Standards & Protocols

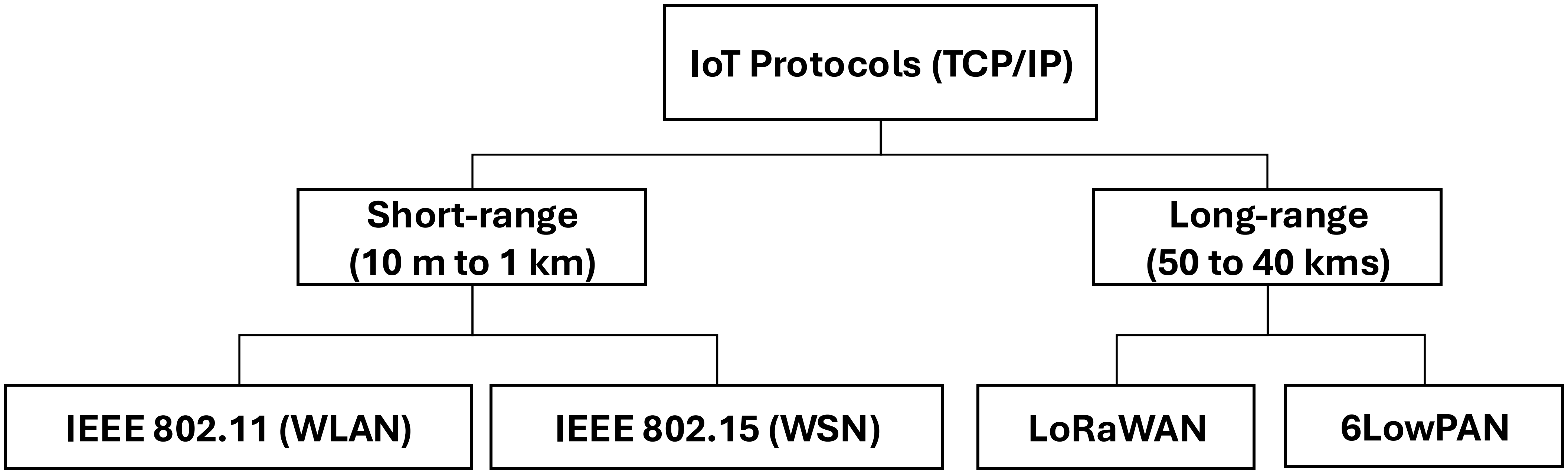
MODULE 2

Overview

- IEEE 802.11
- IEEE 802.15.4
- LoRaWAN
- 6LowPAN
- Application Protocols

Introduction

- **Protocols** - set of **precise and unambiguous rules** that enable seamless communication between different devices in IoT networks.



IEEE Standards

- **IEEE (Institute of Electrical and Electronics Engineers)**
- Global standards organization responsible for developing technical standards in various fields
  - Telecommunications,
  - Information Technology, and
  - Electronics.
- 802 series of IEEE standards:
  - Local Area Networks (LANs),
  - Metropolitan Area Networks (MANs), and
  - Wireless Networks.

