Wi-Fi Crash Course

A noobs guide to key terms and concepts

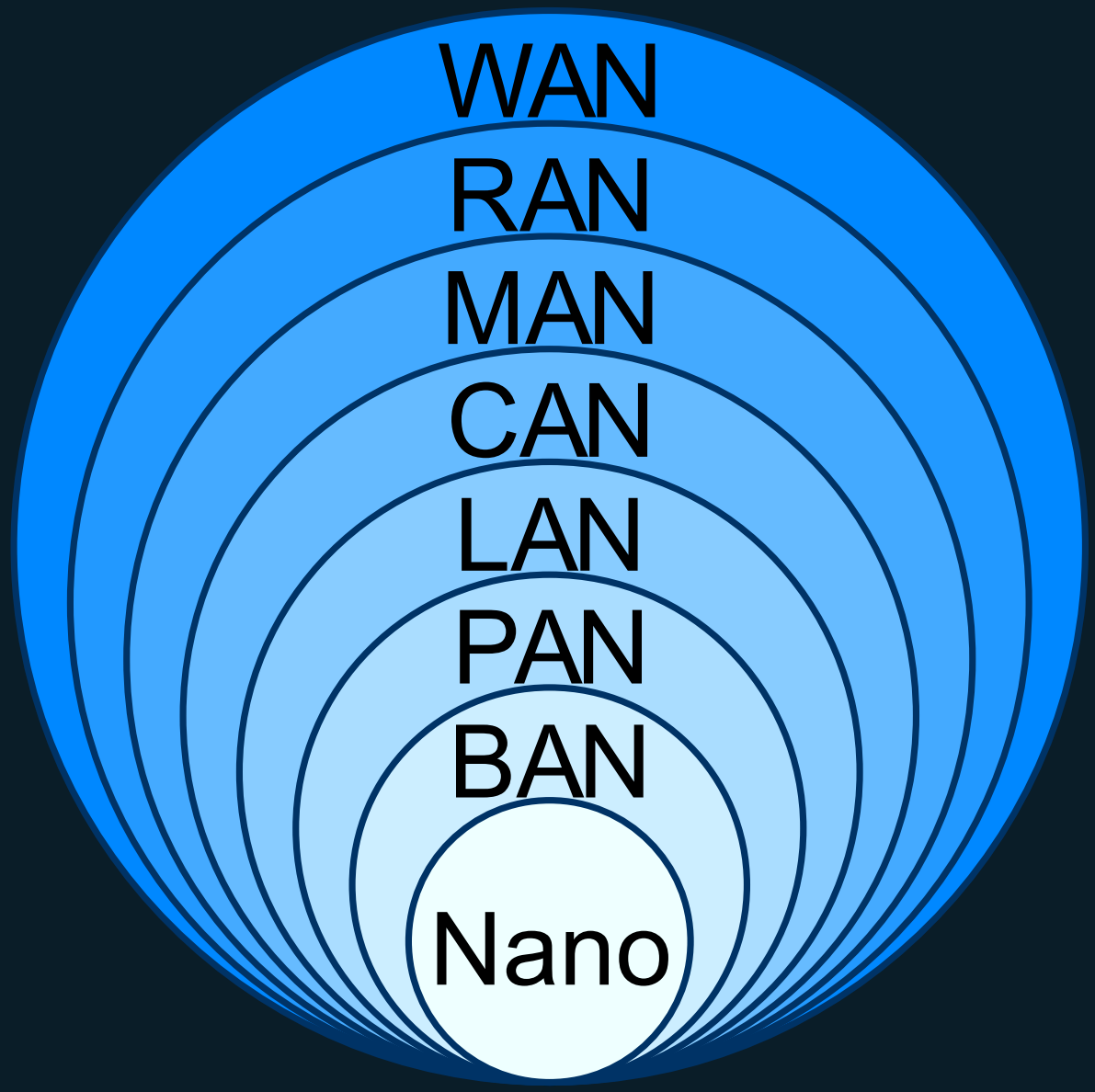
Who am I ?

- Darian Leung
- Senior Embedded Software Engineer
- 7 years at Espressif
- Software Platforms Team
- ESP-IDF Development
  - Core Subsystems
  - Protocols

Contents

What is Wi-Fi & IEEE 802.11

WLAN, Standards, and Amendments



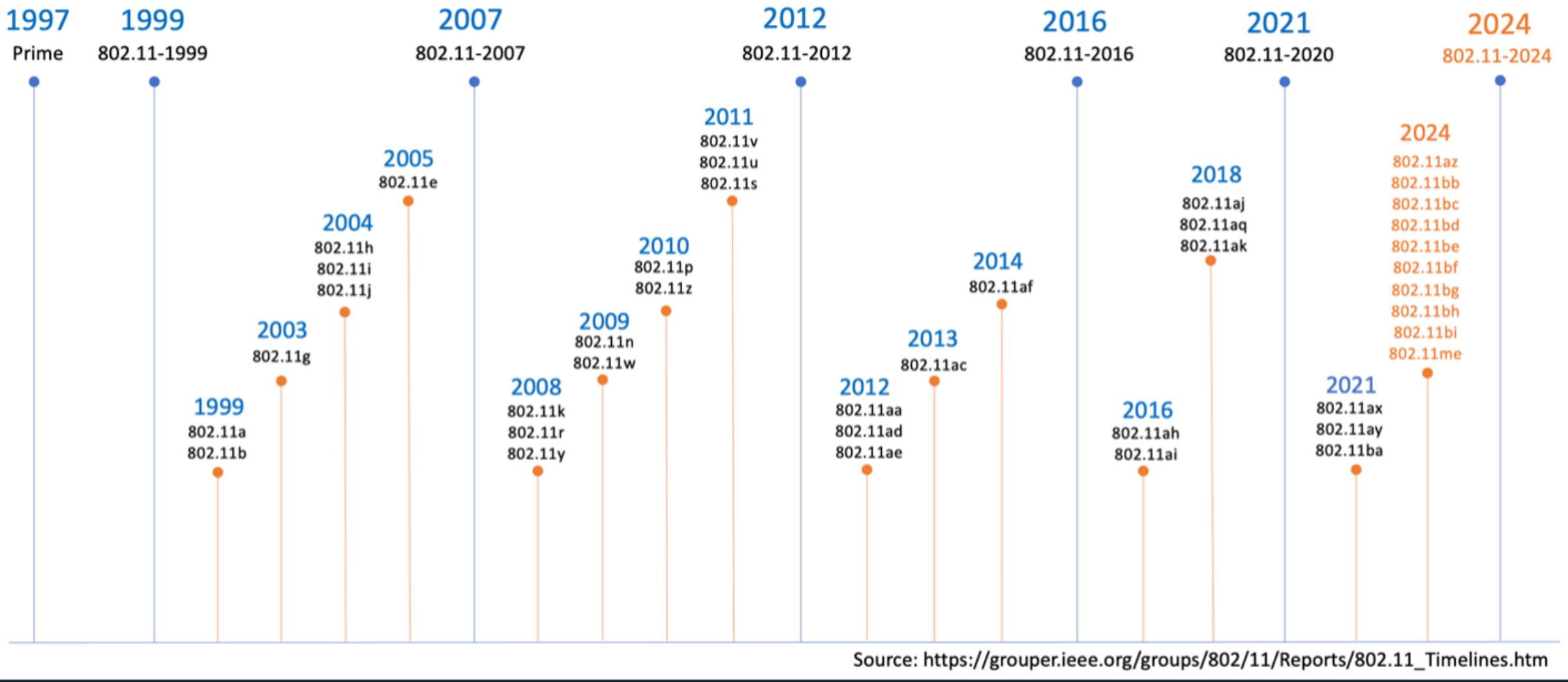
- Computer networks categorized by spatial scope
- Local Area Network (LAN)
  - E.g., residence, campus, office
- Ethernet: Wired LAN
- Wi-Fi: Wireless LAN (WLAN)

What is LAN & WLAN

- IEEE 802.11
  - Set of protocol standards for Wireless Local Area Networks (WLAN)
  - Created/maintained by IEEE
- Wi-Fi
  - Trademark owned by Wi-Fi Alliance
  - Certified products labelled “Wi-Fi Certified”
- Terms used interchangeably

Wi-Fi vs IEEE 802.11

IEEE 802.11 Standards Timeline



Source: https://grouper.ieee.org/groups/802/11/Reports/802.11_Timelines.htm

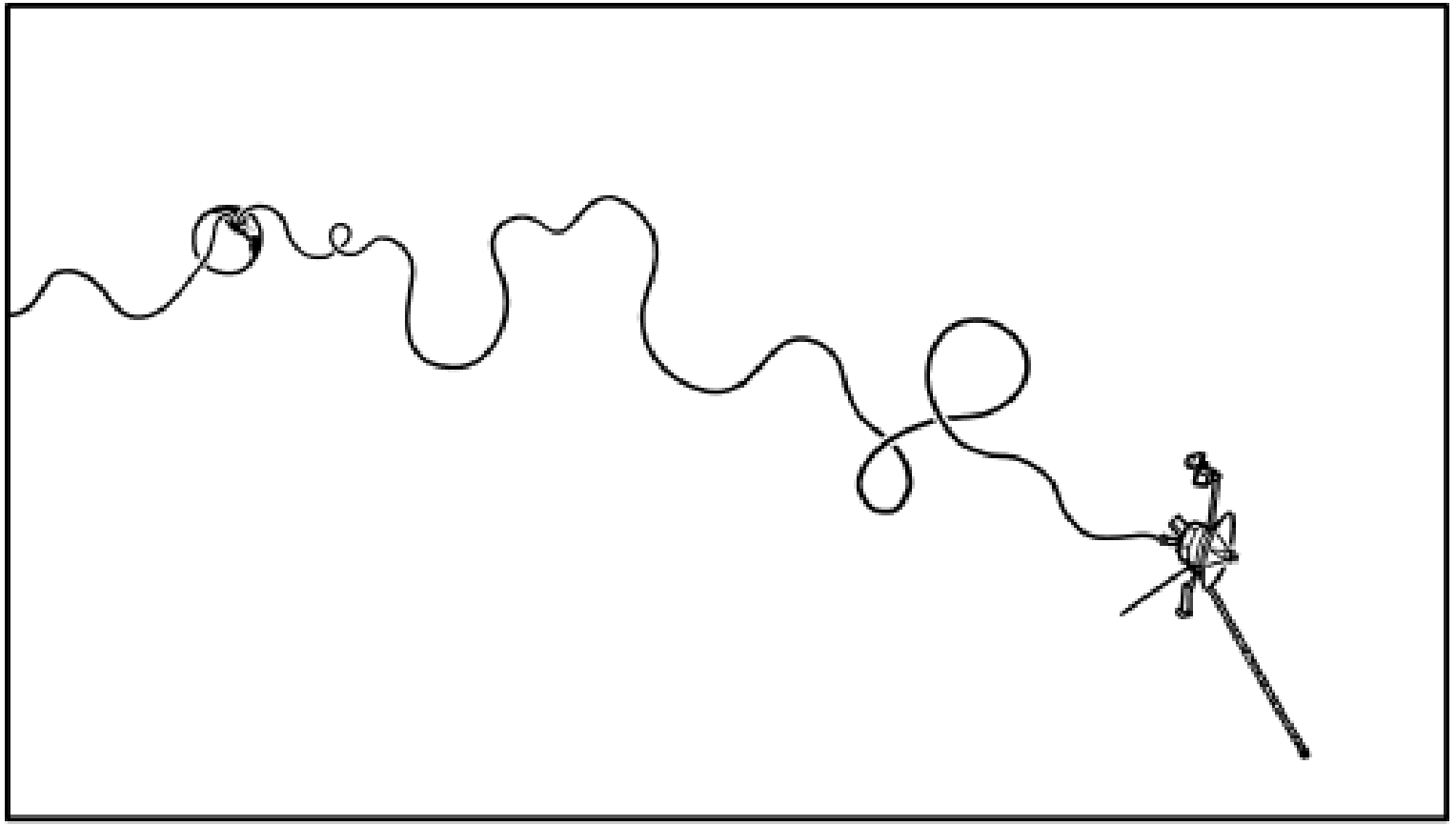
802.11 Versioning

Wi-Fi Gen	Key Features Added	Amendment	Incorporated Standard	Max Link Rate (Mb/s)
0	DSSS, FHSS	N/A	802.11-1997	1-2
1	CCK	802.11b-1999	802.11-2007	11
2	5GHz OFDM	802.11a-1999	802.11-2007	6-54
3	2.4GHz OFDM	802.11g-2003	802.11-2007	6-54
4	MIMO	802.11n-2009	802.11-2012	6.5-600
5	5GHz MU-MIMO, 256-QAM	802.11ac-2013	802.11-2016	6.5–6933
6	TWT, OFDMA, 1024-QAM,	802.11ax-2021	N/A	0.4–9608

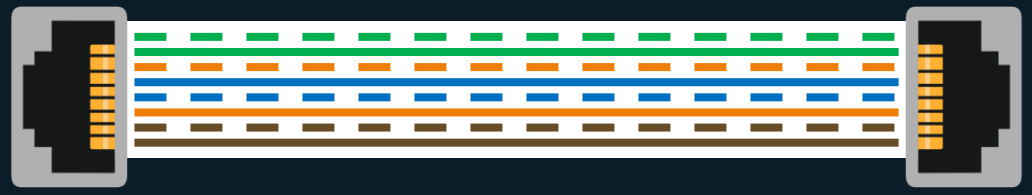
Amendments & Generations

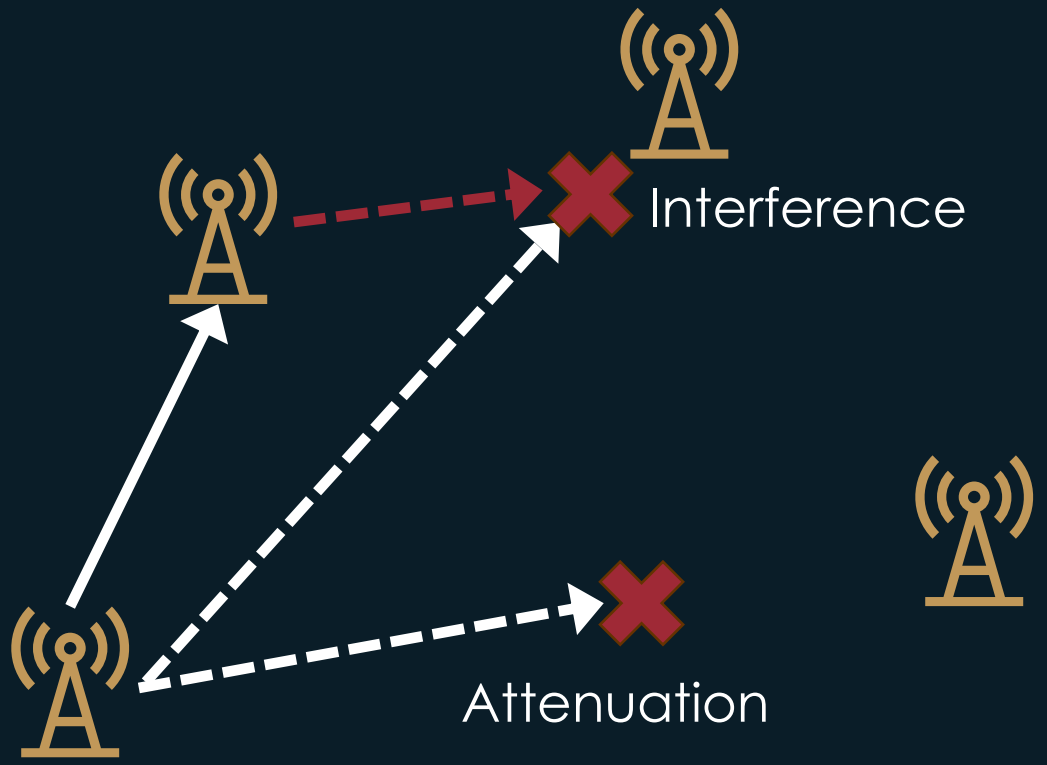
The Wireless Medium

Wired vs Wireless



SAD NEWS: DUE TO HIGH COPPER PRICES AND BUDGET CONSTRAINTS, NASA MAY FINALLY HAVE TO CUT THE WIRES THAT THEY'VE BEEN SPOOLING OUT TO COMMUNICATE WITH VOYAGER 1 AND 2.





