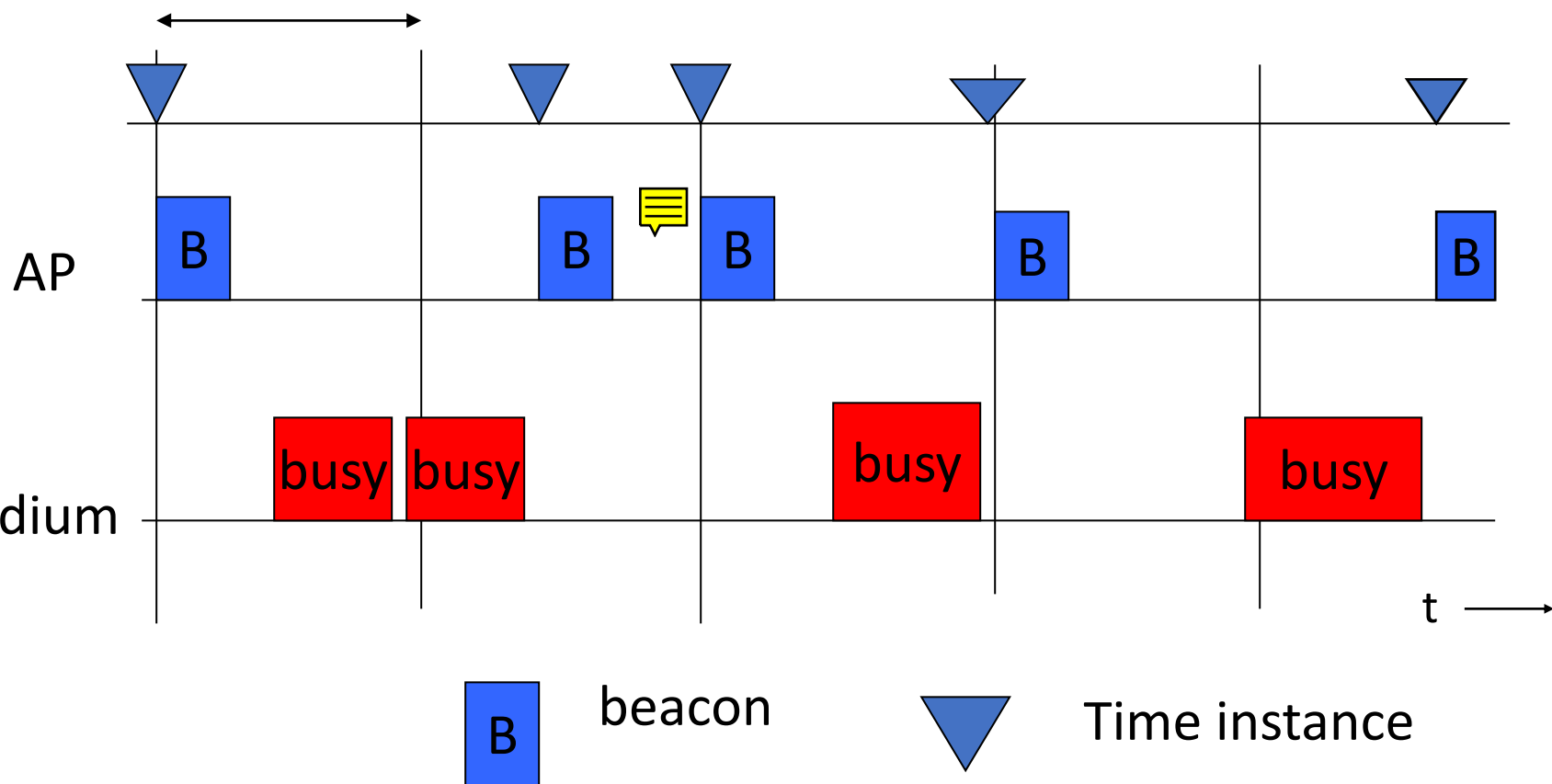
# Synchronization

- Timing synchronization function (TSF)
  - Beacons of the AP are sent in well-defined instants.
  - Content of packet is the exact instant when it goes to the network.
- Used also for power management
  - All clocks of all stations in the BSS are synchronized
    - This allows STA to wake-up to check if packets exist.