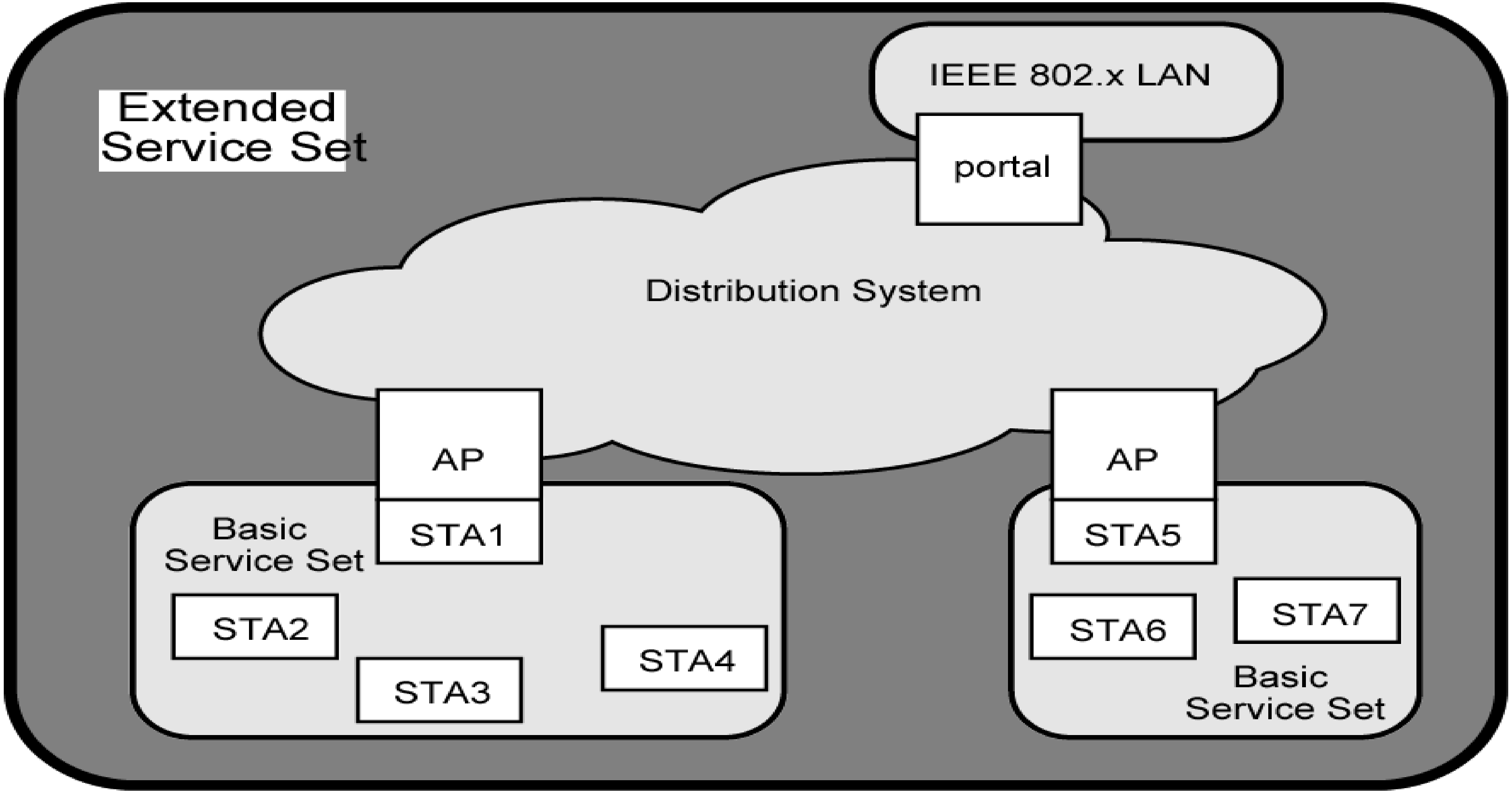
IEEE 802.11 (WLAN)

- IEEE 802.11 – **Physical & MAC layer** in OSI
- IEEE 802.11 family of standards, commonly known as **Wi-Fi**
- Adapted to meet the specific requirements of the Internet of Things (IoT)
- **IEEE 802.11ah**, also referred to as **Wi-Fi HaLow**
  - Facilitate **low-power, long-range wireless communication** suitable for **IoT applications**.

IEEE 802.11 Features

- Operates in the **900 MHz license-exempt band** - extended range compared to traditional Wi-Fi
  - operates at higher frequencies **(2.4 GHz, 5 GHz, and 6 GHz)**
- Capable of **covering distances exceeding 1 km**
- Low Power Consumption - **up to 10 years**
- Supports mechanisms like **sleep mode notifications to optimize energy usage**
- High Capacity - **8191 stations** to connect to a single **Access Point (AP)**
- Robust Communication - **Modulation and Coding Schemes (MCS)** and supports **Multiple-Input Multiple-Output (MIMO)** technology (4 x 4)