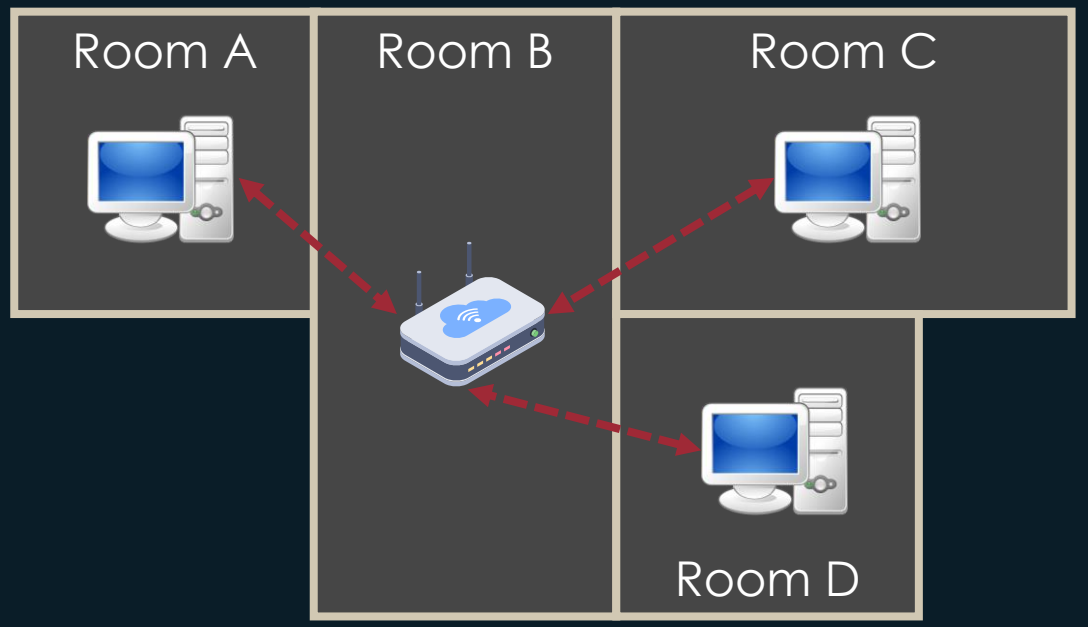
Wired (Ethernet)

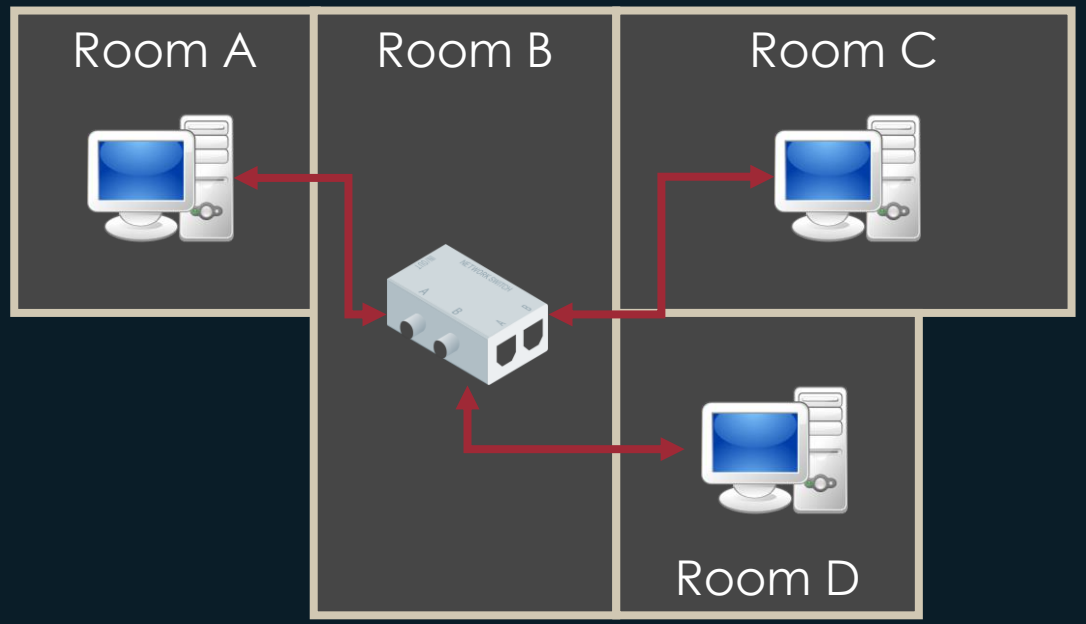
- Unicast (if not bus)
- Reliable delivery (differential signaling)
- Full-duplex (if multiple wires)

Wireless (Wi-Fi)

- Broadcast
- Half-duplex (same frequency)
- Unreliable delivery
  - Attenuation
  - RF interference

Wired vs Wireless Medium





Advantages

- Device Mobility
- Ease of deployment
- Flexibility
- Cost

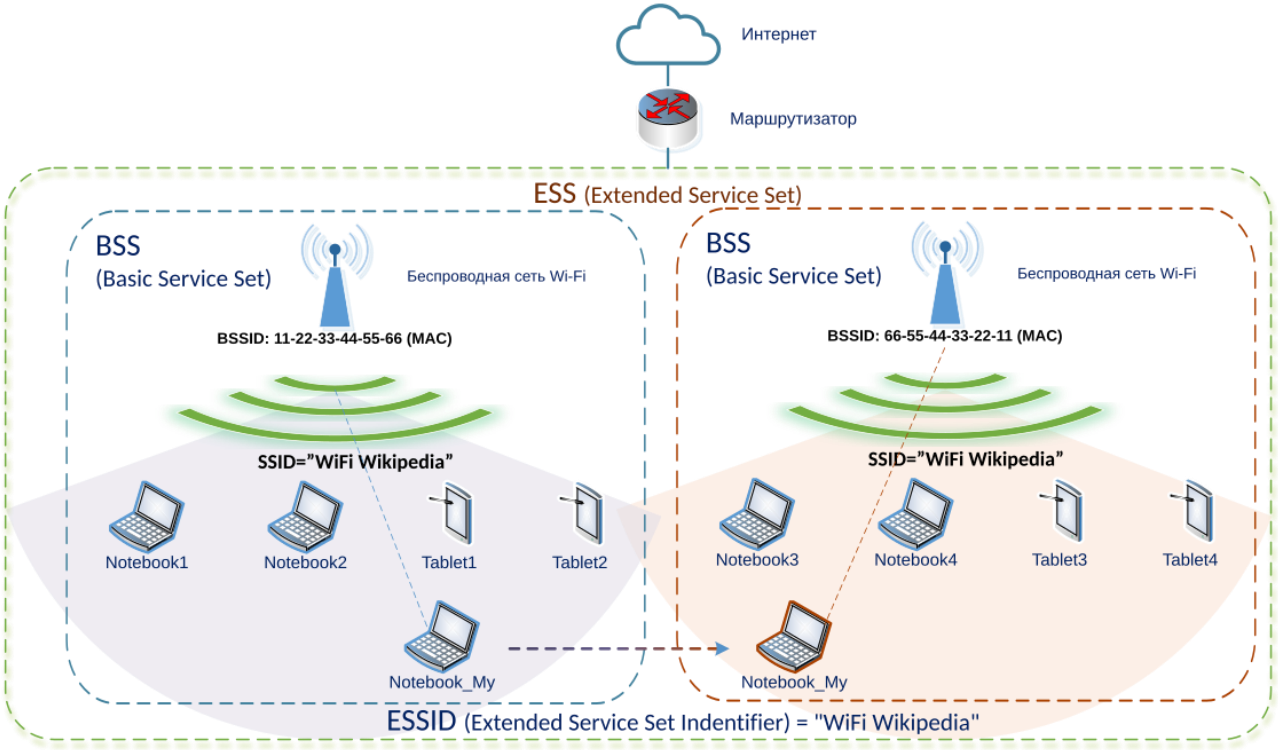
Disadvantages

- Lower Throughput
- Less reliability
- Less security

Benefits of Wireless

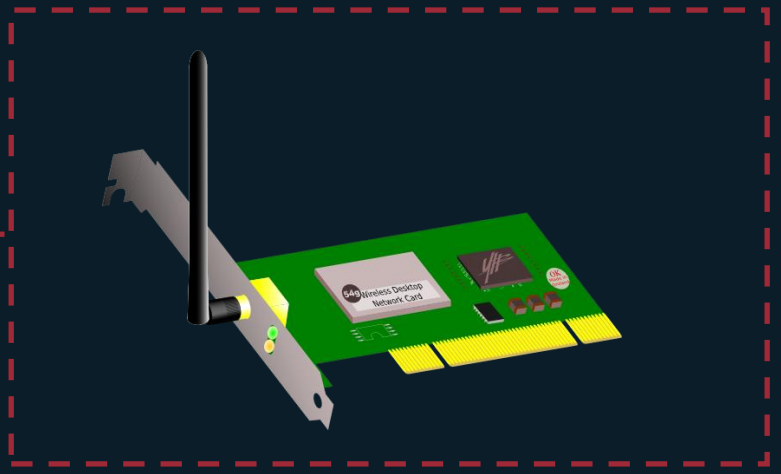
Wi-Fi Topologies

Terminology & Topologies



STA-A

AA:BB:CC:DD:EE:01



STA-B

AA:BB:CC:DD:EE:02

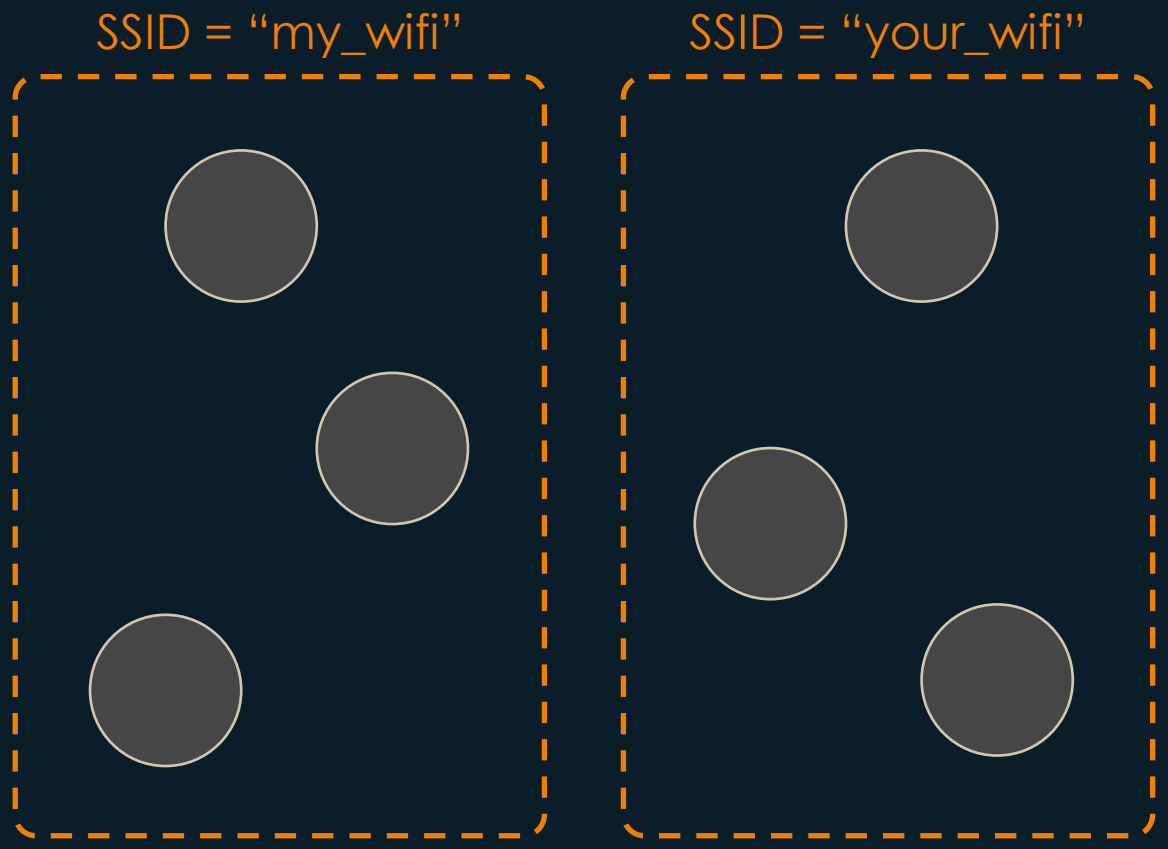
STA-B

AA:BB:CC:DD:EE:03

- Any 802.11 capable device is known as a station (STA)
- Typically the Wireless Network Interface Controller (WNIC)
- Unique MAC address
- Antenna/Radio for wireless connection