# Synchronization

Delay between beacons







# Outline

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



# Some More MAC Features

- Use of RTS/CTS is controlled by an RTS threshold
  - RTS/CTS is only used for data packets longer than the RTS threshold
  - Pointless to use RTS/CTS for short data packets – high overhead!
- Number of retries is limited by a Retry Counter
  - Short retry counter: for packets shorter than RTS threshold
  - Long retry counter: for packets longer than RTS threshold
- Packets can be fragmented.
  - Each fragment is acknowledged
  - But all fragments are sent in one sequence
  - Sending shorter frames can reduce impact of bit errors
  - Lifetime timer: maximum time for all fragments of frame



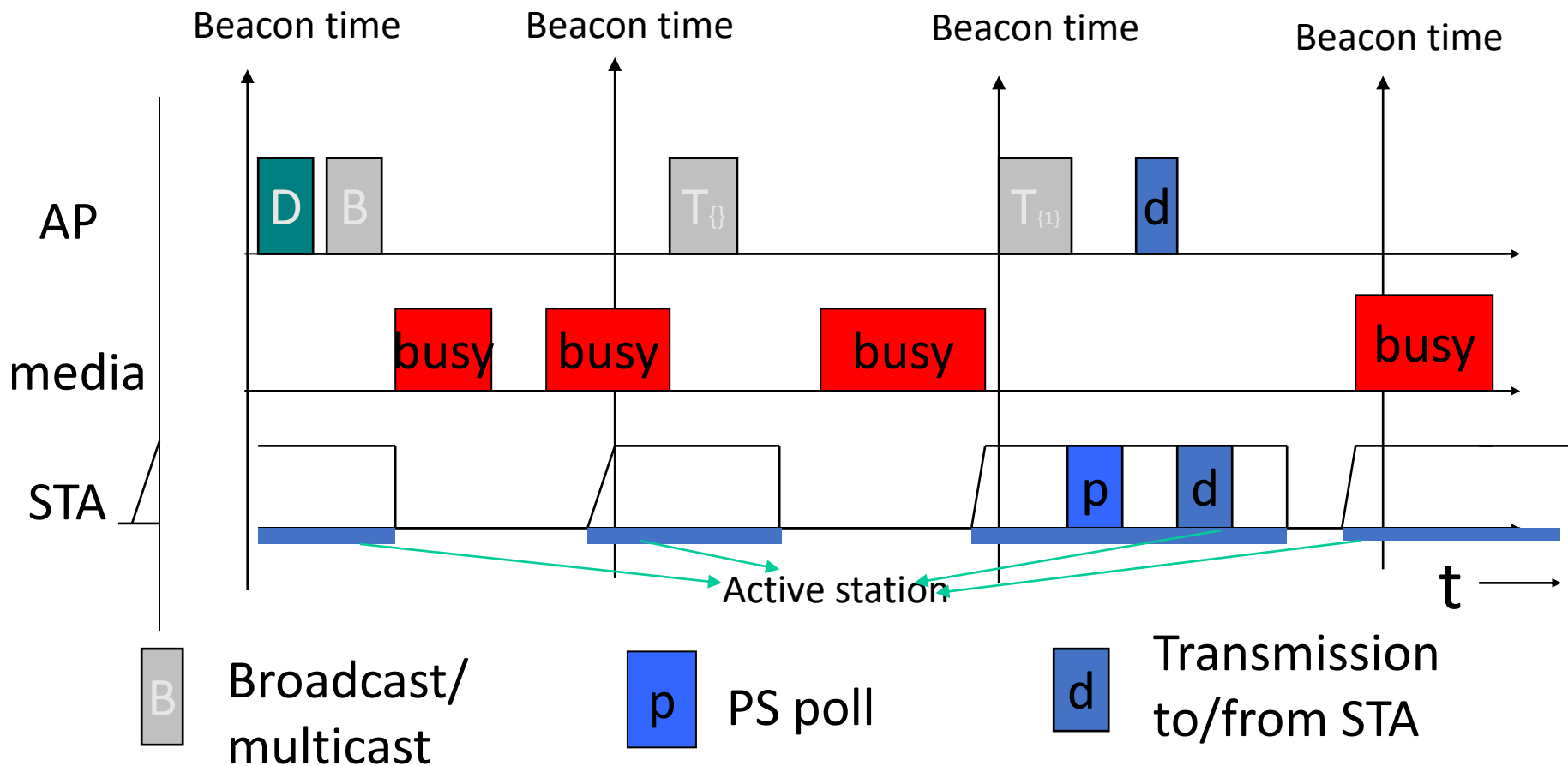


# Power management (infrastructure)

- APs buffer packets to stations in power saving mode
  - APs announce in beacons which packets are waiting with the TIM (traffic indication Map)
  - Broadcast/multicast frames are also buffered at AP
    - Sent after beacons, same common timing period.
    - Uses Delivery Traffic Indication Map (DTIM)
    - AP controls DTIM interval
- STA in power save wake periodically to listen for beacons
  - If it has data pending, send a PS-Poll
  - AP sends buffered data to this PS-poll