IEEE 802.11 Architecture



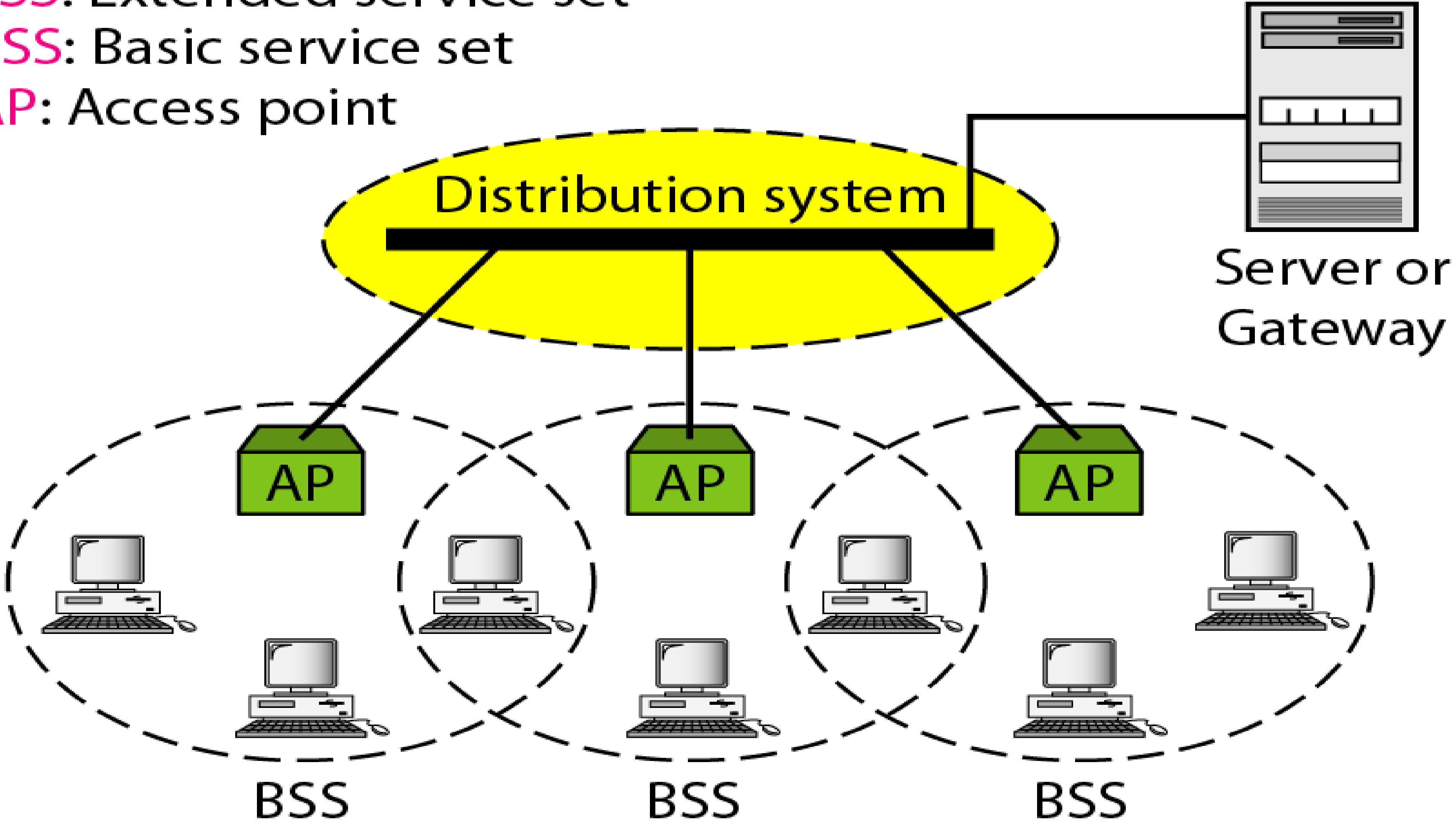
STA = station
AP = access point

IEEE 802.11 Architecture

- **Basic Service Set (BSS)**
  - consists of one or more wireless stations and a central device known as an Access Point (AP)
  - AP acts as a hub that facilitates communication between wireless devices and the wired network
- **Extended Service Set (ESS)**
  - ESS comprises multiple BSSs interconnected by a distribution system (DS)
  - Broader coverage and seamless roaming between different APs
- **Distribution System (DS)**
  - DS connects multiple APs within an ESS
  - Enables data transfer between different BSSs and linking wireless networks to wired networks
- **Independent Basic Service Set (IBSS)**
  - IBSS is a peer-to-peer network where stations communicate directly with each other without an AP