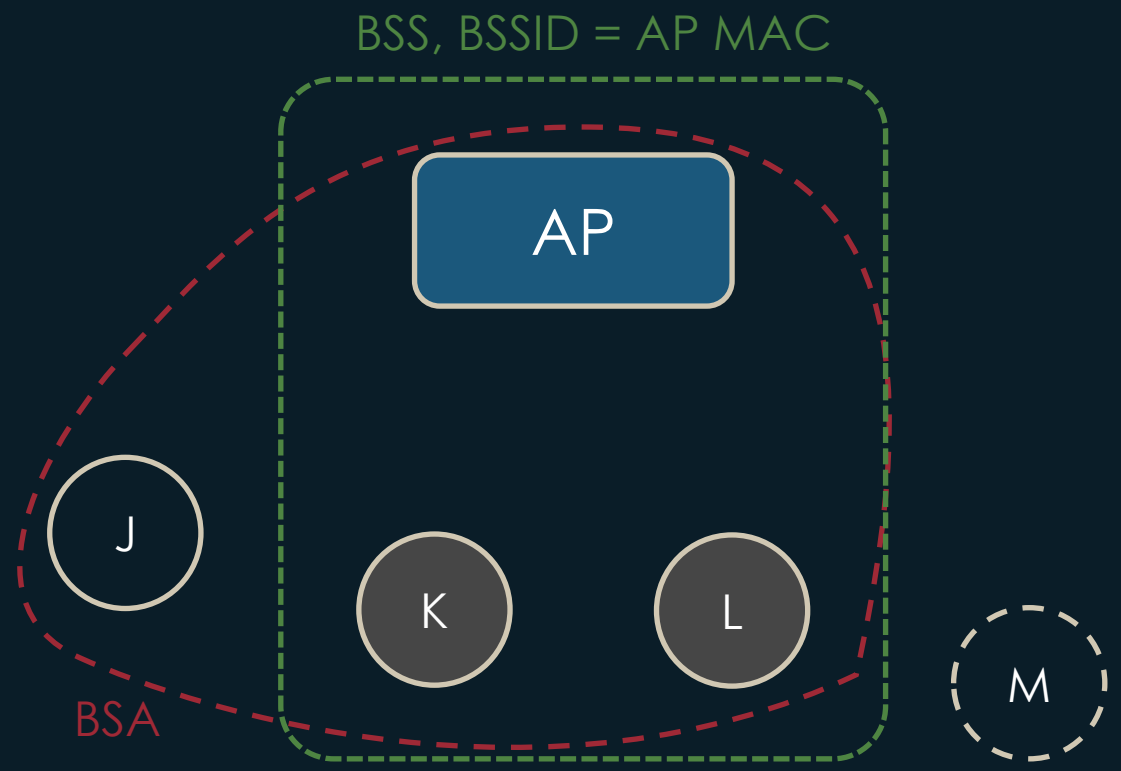
Wi-Fi Stations

STA



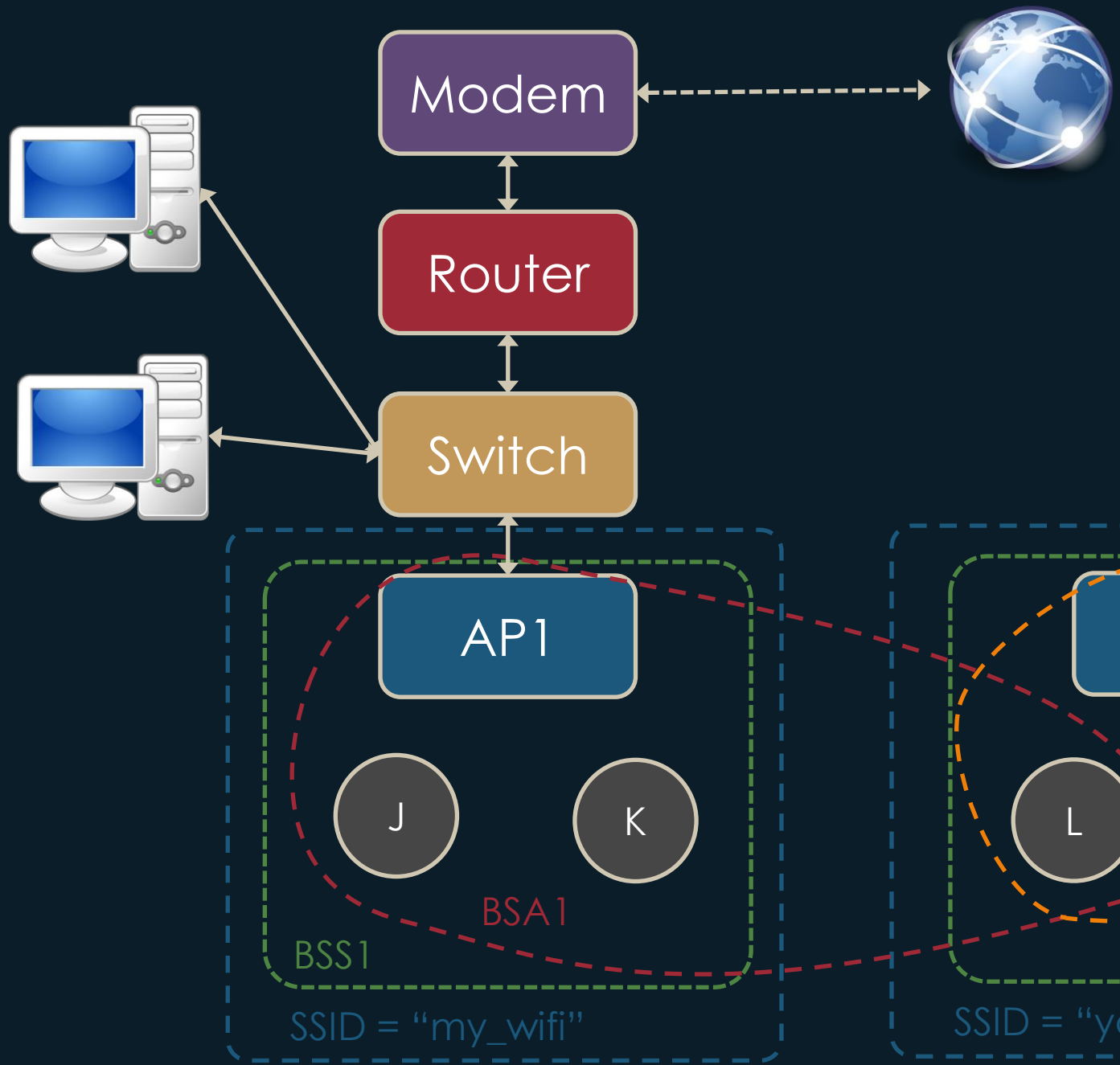
- Grouping of STAs is a Service Set (i.e., WLAN)
- Service Set Identifier (SSID)

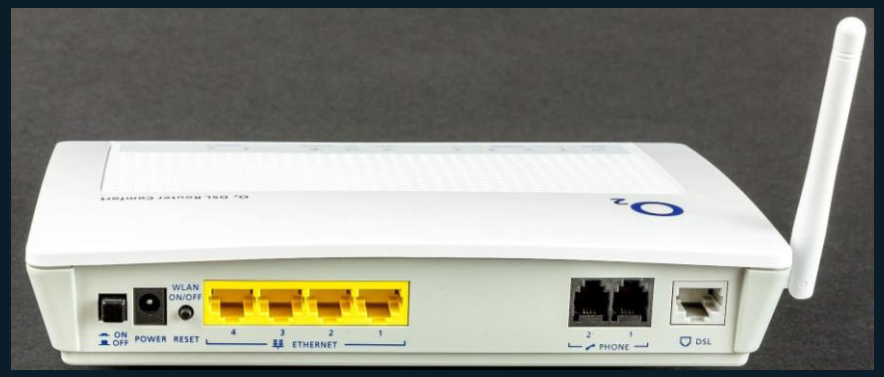
Service Sets



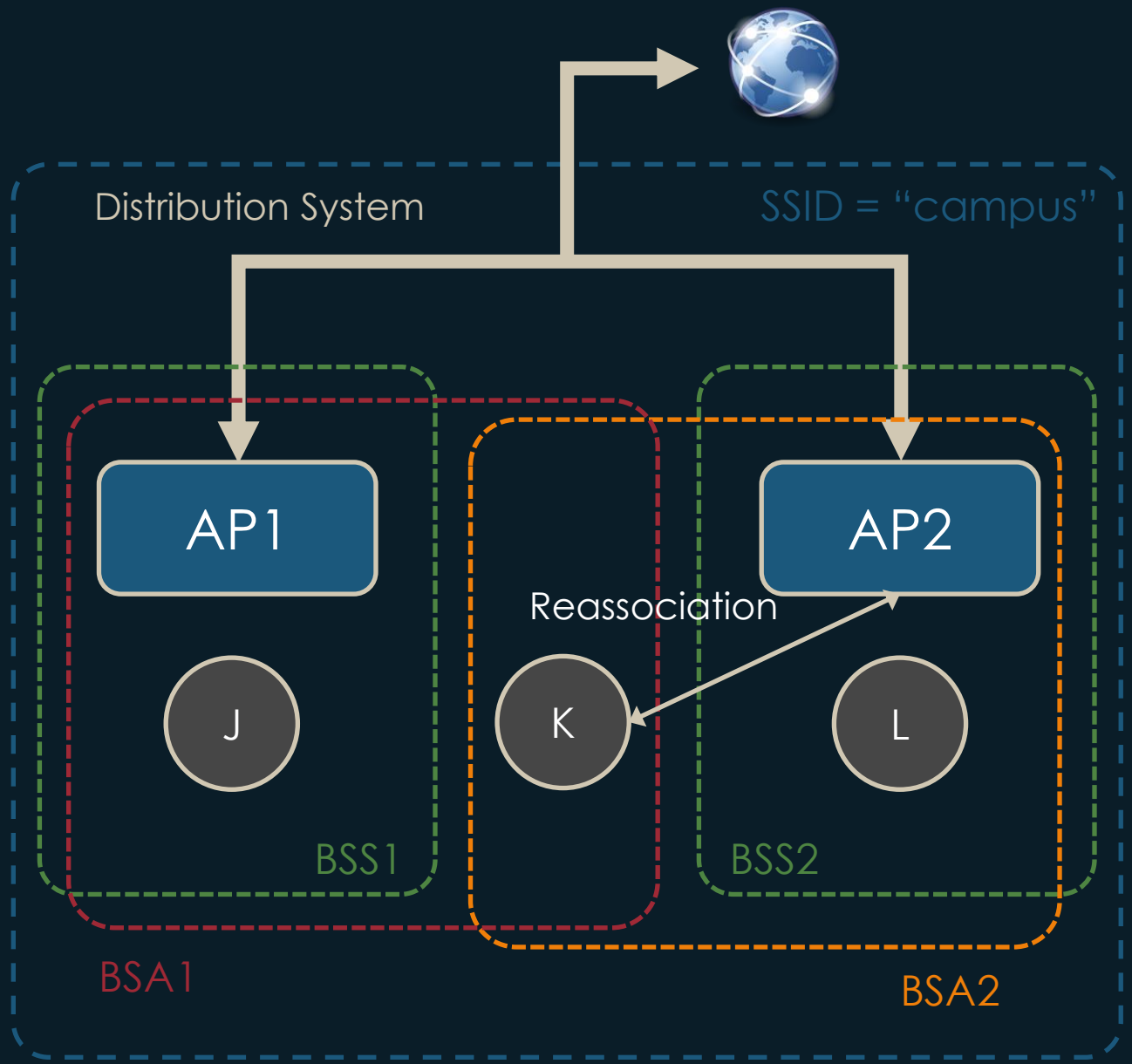
- (Infrastructure) BSS
  - Typical SOHO network
  - Single AP, one or more STAs
- Access Point (AP)
  - Is itself a STA
  - Acts like network switch
- BSS Identifier (BSSID)
  - Not the same as SSID
  - Is MAC address of AP
- STAs associate with AP
- Basic Service Area (BSA)
  - Physical coverage of AP
  - Based on RSSI thresholds

Basic Service Set (BSS)



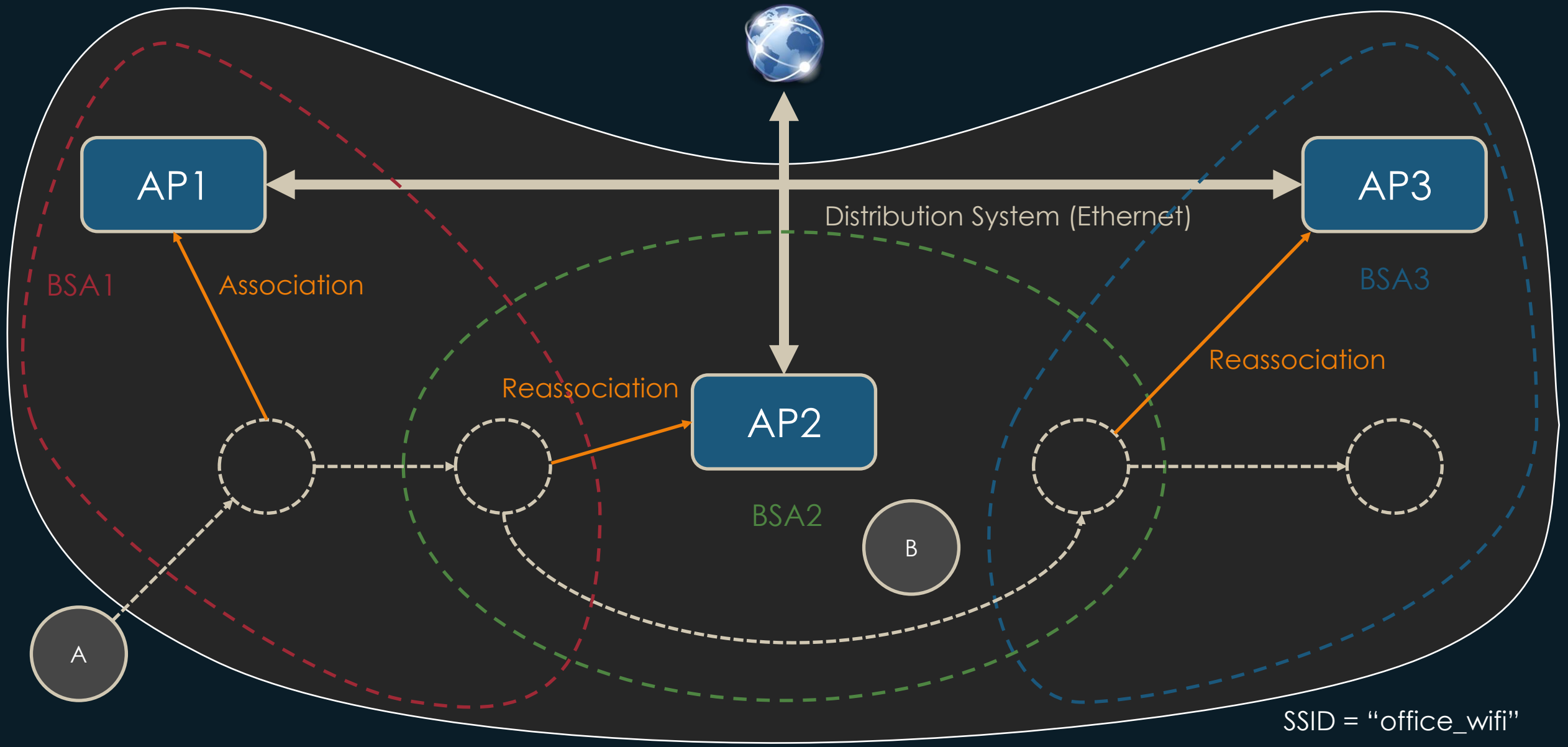


BSS in Practice



- Extended Service Set (ESS)
  - Two or more BSS connected by a DS
- Seamless roaming
  - Overlapping BSAs to form ESA
  - STA reassociates with stronger AP
- Distribution System (DS)
  - Implementation not defined by 802.11
  - Tracking STA associations
  - Forwards frames between APs
- Same logical network
  - Same SSID