- TSF (Timing Synchronization Function) assures AP and stations are synchronized
  - Synchronizes clocks of the nodes in the BSS



# Power management





How does a station connect to an  
Access Point?



# Control services at MAC

- Synchronization, Roaming and Association
  - Functions to find a network
  - Change APs
  - Search APs.
- Power Management
  - sleep mode without losing packets
  - Power management functions
- MIB: Management information base
- Security: authentication and cypher



# SSID

- Mechanism used to segment wireless networks
  - Multiple independent wireless networks can coexist in the same location
- Each AP is programmed with a SSID that corresponds to its network
- Client computer presents correct SSID to access AP
- Security Compromises
  - AP can be configured to “broadcast” its SSID
  - Broadcasting can be disabled to improve security
  - SSID may be shared among users of the wireless segment





# Association Management: Scanning

- Scanning is needed to:
  - Find and connect to a networks
  - Find a new AP during roaming
- Passive Scanning:
  - Station simply listens for Beacon and get info of the BSS. Power is saved.
- Active Scanning:
  - Station transmits Probe Request; elicits Probe Response from AP. Saves time.



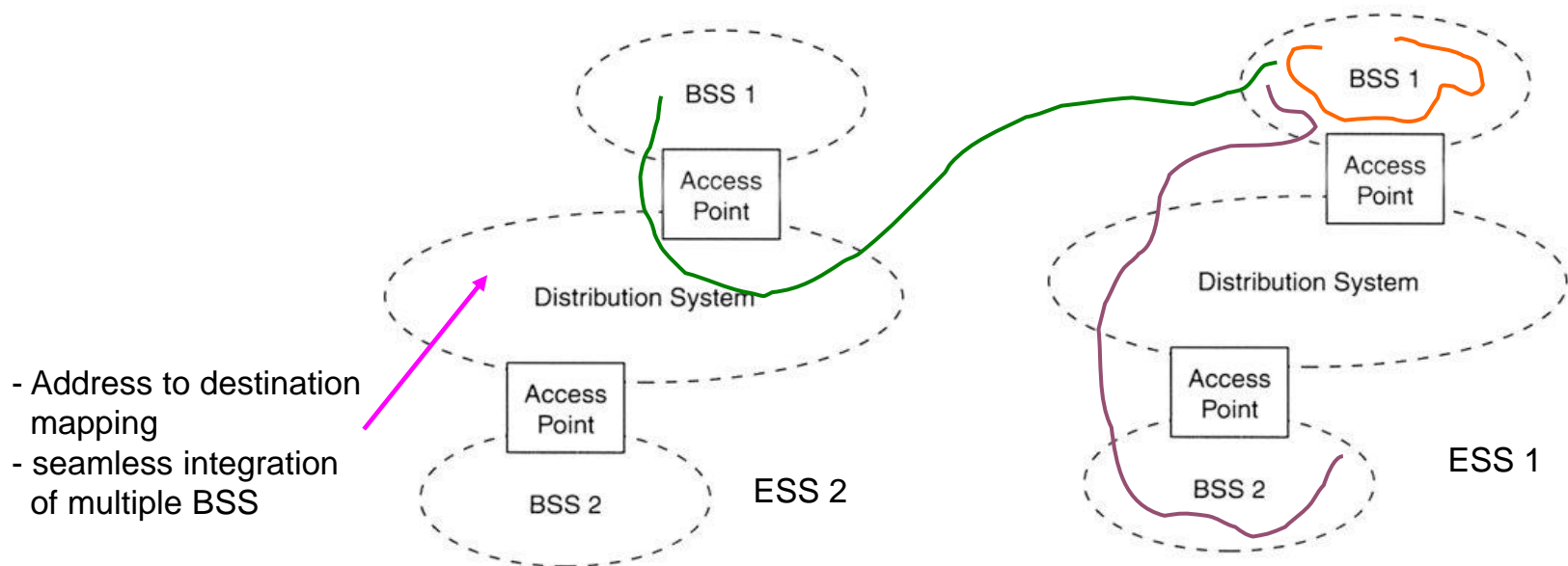
# Association Management: Scanning, and Joining