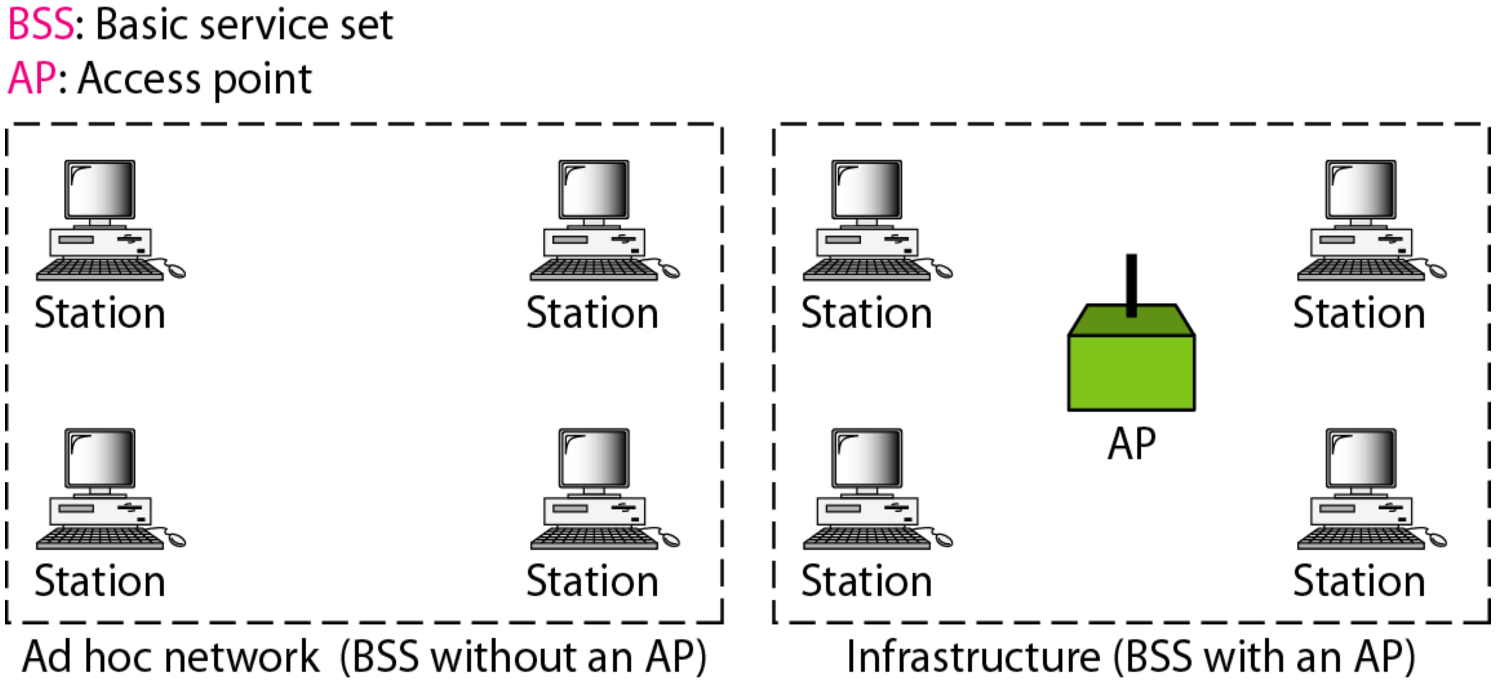
IEEE 802.11 Architecture

ESS: Extended service set
BSS: Basic service set
AP: Access point



Operating Modes

- **Infrastructure Mode: communication occurs through an AP**, which manages data traffic and provides access to wired resources
- **Ad-Hoc Mode: allows devices to connect directly to each other without using an AP**, suitable for temporary or small-scale networks



IEEE 802.11 Services

Service Number	Service Name	Service Provider	Used to Support
1	Association	Distribution System	MSDU delivery
2	Authentication	Station	LAN access and security
3	Deauthentication	Station	LAN access and security
4	Disassociation	Distribution System	MSDU delivery
5	Distribution	Distribution System	MSDU delivery
6	Integration	Distribution System	MSDU delivery
7	MSDU Delivery	Station	MSDU delivery
8	Privacy	Station	LAN access and security
9	Reassociation	Distribution System	MSDU delivery

IEEE 802.11 Services

- **Association**: This service allows a station to connect to an Access Point (AP) to gain access to the distribution system, enabling communication within the network.
- **Authentication**: Ensures that a device is authorized to access the network. It establishes a secure connection between the station and the AP.
- **De-authentication**: Terminates the authentication relationship between a station and an AP, effectively disconnecting the station from the network.
- **Disassociation**: Notifies the AP that a station is no longer associated with it, which can be initiated by the station or due to loss of connectivity.

IEEE 802.11 Services

- **Distribution**: Facilitates the transfer of data frames between different access points within the distribution system, allowing communication between stations in different Basic Service Sets (BSS).
- **Integration**: Enables communication between stations on an IEEE 802.11 WLAN and those on an integrated wired LAN, handling address translation and media conversion.
- **MSDU Delivery**: Manages the delivery of MAC Service Data Units (MSDUs) between stations, ensuring reliable communication across the network.
- **Privacy**: Provides encryption services for data transmitted over the wireless medium, enhancing security against unauthorized access and eavesdropping.
- **Reassociation**: Allows a station to change its association from one AP to another within the same Extended Service Set (ESS), enabling seamless roaming without losing connectivity