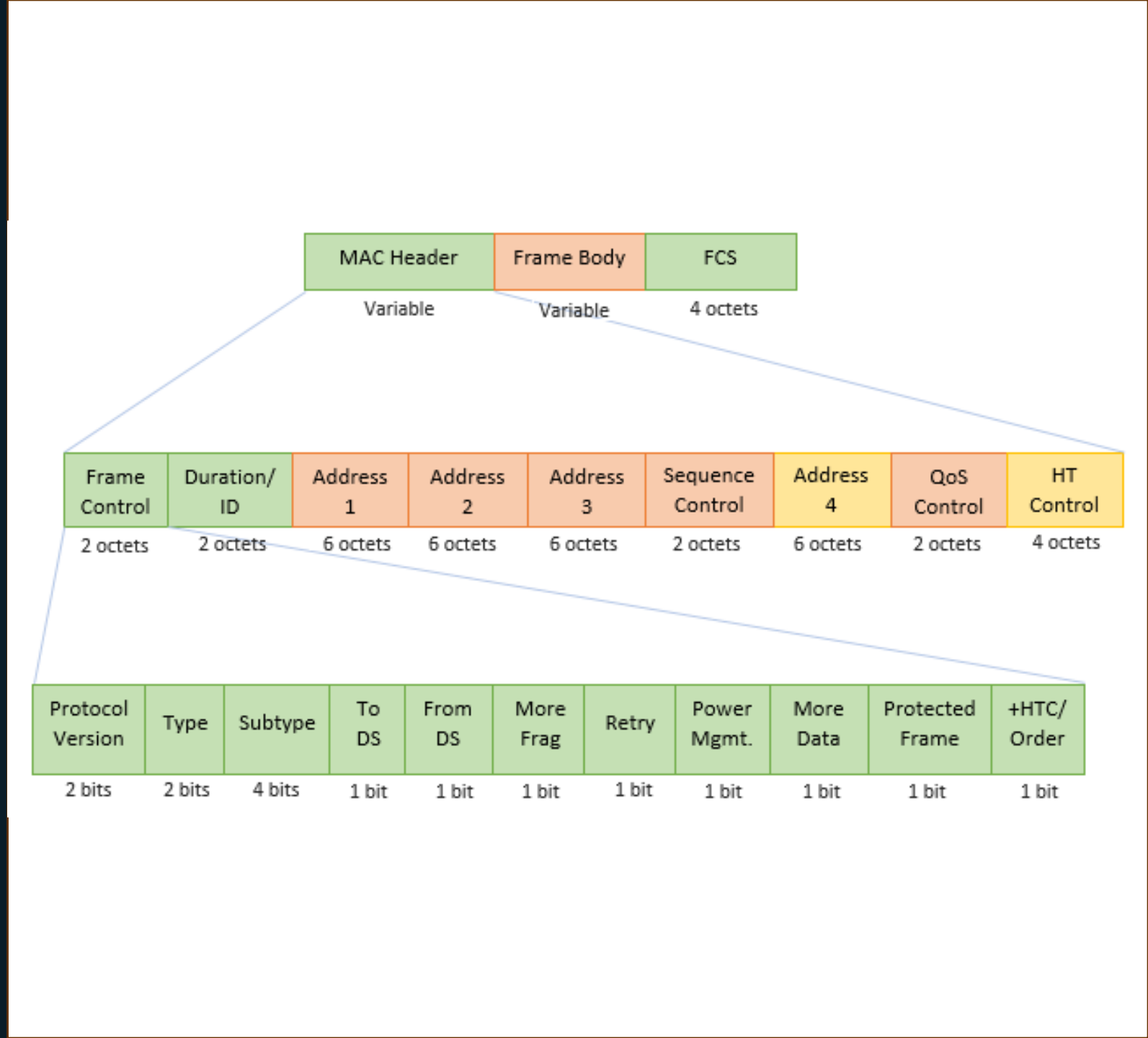
Extended Service Set (ESS)

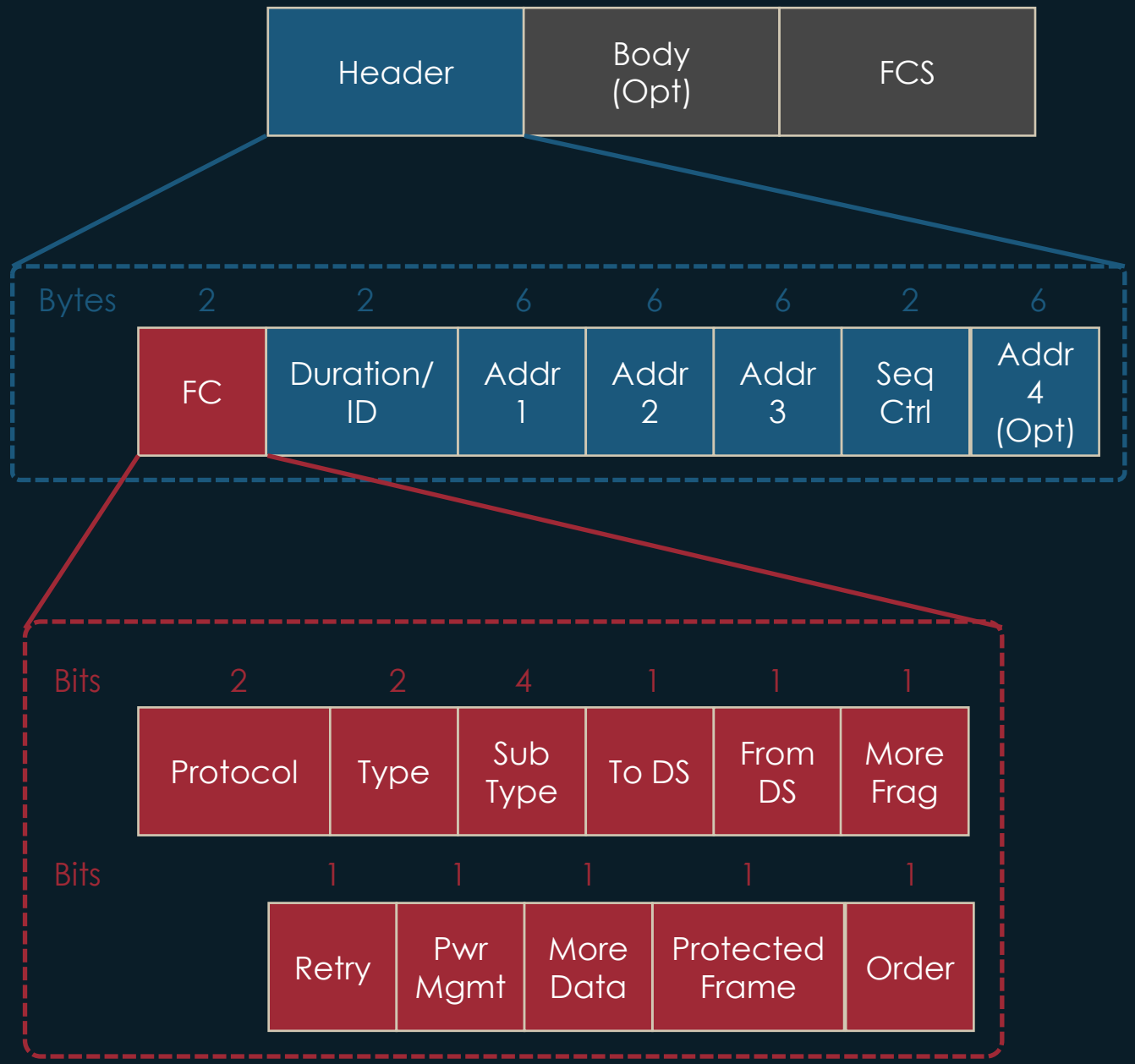


ESS in Practice

MAC Frames

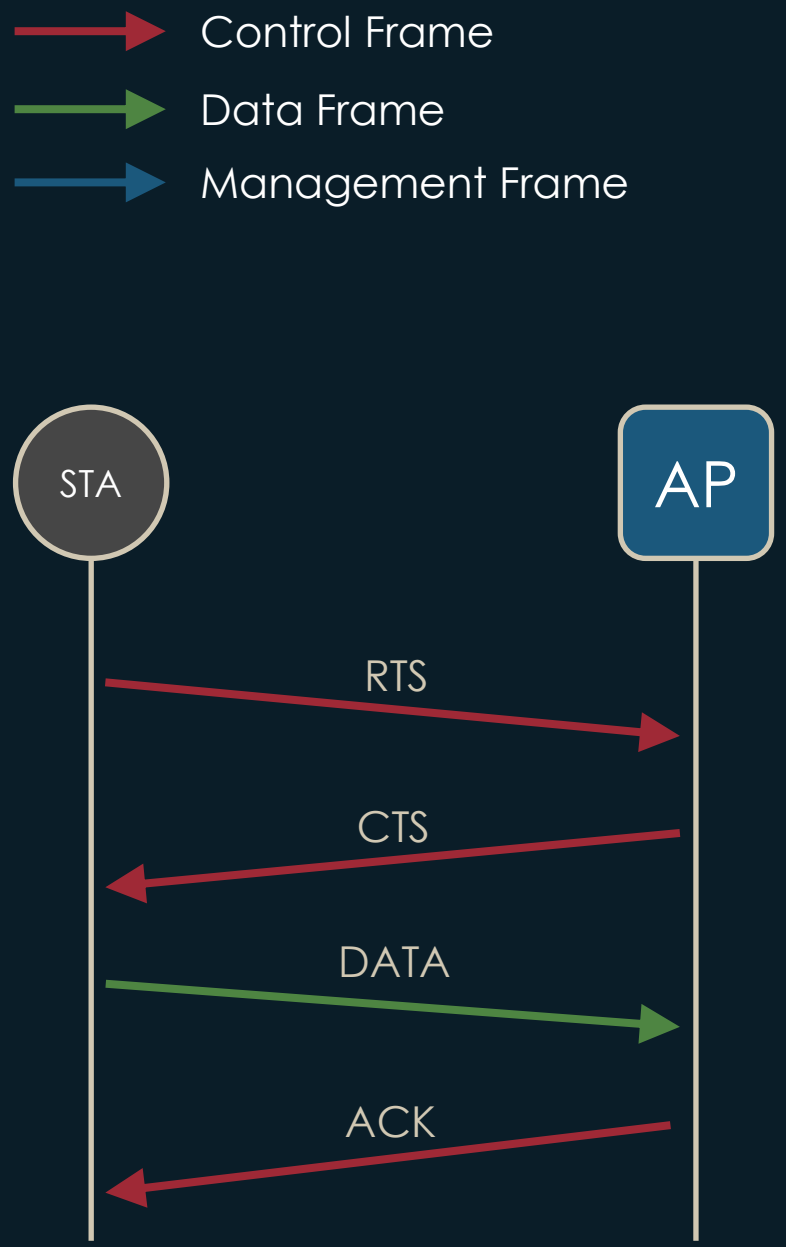
Frame, Frame Types





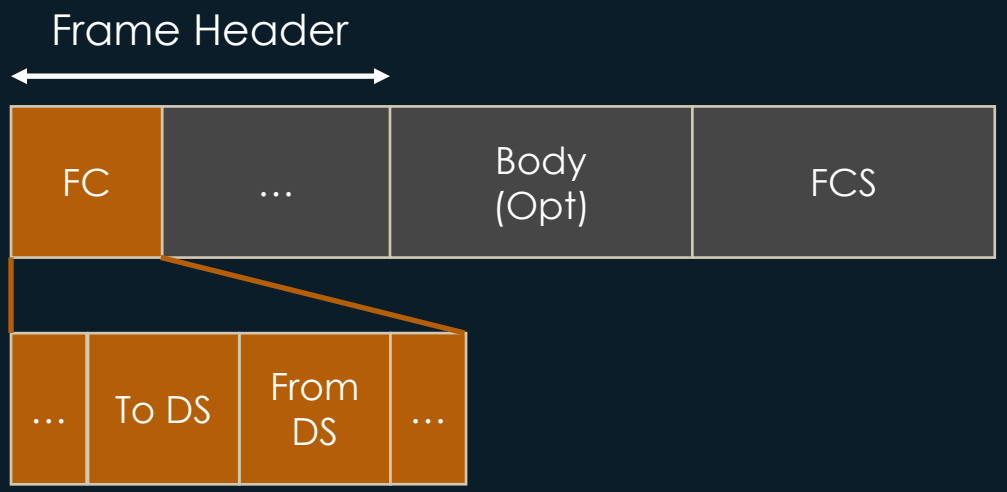
- Frames are a basic unit transmission
- Frame Body
  - Payload or contents
- Frame Check Sequence (FCS)
  - CRC calculated from header and body
- Frame Header
  - Source/Receiver/Destination MAC addresses
  - Sequence Control: Related to sequencing and fragmenting of payloads
  - Frame Control (FC) determines frame type