- Station must associate with an AP before they can use the network
  - AP must know about them so it can forward packets
- Re-association (roaming): association is transferred
  - Supports mobility in the same ESS
- Disassociation: station or AP can terminate association
- Stations can detect AP based on scanning
- Joining a BSS
  - Synchronization in Timestamp Field and frequency (i.e., channel) :
  - Adopt PHY parameters
  - Other parameters: BSSID, WEP, Beacon Period, etc.



# IEEE 802.11 Mobility

- Standard defines the following mobility types:
  - **No-transition:** no movement or moving within a local BSS
  - **BSS-transition:** station moves from one BSS in one ESS to another BSS within the same ESS
  - **ESS-transition:** station moves from a BSS in one ESS to a BSS in a different ESS (continuous roaming not supported)





# Roaming

- Roaming: station changes network (BSS)
- STA may go:
  - Outside the coverage area of their AP
  - But still under the coverage area of another AP
- Reassociate the STA with the new AP allows the communication to continue



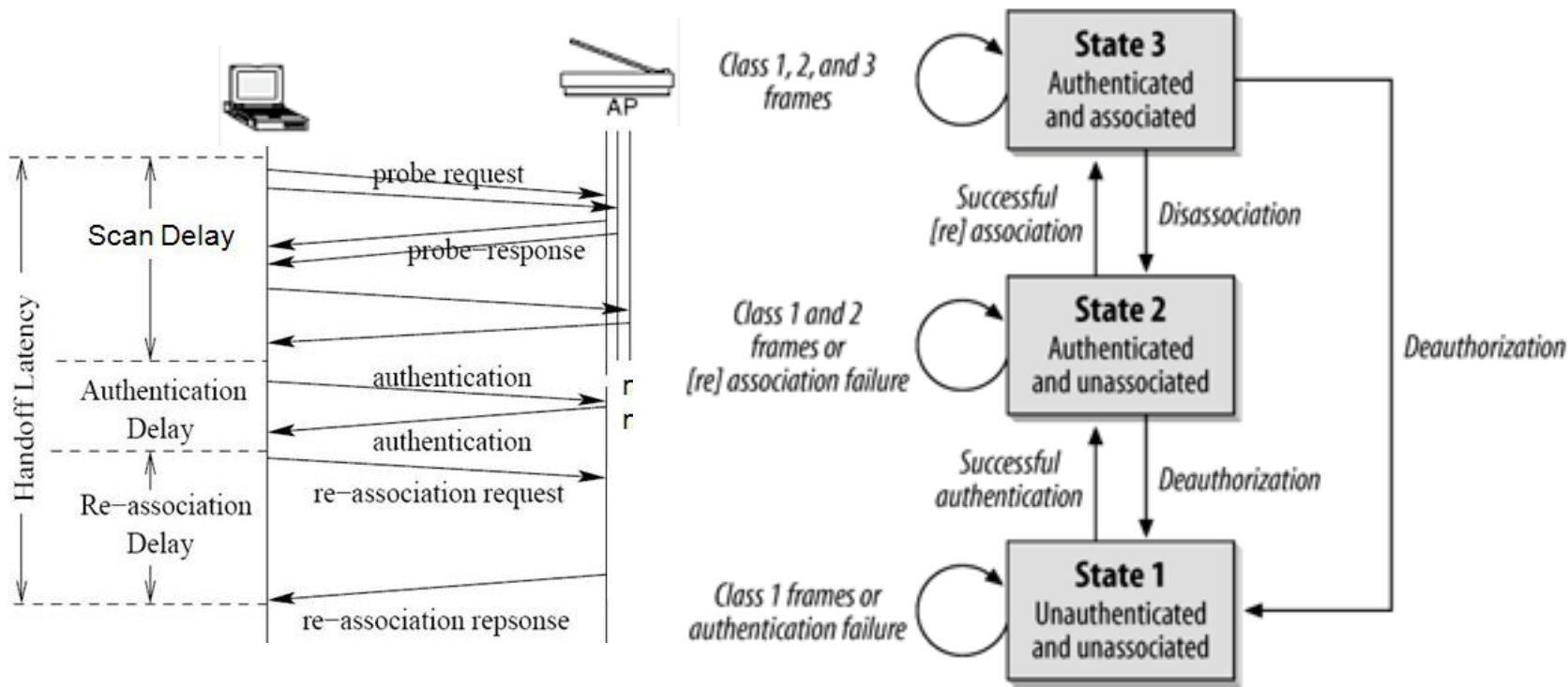
# Roaming

- STA decides that the signal with the current AP is bad.
- STA does scanning (act/pas) to find new AP
- STA reassociates with the New AP (NAP)
  - Includes authorization.
- Without positive answer
  - STA does new scan
- With positive answer:
  - STA changed network to the new NAP
  - AP informs the ESS of the new association
  - Information in the distributed system is always updated.



# Attachment to a BSS

- The STA finds a BSS/AP through **Scanning/Probing**
- Both **Authentication** as well as **Association** are necessary to enter a BSS





# Phase 1: Scanning

- The STA searches for APs
  - **Passive Scanning**
    - STA analyzes channels looking for **Beacon** packets, which are periodically sent by the AP, announcing its presence and SSID
  - **Active Scanning**
    - STA sends **Probe Request** packets to all channels in sequence