IEEE802.11 - Mobility Types

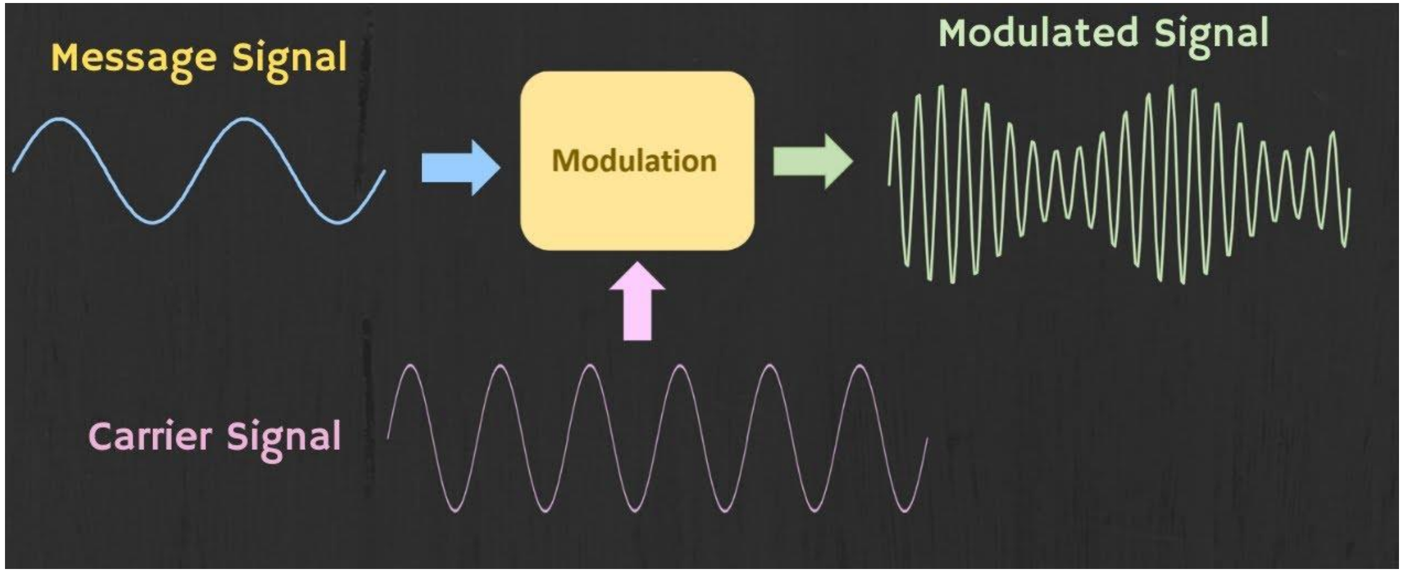
- **No-transition mobility** – either stationary or moving only inside a BSS
  - Ex: A user walking around their home while connected to a Wi-Fi router.
- **BSS-transition mobility** – can move from one BSS to another, but confined inside one ESS
  - Ex: A user with a laptop moves from one room (connected to AP1) to another room (connected to AP2) within the same office building, allowing them to stay connected while moving.
- **ESS-transition mobility** – can move from one ESS to another
  - Ex: A user leaves their workplace Wi-Fi network and connects to a public Wi-Fi hotspot at a café, requiring a new authentication process and possibly losing active connections.

IEEE802.11 - Modulation

- **Modulation** - process of varying one or more properties of a periodic waveform (signal) to encode information from a separate signal

- **Key Characteristics of Modulation**
  - **Modulating Signal**
    - The original information signal that contains the data to be transmitted (e.g., audio or video signals).
  - **Carrier Signal**
    - A steady waveform that carries the information. It typically has constant amplitude and frequency before modulation.

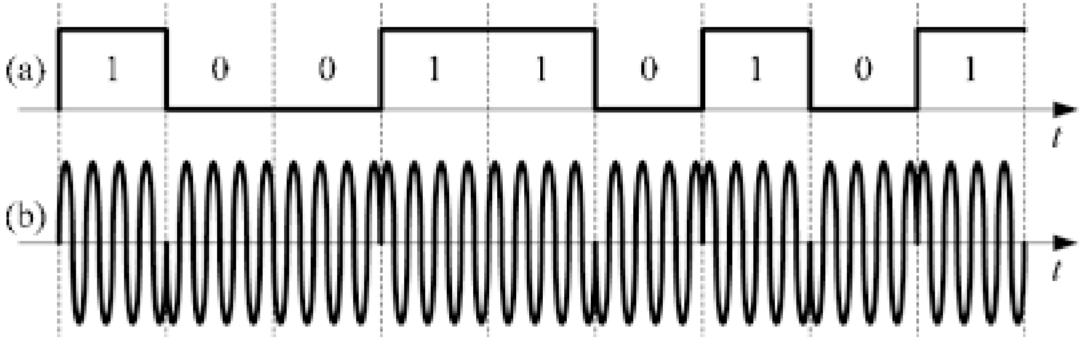
- **Types of Modulation:**
  - Amplitude Modulation (AM)
  - Frequency Modulation (FM)
  - Phase Modulation (PM)