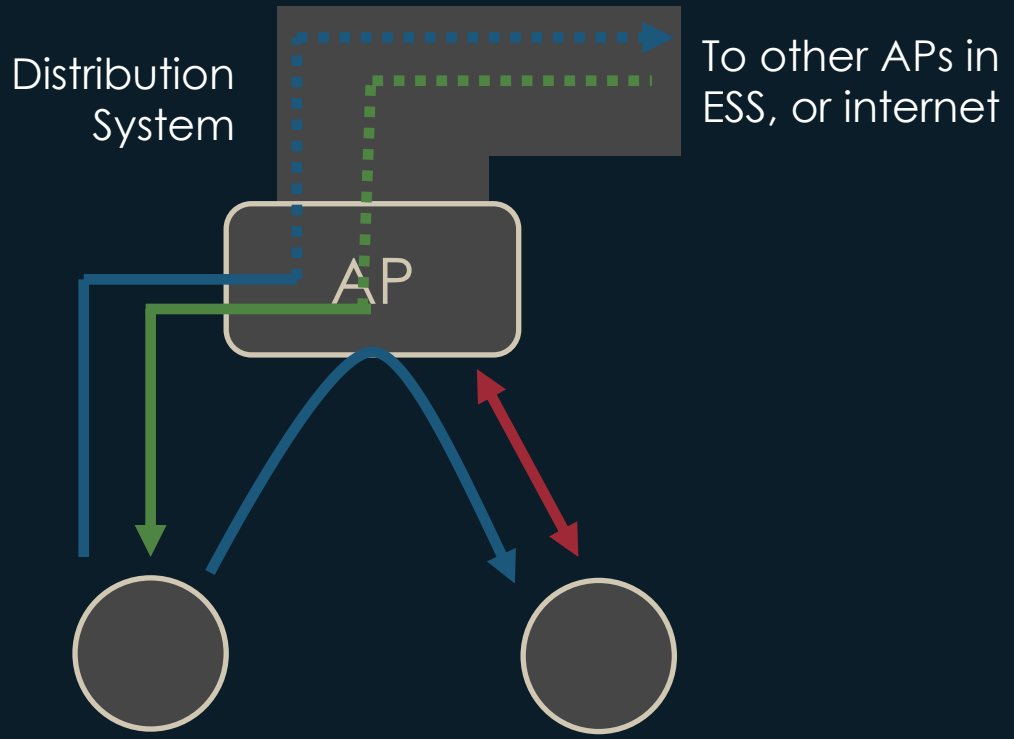
MAC Frame



- Data Frames
  - Carries data from higher-layer protocol
  - E.g., IP packet
- Control Frames
  - Assist with delivery of other frames
  - No frame body (i.e., payload)
  - Typically part of multi-frame exchange
- Management Frames
  - Manages STAs in the BSS
  - E.g., Scanning, Association, reassociation

Frame Types

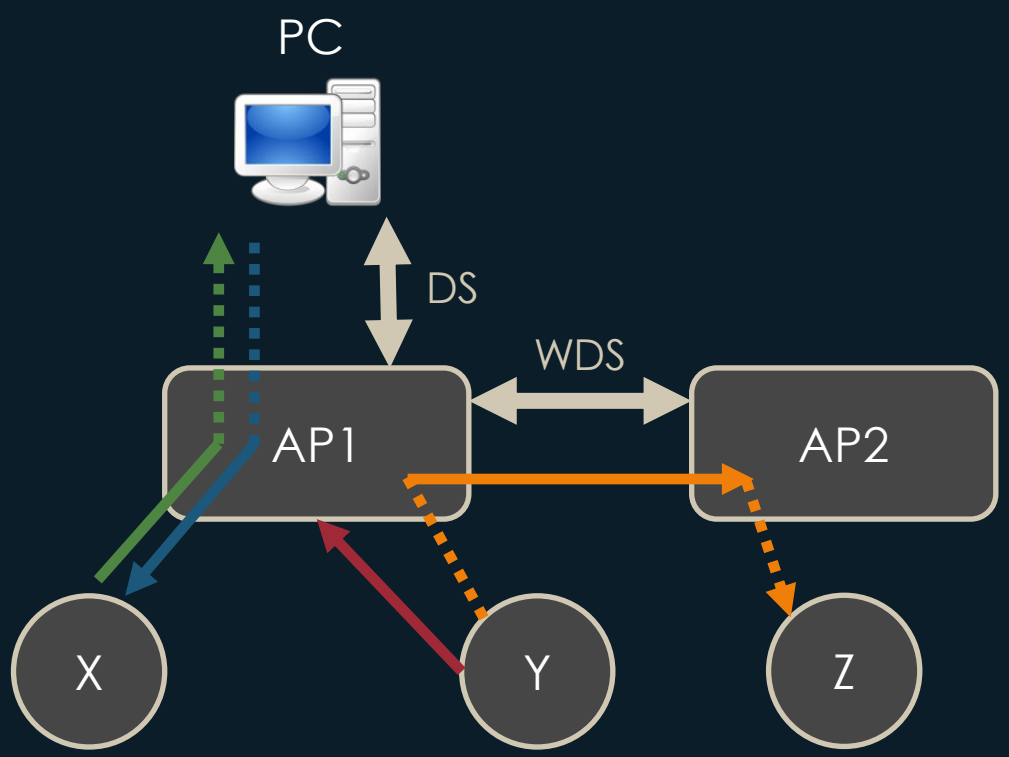




- Bits indicated direction of a wireless frame's traversal
  - To DS: Frame is destined for DS
  - Form DS: Frame is from DS
- 2-bit combination affects how header MAC Addresses 1 to 4 fields are interpreted

	To DS = 0	To DS = 1
From DS = 0	Management and Control Frames	Data frames from STA to AP
From DS = 1	Data frames from AP to STA	Only used in Wireless Distribution Systems

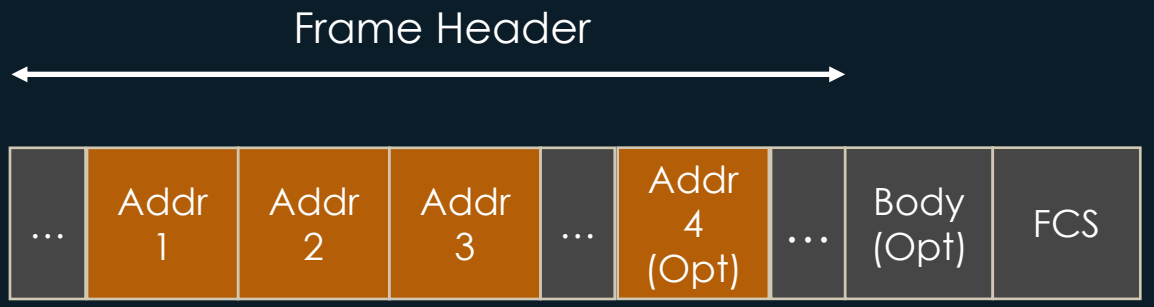
To/From DS Bits



SA	DA	TA	RA	To DS	From DS
Y	AP1	Y	AP1	0	0
PC	X	AP1	X	0	1
X	PC	X	AP1	1	0
Y	Z	AP1	AP2	1	1

- All address fields are MAC Addresses
  - (6 bytes) `XX:XX:XX:XX:XX:XX`
  - Shares address space with Ethernet
- Source Address (SA)
  - Original source of the MAC frame
- Destination Address (DA)
  - Final destination of the MAC frame
- Transmitter Address (TA)
  - STA/AP that transmitted the frame onto wireless medium
- Receiver Address (RA)
  - STA/AP that should process the wireless frame
- Notice that there is always an address repeated

Address Types



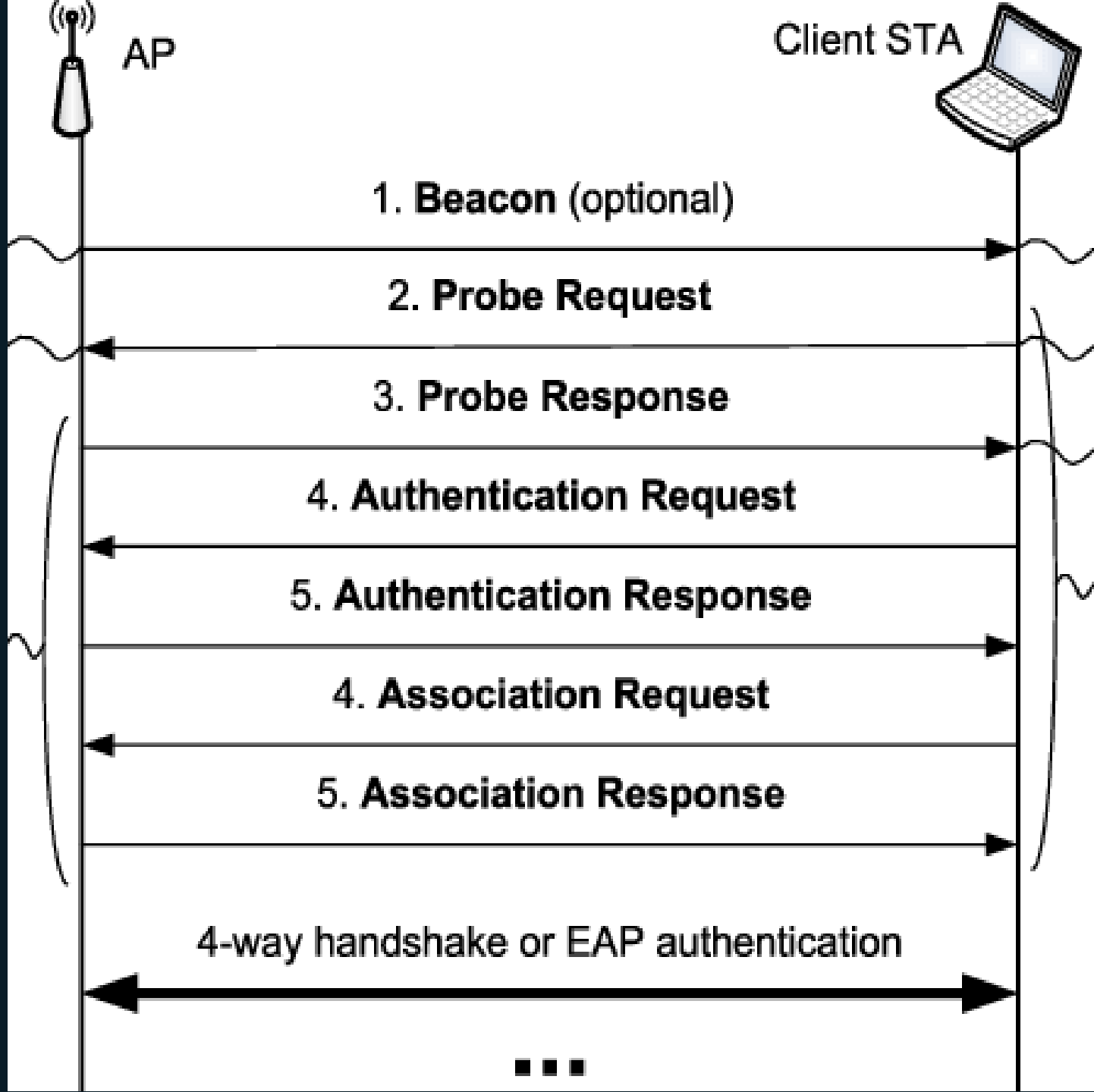
- Addr 4 is optional. Only used when "To DS" and "From DS" are 0
- Address fields can represent SA, DA, TA, RA, BSSID
- "To DS" and "From DS" fields indicate how to interpret address fields

To DS	From DS	Addr 1	Addr 2	Addr 3	Addr 4	Comment
0	0	DA = RA	SA = TA	BSSID	N/A	Control/management frames
0	1	DA = RA	TA = BSSID	SA	N/A	Data frame from AP to STA
1	0	RA = BSSID	TA = SA	DA	N/A	Data frame from STA to AP
1	1	RA	TA	DA	SA	Data frames between APs in WDS