    - AP's listening in these different channels respond with a **Probe Response**



## Phase 2: Authentication

- After finding and selecting an AP, the STA has to authenticate with it. Two main methods:
- Method 1: **Open System Authentication**
  - Default procedure, executed in 2 steps:
    - 1 - STA sends an authentication frame including its identity
    - 2 - AP responds with a frame as a Ack/NAck
- Method 2: **Shared Key Authentication**
  - STA and AP have a shared secret, obtained in some other way
  - 1 – STA sends an initial authentication request
  - 2 – AP replies to the STA with a challenge
  - 3 – STA decyphers the challenge with its own key and sends it to the AP
  - 4 – AP uses its own key to decipher the challenge and compares results





## Phase 3: Association

- After authenticated, the STA begins the **association** process, i.e., Exchange roaming and capacity information between STA and AP
- Procedure:
  - 1 – STA sends a **Associate Request** to AP, indicating supported transmission rates and intended association SSID
  - 2 – AP allocates resources and decides if it accepts or rejects the STA
  - 3 – AP sends an **Association Response**, indicating the association identifying and supported transmission rates, in case the association is accepted
  - 4 (optional) – In case of a handover (transition of the STA between two different APs), the new AP informs the old AP
- Only after associating to the AP, can the STA start to send and receive data



# MESH (TODO)



# How to extend range in Wi-Fi?



# Wi-Fi “extenders”.

- Inexpensive
- They set up a new SSID, and forward all traffic to the original SSID
- Multi-hop configurations are possible
  - Require manual configuration
- Because the original access point and the extender have different SSIDs
  - Many devices will not automatically connect to whichever is closer
  - They prefer to maintain connection with the original SSID until that signal disappears
  - This is, for many mobile users, reason enough to give up on this strategy.