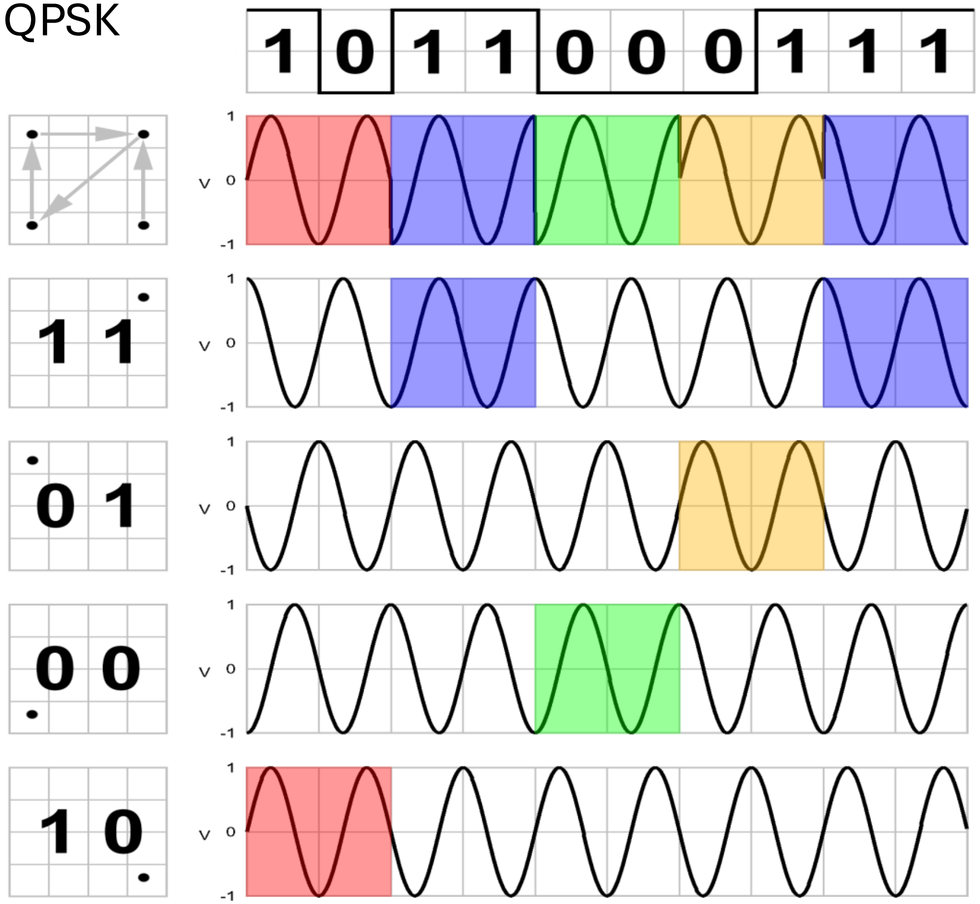
IEEE 802.11 - Modulation Techniques

Modulation Technique	Description	Key Features
BPSK (Binary Phase Shift Keying)	Encodes data by varying the phase of the carrier signal between two states (0 and 1).	Simple modulation, transmits 1 bit per symbol.
QPSK (Quadrature Phase Shift Keying)	Extends BPSK by using four phase states (00, 01, 10, 11).	Transmits 2 bits per symbol, higher data rate than BPSK.
16-QAM (Quadrature Amplitude Modulation)	Combines amplitude and phase modulation to transmit four bits per symbol.	Higher data rates, requires better signal-to-noise ratio compared to BPSK/QPSK.
64-QAM	Extends QAM to transmit six bits per symbol.	Very high data rates, demands excellent signal quality and higher signal-to-noise ratio.
OFDM (Orthogonal Frequency Division Multiplexing)	Splits a signal into multiple smaller sub-signals transmitted simultaneously at different frequencies.	Reduces interference, improves robustness against fading, widely used in modern communication systems.