Address Felds

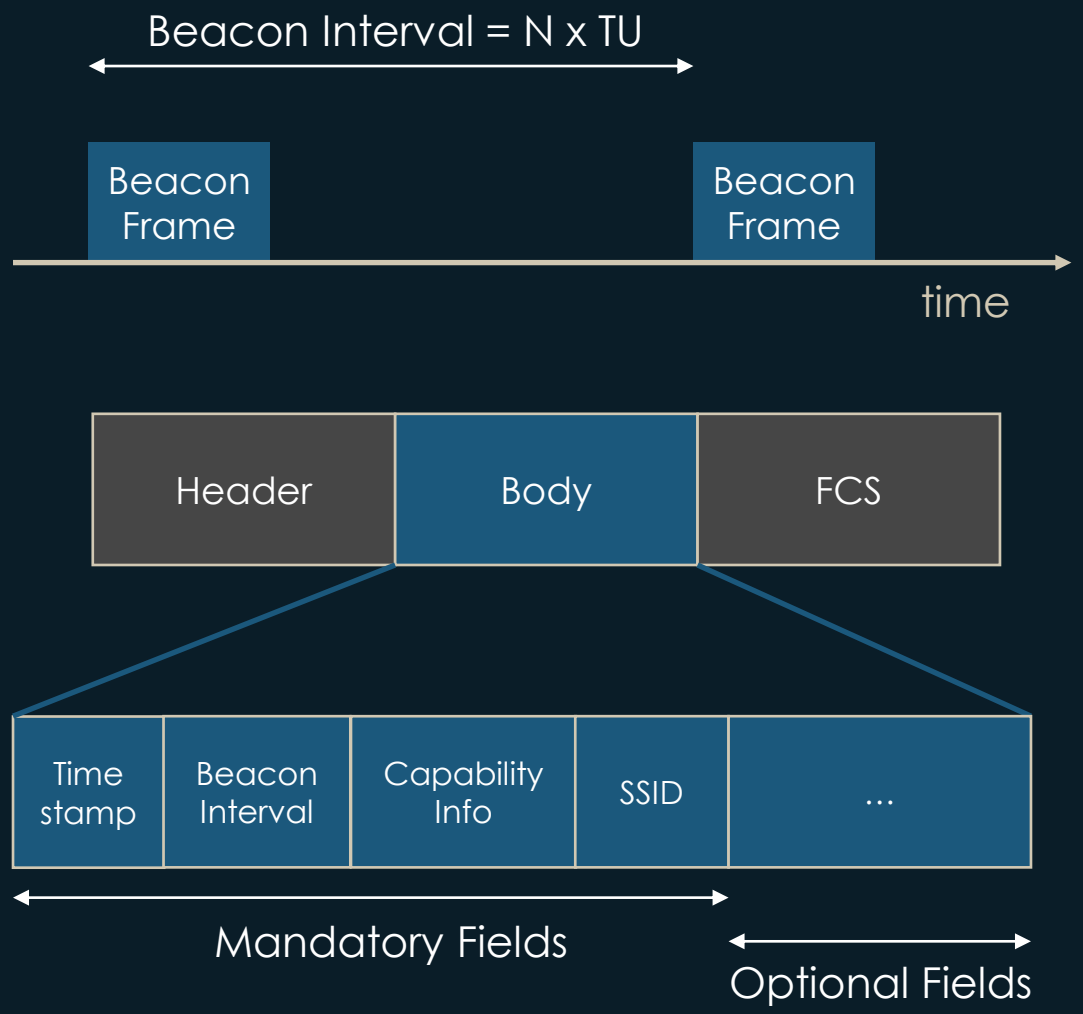
Management Operations

How the wireless link is established and maintained



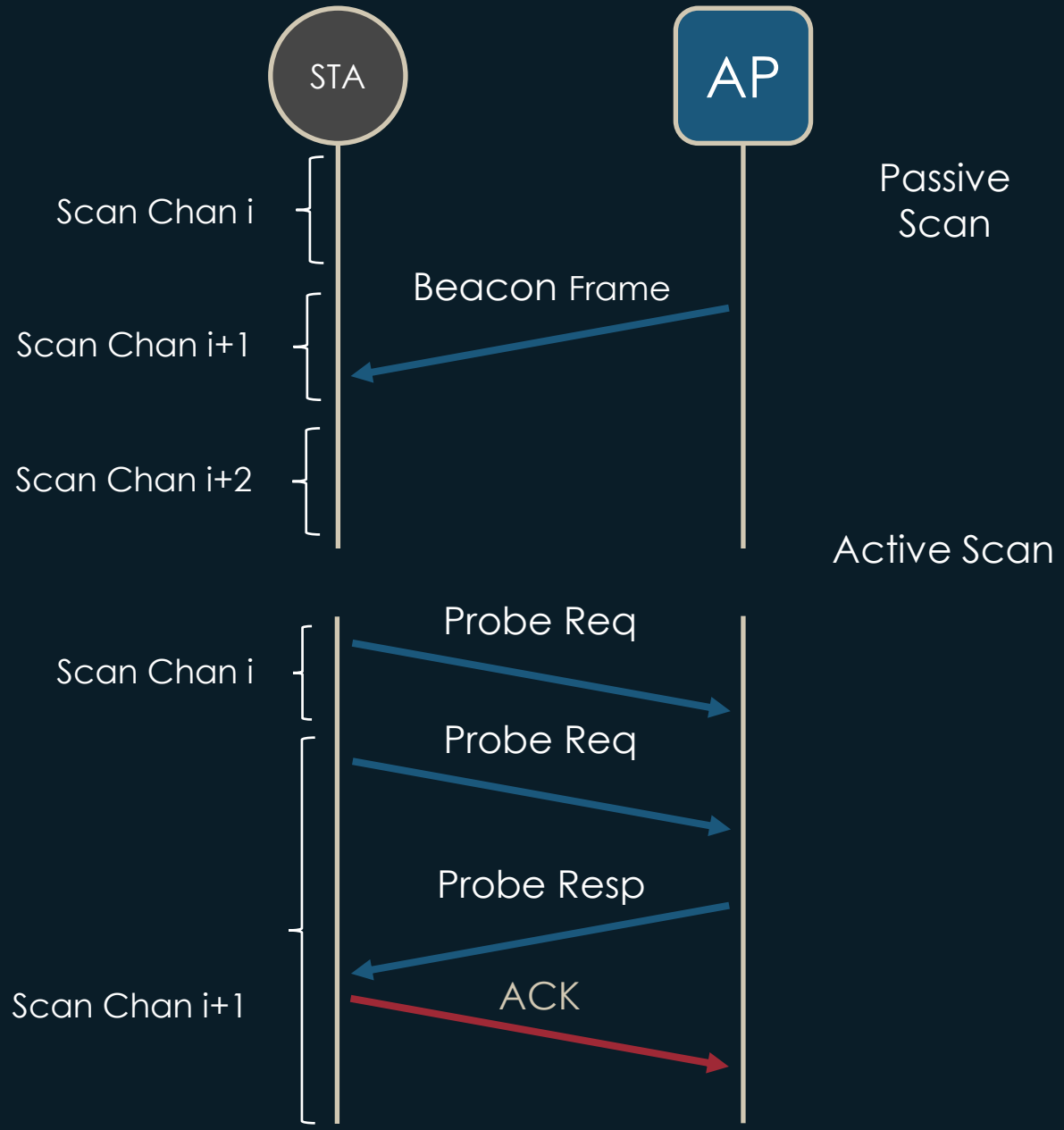
Management Operations

- Establish and maintain the wireless link
- Cooperative effort between APs and STAs
- Typically involves exchanging various management frames
- Scanning
- Authentication
- Association



- Allows networks to announce their existence
- Transmitted periodically by AP in BSS at beacon interval
  - Time units (TU) of 1024μs
  - Typical interval is100 TU ≈ 1ms
- SSID of the network
- Service set capabilities
  - Topology (BSS, ESS, IBSS)
  - Modulation, QoS
- Timestamp (μs)
  - Synchronize STAs local clocks

Beacon Frames

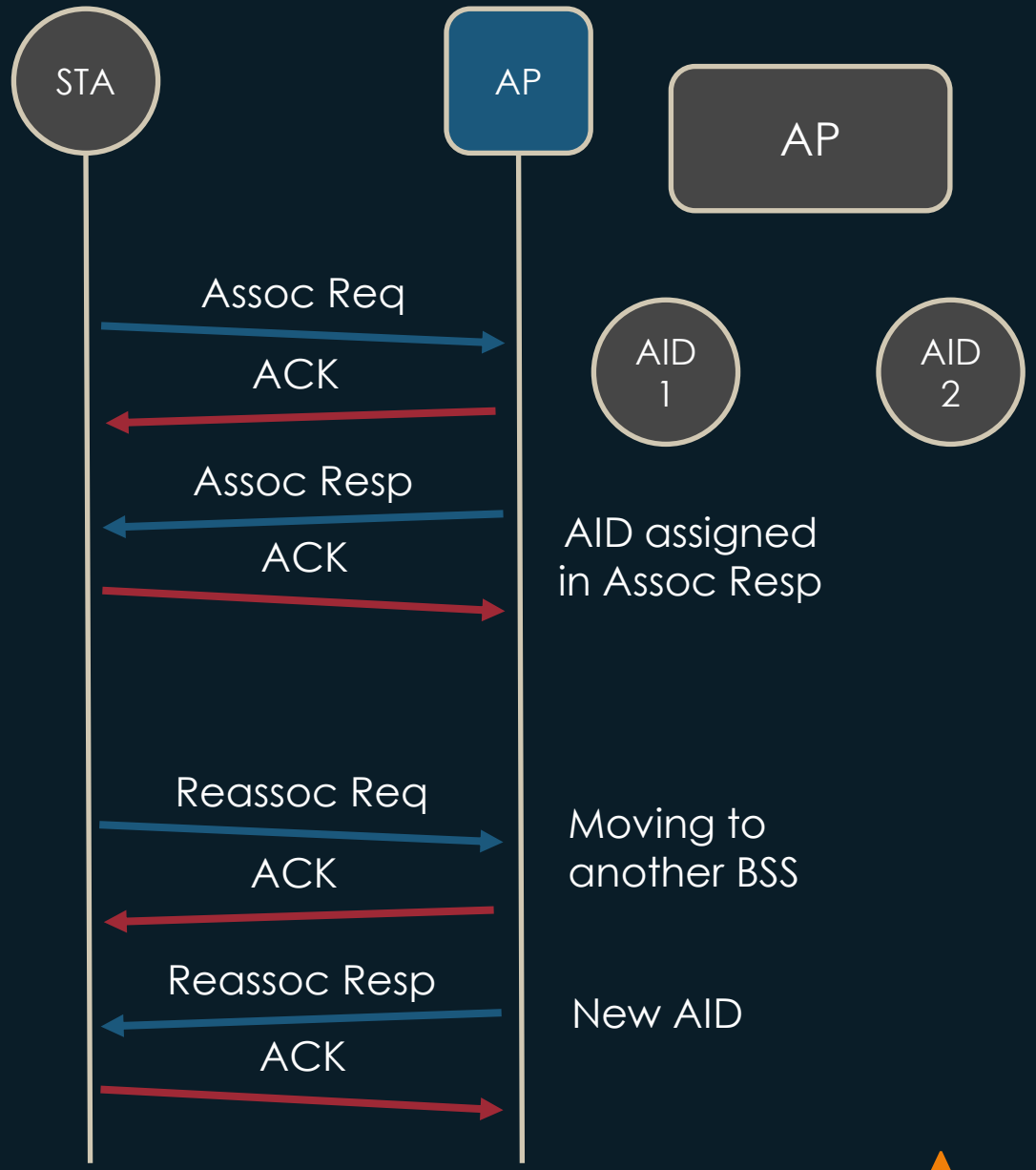


- Process of STAs identifying existing Wi-Fi networks
- Passive Scan
  - Sweeps through different channels (i.e., frequencies)
  - Listens to AP's beacon frames
- Active Scan
  - Sweeps through different channels
  - Transmits a probe request frame
- Generates scan report
- Scan filter by parameters (e.g., SSID, service set type, channel)

Scanning

- Open System Authentication
  - Simple handshake
  - Provides no meaningful security
  - Ensure STA has proper capabilities to join BSS
- Involves Authentication Request and Response frames

Authentication Procedure

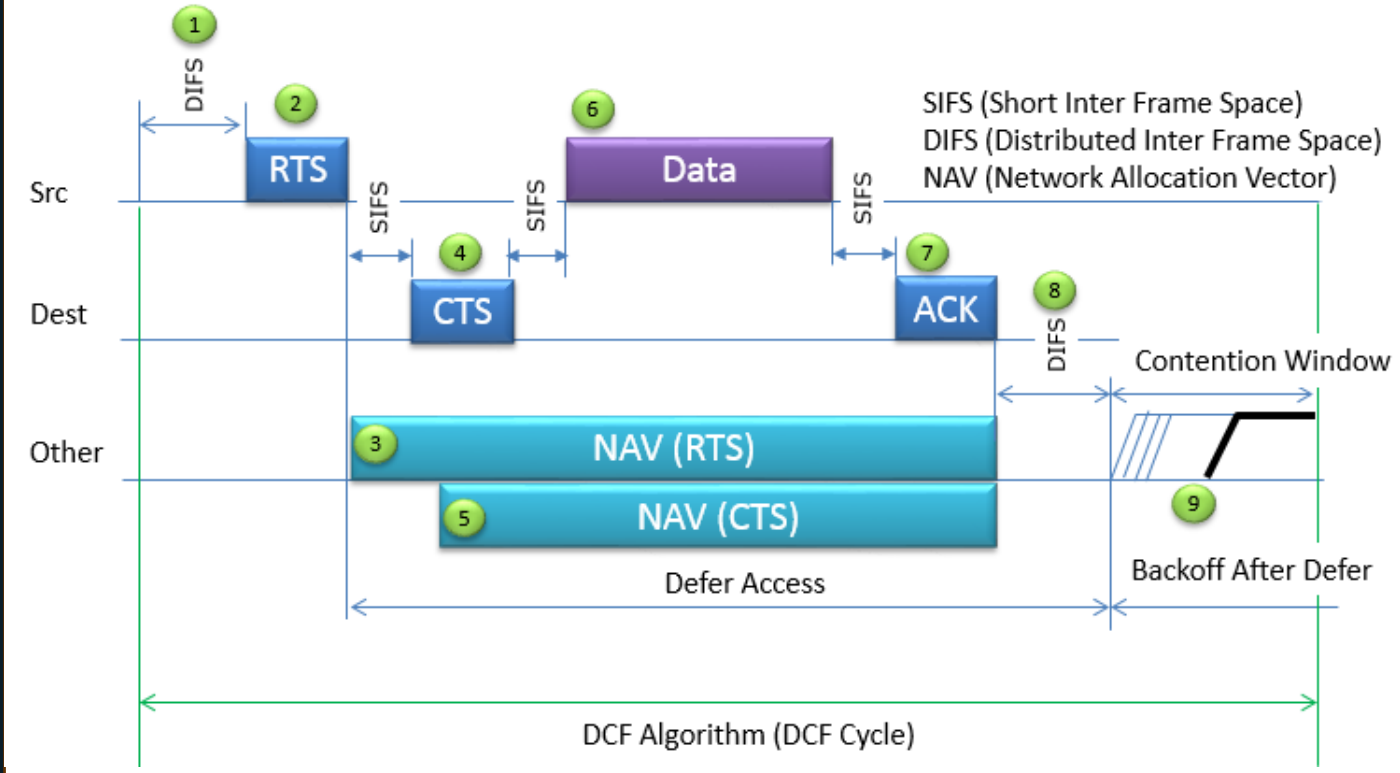


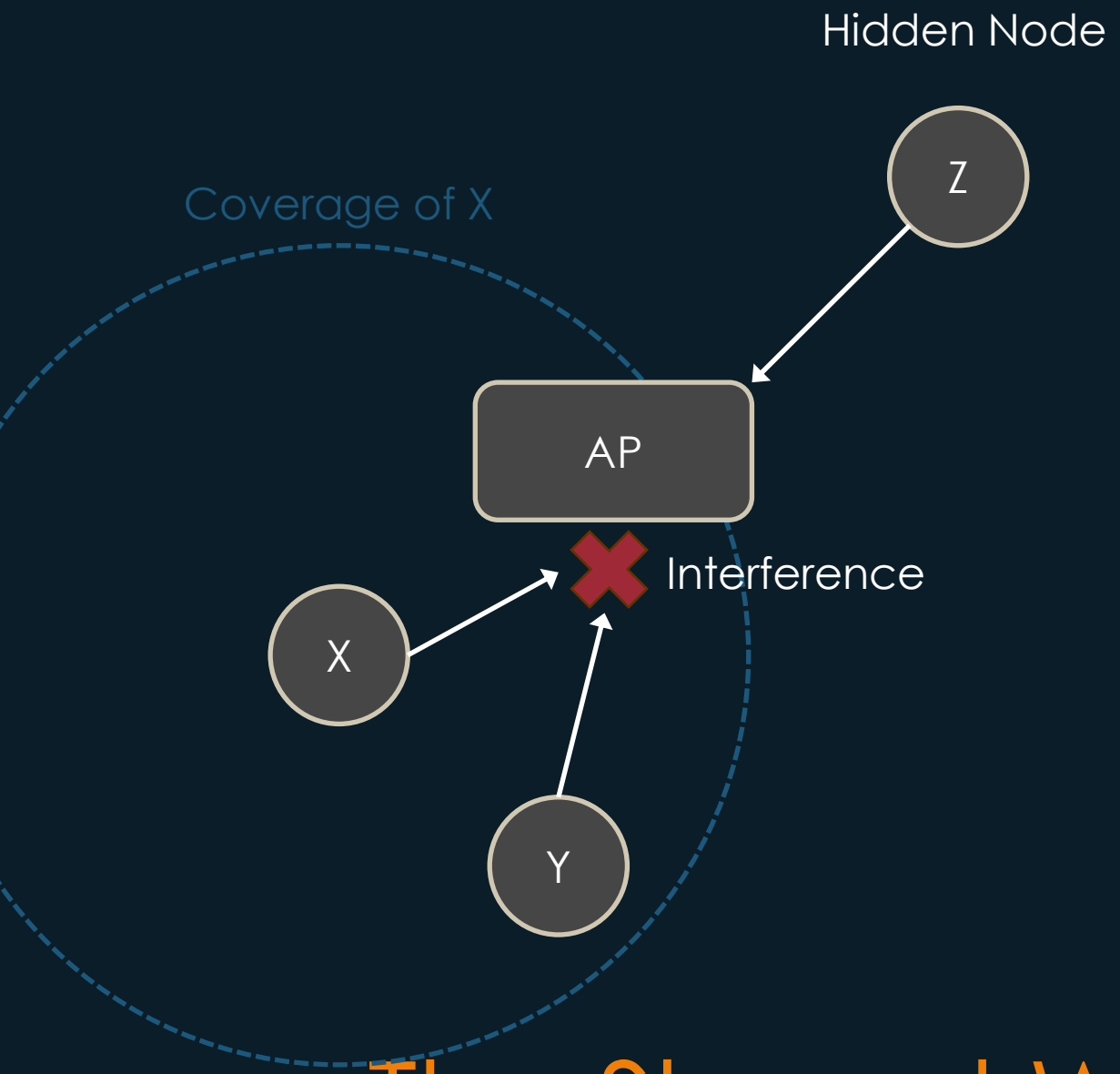
- Procedure for STA to join BSS
- Involves (Re)association request and response frame
- AP assigns Association ID (AID) to each STA in BSS
- DS updated to keep track of BSSs and their associated STAs
- Reassociation Request used when roaming to another BSS
  - New AP contacts old AP to finish reassociation and send response
  - Another AID assigned in new BSS