# Mesh

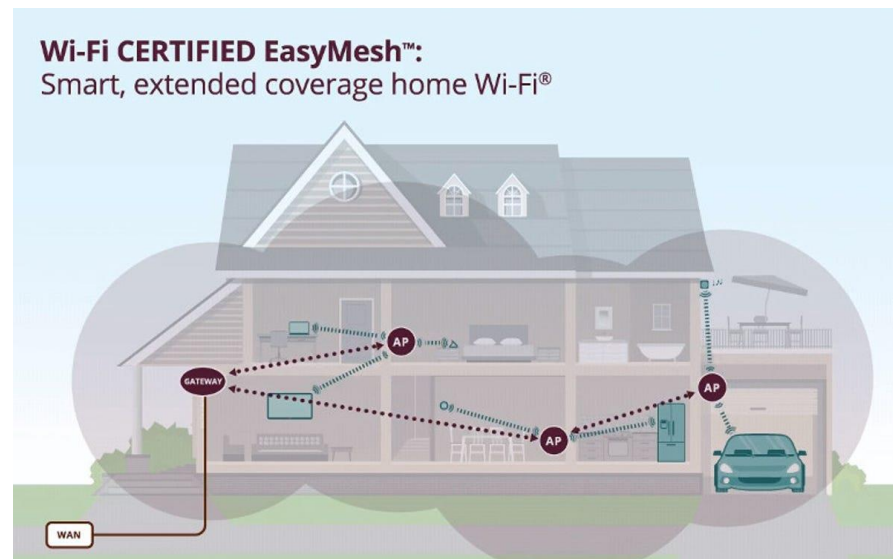
- Different standards
  - IEEE 802.11s standard
    - Focuses on the setup of the mesh networks
    - Uses a mandatory routing protocol – Hybrid Wireless Mesh Protocol
    - Mesh Stations can collocate 802.11 AP's and provide access to the mesh network for 802.11 devices
    - A Mesh Gateway interconnects the mesh to other non-802 networks
  - Wi-Fi Alliance standard (a.k.a., "EasyMesh")
    - Focuses on more "easy" setup of mesh WiFi networks
      - incorporates parts of the [IEEE 1905.1](http://intronetworks.cs.luc.edu/current2/mobile/wireless.htm) standard for home networks, which simplifies initial configuration.
    - Specifies that one access point – the one connected to the Internet – will be a "Multi-AP" Controller
    - the other access points are called Agents.
    - The EasyMesh standard also

<http://intronetworks.cs.luc.edu/current2/mobile/wireless.htm>



# Wi-Fi EasyMesh

- WiFi Alliance Certification program that defines multiple access point home and small office Wi-Fi networks that are easy to install and use, self-adapting, and add multi-vendor interoperability.
- This technology brings both consumers and service providers additional flexibility in choosing Wi-Fi EasyMesh devices for home deployment.
- Wi-Fi EasyMesh uses a controller to manage the network, which consists of the controller, plus additional APs, called agents.
- Establishing controllers to manage and coordinate activity among the agents ensures that each AP does not interfere with the other, bringing both expanded, uniform coverage and more efficient service.





EasyMesh specification relies on other standards / specification, either by extending them or simply referencing them.

This includes, most notably:

- Building on and extending IEEE Standard 1905.1 to configure Wi-Fi access point interfaces
  - **Discovery:** how nodes are finding each other and identifying the controller
  - **Push-Button Configuration:** to initialize "onboarding" of access points-the process commonly referred to as "meshing"
  - **Backhaul communication:** Communication between the nodes / access points in the mesh network

[IEEE 1905.1 standard, Convergent Digital Home Network for Heterogeneous Technologies.](#)



## IEEE 1905.1 standard, Convergent Digital Home Network for Heterogeneous Technologies.

- This technology enables networked devices connected by different network media--say Gigabit Ethernet 2.4Ghz, and 5Ghz Wi-Fi, to operate as if they were connected across a single network. In EasyMesh, the controllers use data from it to configure each agent's AP radios. It also includes mechanisms to configure control-related policies on agents, such as metrics and steering. Additionally, the controller determines the topology of the network of agents, so it can adapt to changing network conditions.
- also utilize mechanisms from the new Wi-Fi Alliance [Agile Multiband](#) standard. New Agile Multiband certified devices will work better as they're moved from spot to spot with intelligent steering and faster network transitions.