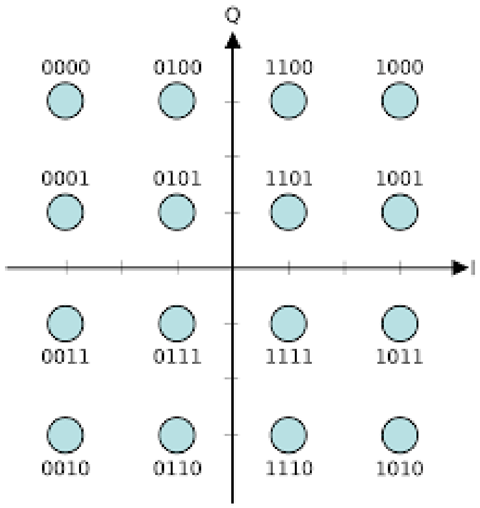
BPSK



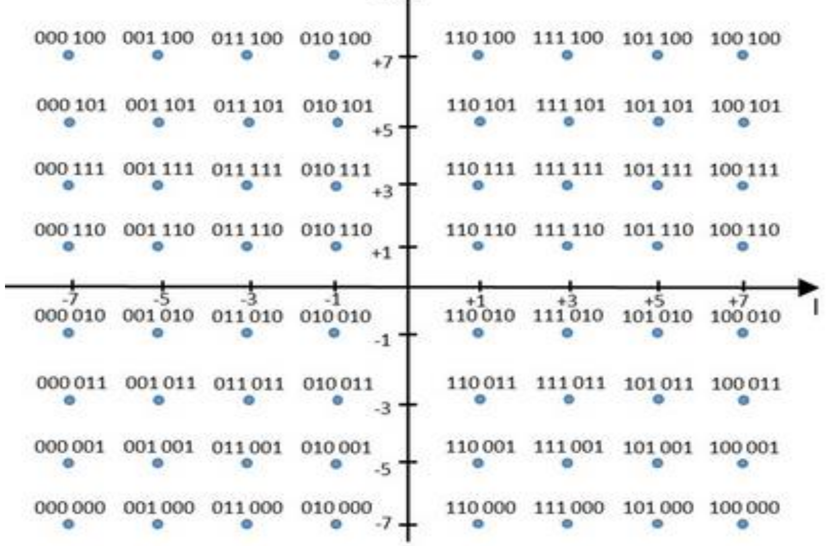
QPSK



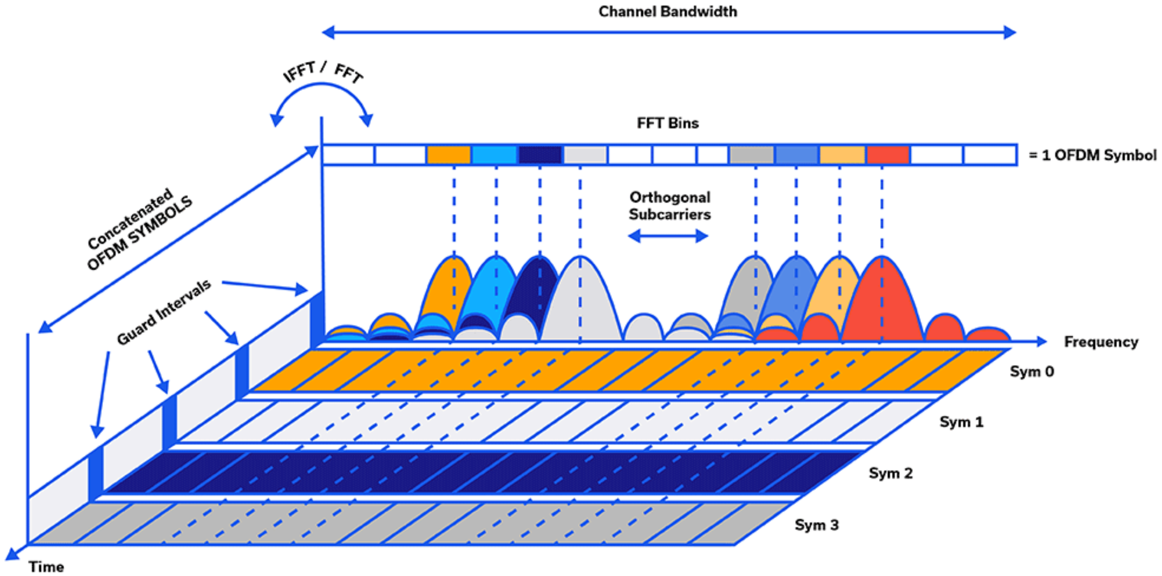
16 QAM