Association Procedure

Medium Access Method

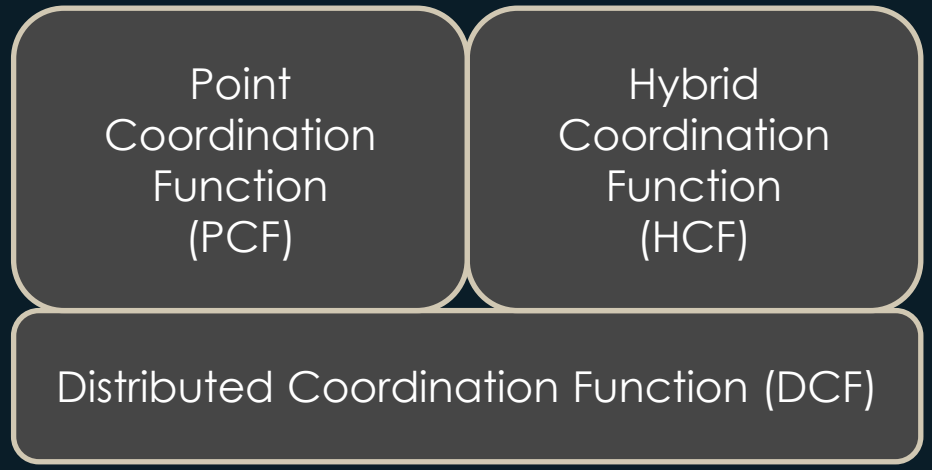
DCF, CSMA/CA, Interframe Space





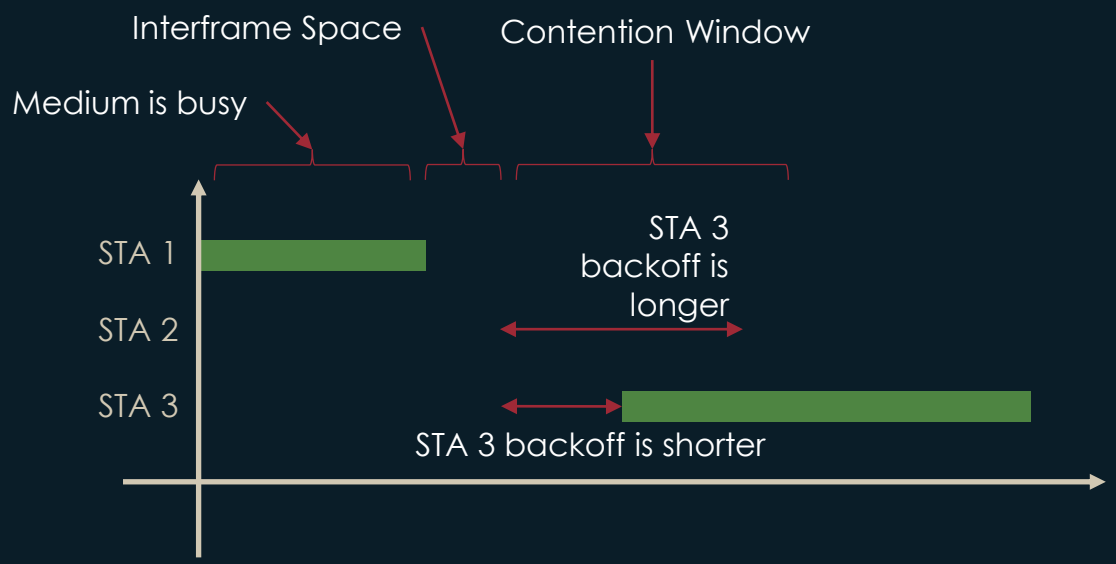
- Simultaneous transmission on the same channel (i.e., frequency) causes interference
  - Must be half-duplex
- Hidden node problem
  - Not all STAs in a BSS are in range of each other's transmissions
- Require some Medium Access Control
  - i.e., mechanisms to coordinate STAs on medium

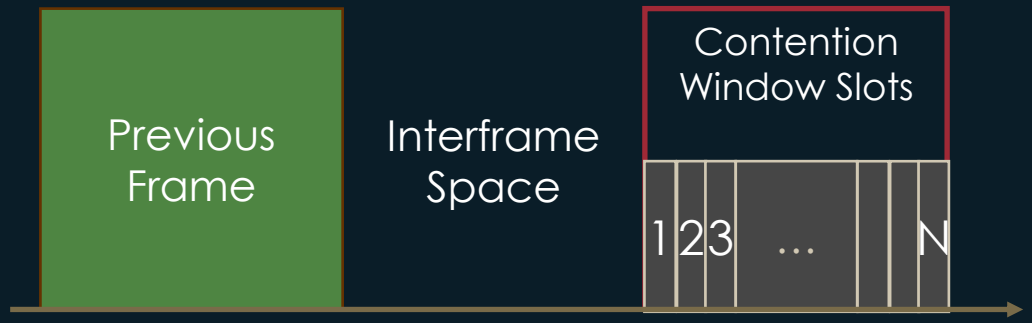
The Shared Wireless Medium



- Distributed Coordination Function (DCF)
  - Medium Access Control (MAC) technique used in 802.11
- Is distributed
  - No central node to coordinate access
  - STAs coordinated cooperatively
- Other MAC techniques (e.g., PCD and HCF) built on top of DCF
- Features
  - CSMA/CA multiple access method
  - Frame prioritization using interframe space
  - Virtual carrier sensing to save power

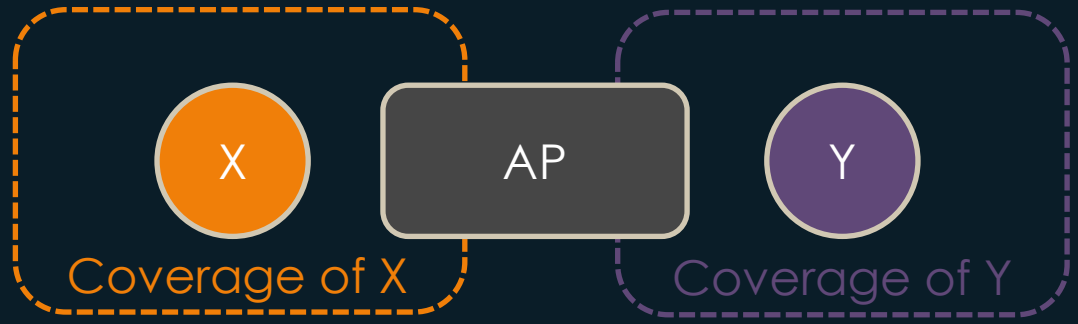
Distributed Coordination Function (DCF)

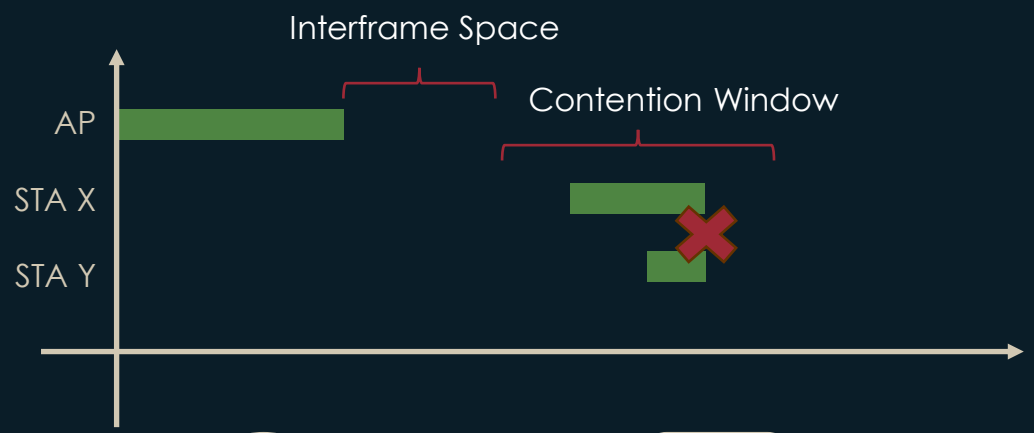


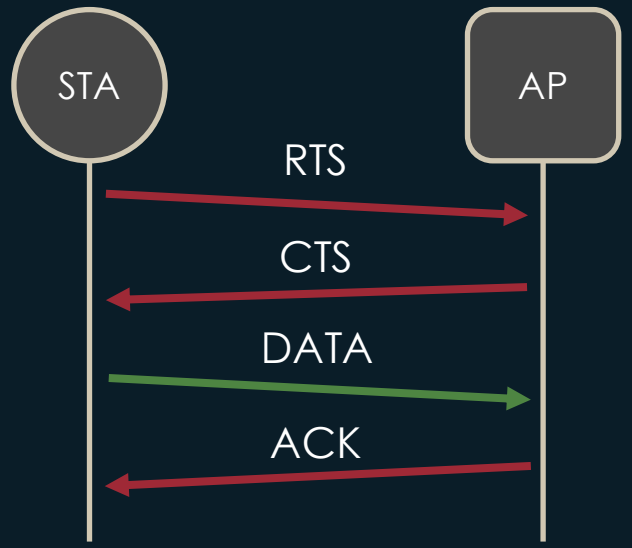


CSMA/CA

- Multiple Access Method is CSMA/CA
- Carrier Sense Multiple Access (CSMA)
  - Listen first, only transmit if medium is idle
- Collision Avoidance (CA)
  - Avoid collisions from simultaneous transmissions using random backoff time
- Contention Window
  - Contention window after interframe space for STAs to contest medium
  - Divided into N slots where N is a power of 2 minus 1 (e.g., 31, 63, 127)
  - STAs random backoff time is $R \times t_{slot}$ where R is a random integer

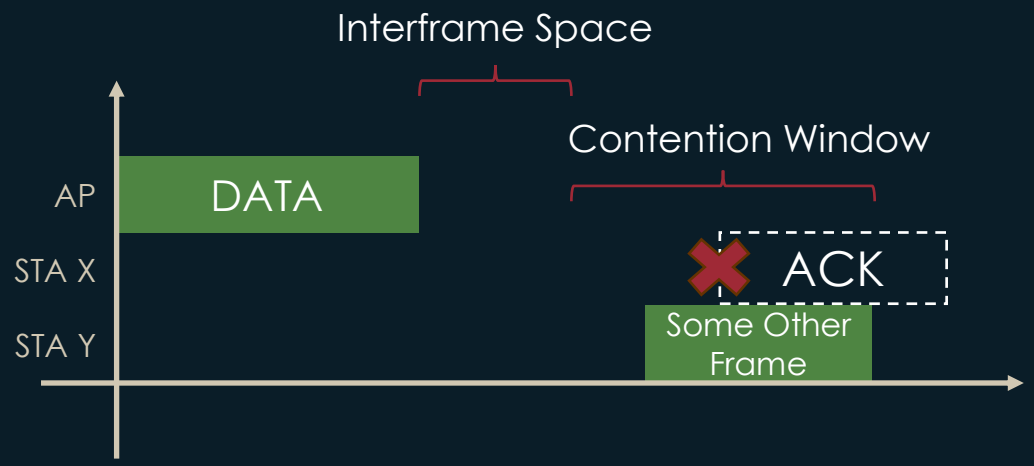


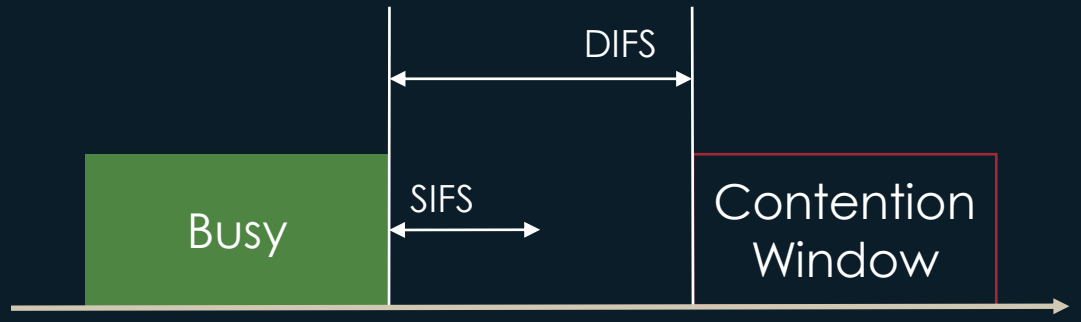




- Hidden node problem
  - Distant node may erroneously think medium is idle
- Transmitting nodes need confirmation of delivery
- Four-way frame exchange to workaround these issues
  - RTS, CTS, DATA, ACK
- Request/Clear To Send (RTS/CTS)
  - Mitigates hidden node problem
- Acknowledgement
  - Verifies successful delivery
- 4-way exchange deals with collisions, not prevent them