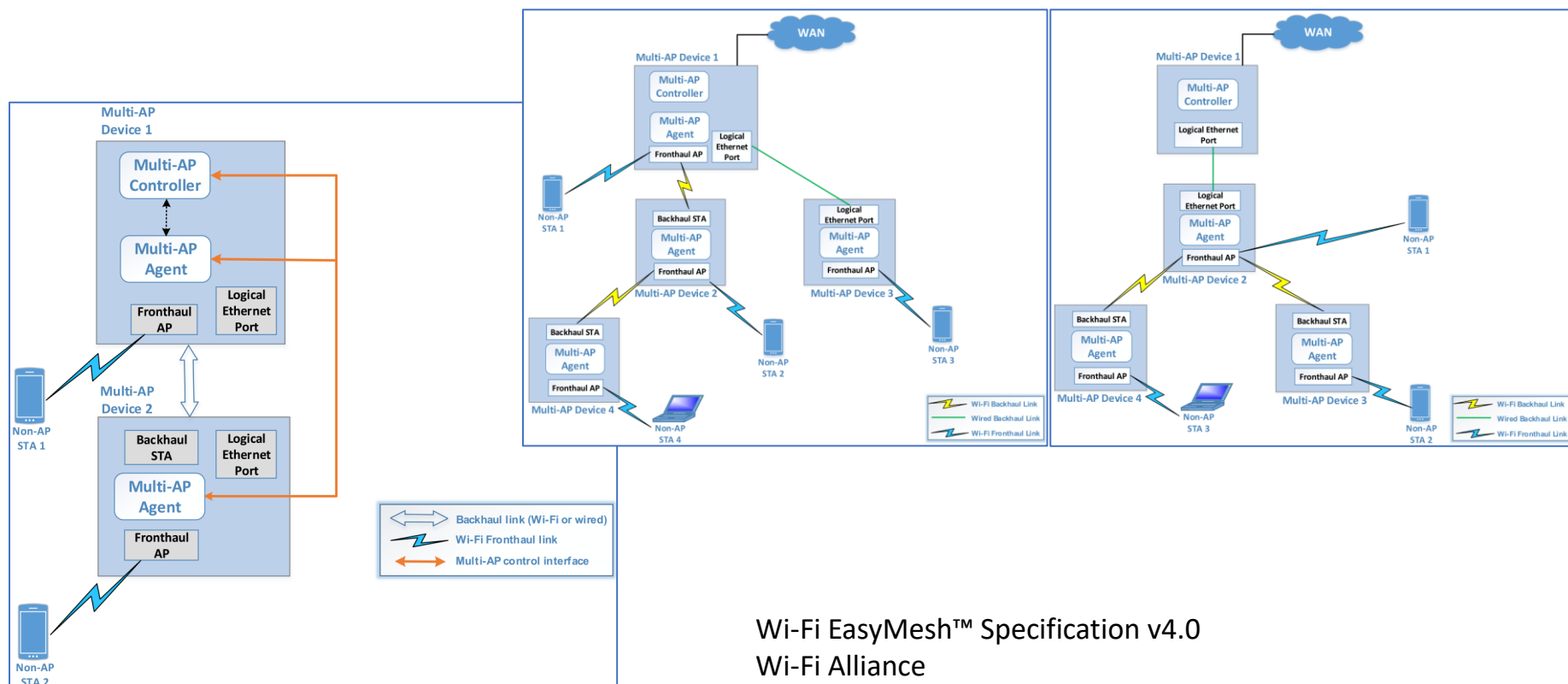


# Architecture and components

- **Controller** - every EasyMesh network must have one. The controller can be a unique device or embedded in a device that also has other functionality
- **Agent** - in order for a mesh network to exist, at least two agents must be connected to the controller
- **Device** - any component of a mesh network, whether it contains a controller, an agent, or both



# Example deployments





- the specification does *not* standardize algorithms or decision-making
- How to do client steering makes up a significant part of the specification, telling manufacturers how to direct a client from one access point to another.
- When a client should be steered is not covered. Therefore, algorithms will still vary (and client roaming mechanisms may of course still interfere).



## NETWORK OPERATION MECHANISMS



Network operation mechanisms are needed to create and maintain a self-optimizing network that maximizes performance and improves client roaming

- **Capability reporting** - The master node uses the information sent by other nodes to maintain optimal network performance. Based on network conditions reported by the nodes in the network, the master node could send control commands to one or more nodes to move to a different channel, decrease transmit power, or report bandwidth utilization
- **Channel selection** - The Wi-Fi EasyMesh controller obtains preferred operating channels for the nodes and sets the operating configuration (such as channels, transmit power, etc.) including preferences and restrictions for each radio in the nodes
- **Link metric collection** - Defines the protocol for network devices to convey link metric information associated with the network
- **Client steering** - Master Node may choose to send control messages to "steer", or suggest, a client move its connection from one node to another
- **Optimizing connection between agents** - Manage the connections between nodes by selecting the best path (wired, wireless, or mixed) between nodes to optimize the network