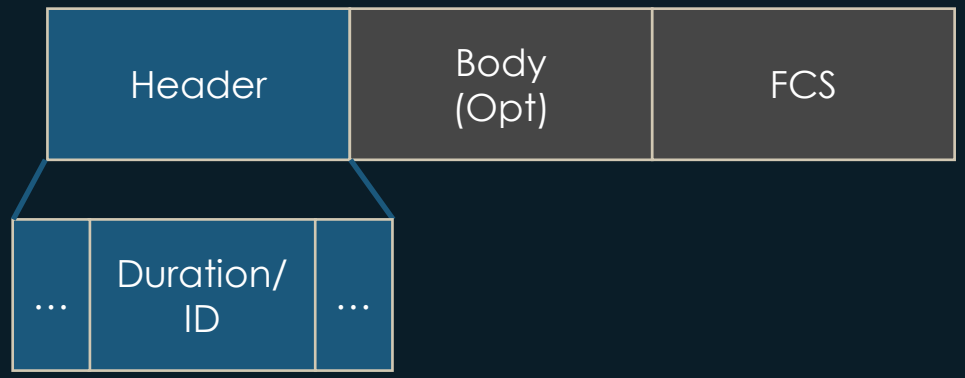
4-Way Frame Exchange

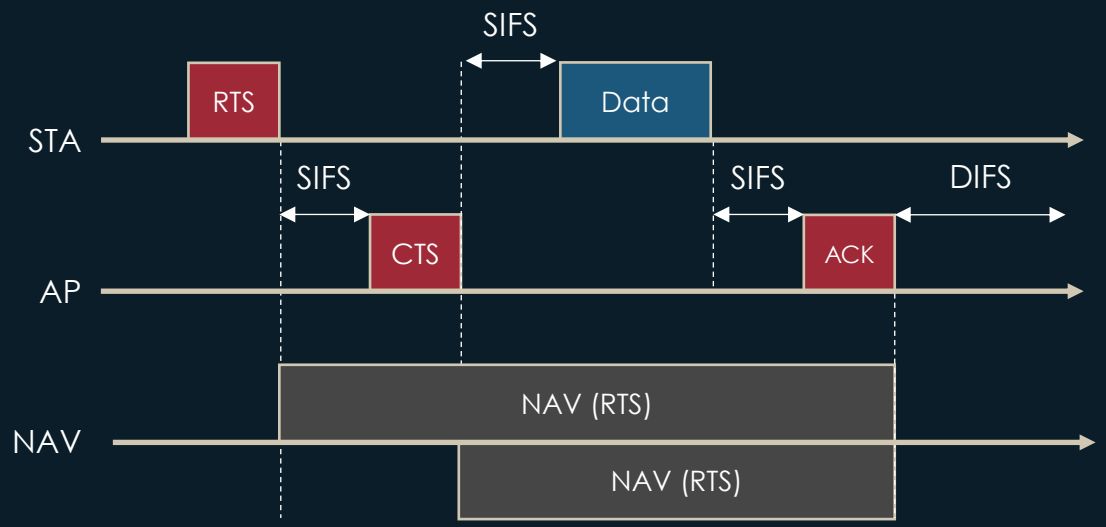




Interframe Spacing

- Must ensure frames in atomic operations get medium
  - e.g., 4-way frame exchange is not interrupted by an unrelated frame
- Need a way to prioritize different frame types
  - E.g., RTS/CTS/ACK frames should get priority
- Different types of interframe space
  - e.g., SIFS, PIFS, DIFS, EIFS
- Short Interframe Space (SIFS)
  - Shortest, thus highest priority
  - Used by CTS/ACK
- DCF Interframe Space (DIFS)
  - Lower priority
  - Minimum idle time for contention-based services (i.e., start of most atomic operations)



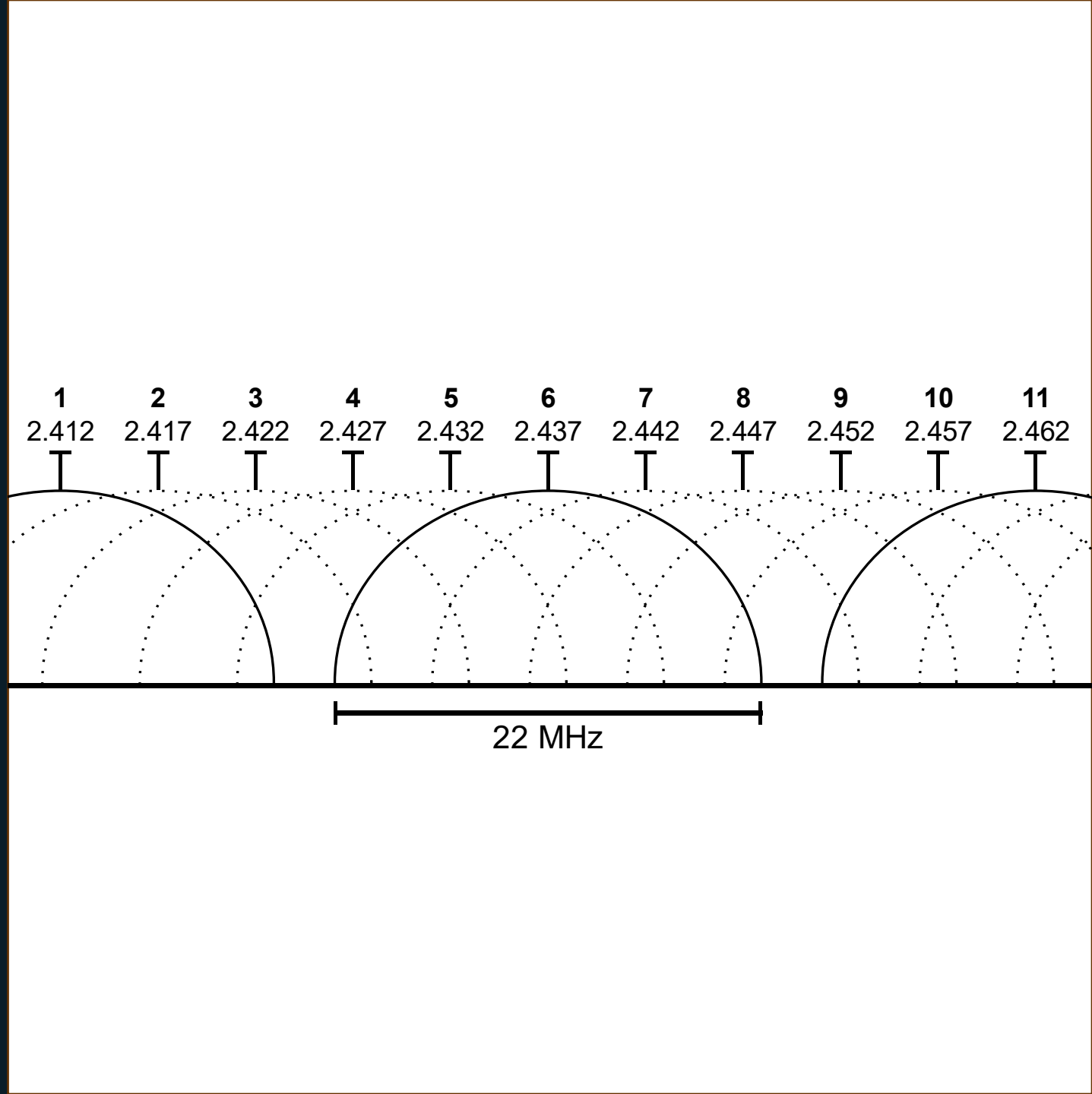


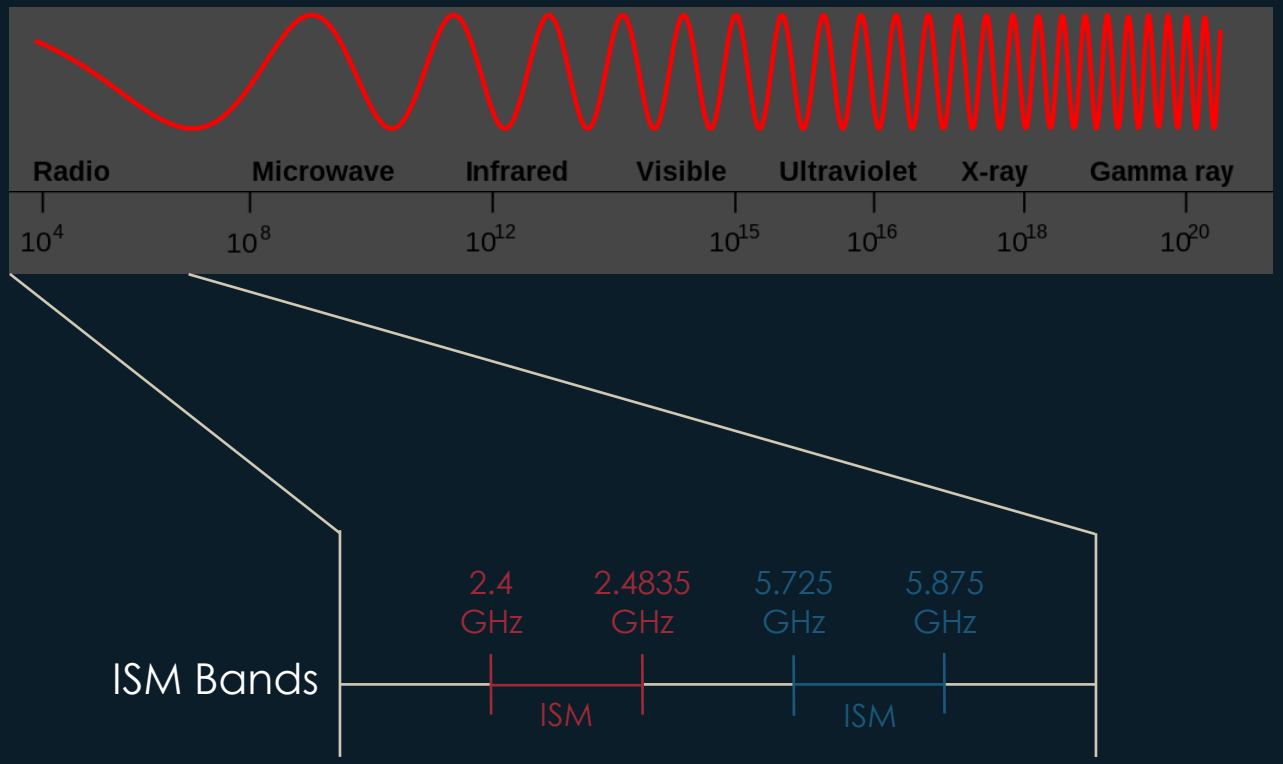
Carrier Sensing

- Physical Carrier Sensing
  - Listening to physical medium
  - Power hungry, need to keep RF components powered
  - Hidden node problem
- Virtual Carrier Sensing
  - Track when medium is busy without physical sensing
- Network Allocation Vector (NAV)
  - Timer in each STA indicating time left until medium is idle
- Working Principal
  - Duration/ID" field in frame header indicates remaining duration of frame exchange.
  - NAV updated by "Duration/ID" field
  - All STAs in range of AP, solves hidden node

Physical Layer

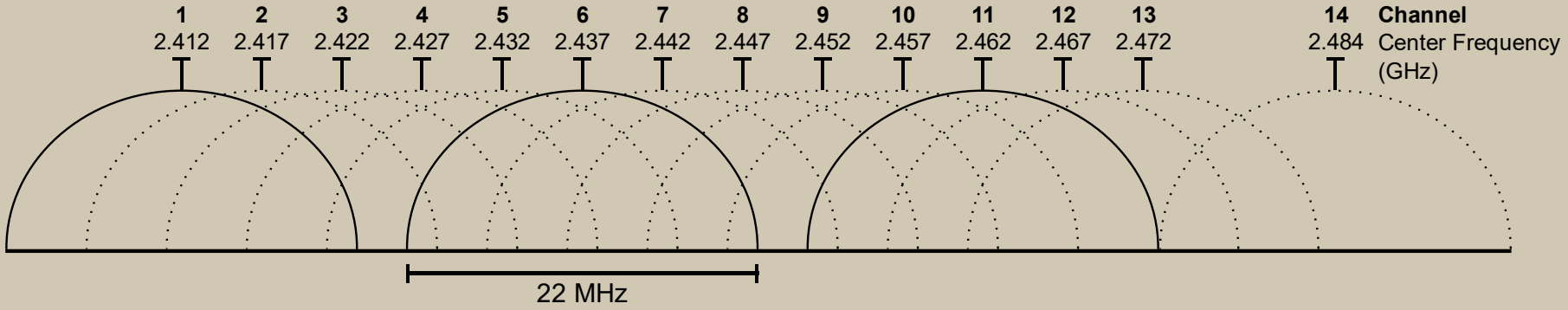
ISM Band, Channels

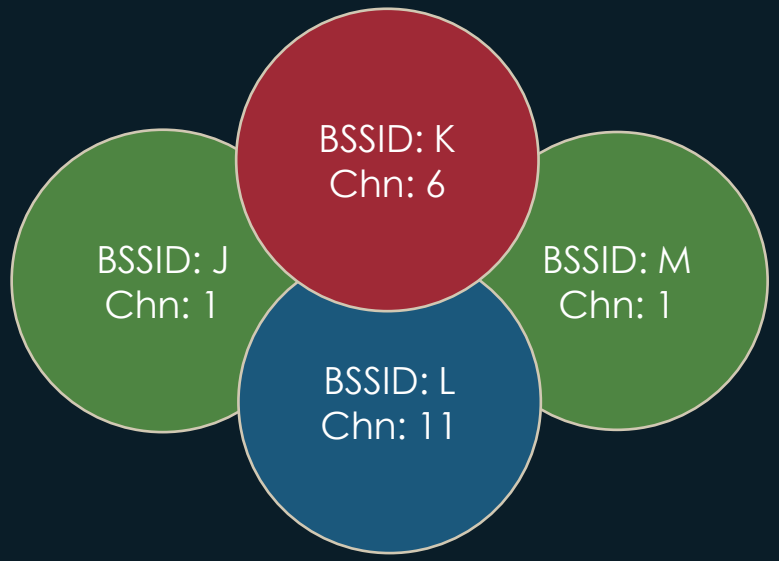




- Most wireless communication uses radio waves
- Radio spectrum is regulated and split into bands by ITU
- Industrial, Scientific, and Medical (ISM) band
  - License free band of radio frequencies
- Wi-Fi uses ISM bands of radio spectrum
  - 2.4 GHz to 2.4835 GHz
  - 5.725 GHz to 5.875 GHz

ISM Band





Channels

- A channel is a frequency range
  - Center Frequency
  - Bandwidth (22 MHz)
  - Numbered 1 to 14
  - Overlapping
- STAs in a BSS use the same channel
- Channel selection
  - Non-Wi-Fi interference (e.g., Microwave oven, Bluetooth)
  - Adjacent Channel Interference from neighboring BSS

Further Topics

- Topology
  - IBSS, MBSS
- MAC Frames
  - Fragmenting
- Security (WEP, WPA)
- Power Saving
  - PS-Poll, TWT
- Modulation Schemes
  - DSSS, OFDM, OFDMA, QAM

Resources

- Slides
  - https://github.com/Dazza0/wifi-crash-course
- “802.11 Wireless Networks: The Definitive Guide”
  - Matthew Gast
- CWNA Certified Wireless Network Administrator Study Guide
  - David D. Coleman & David A. Westcott

Thanks For Watching !