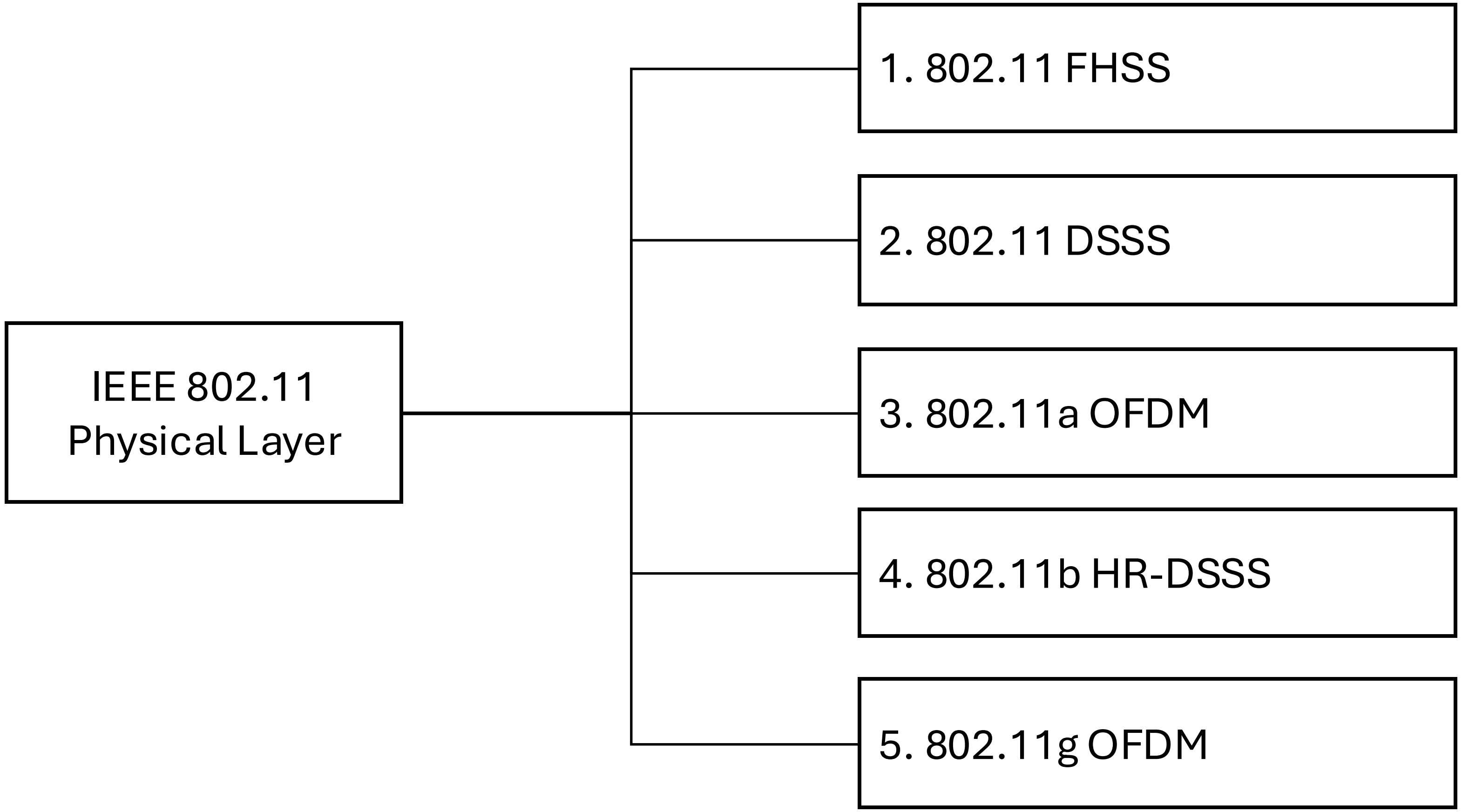
64 QAM



OFDM



IEEE 802.11 - Physical Layer Specifications



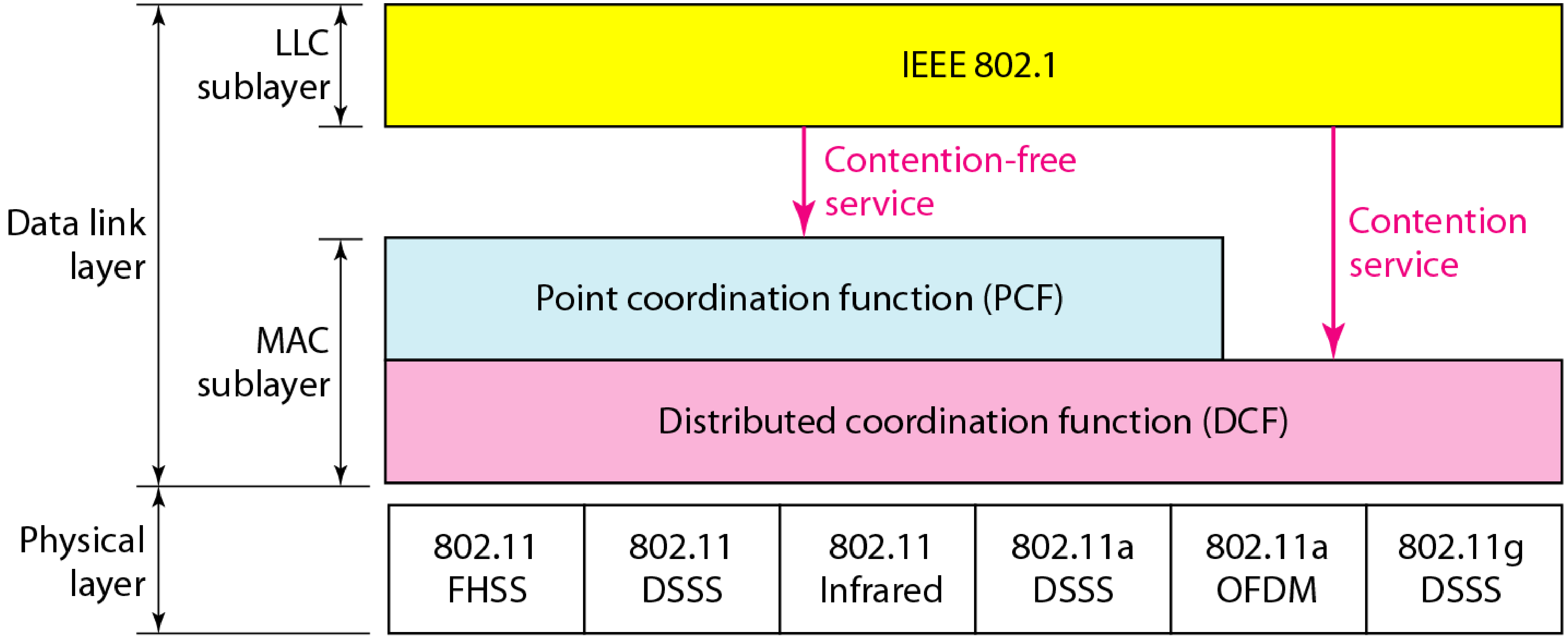
Specification	Modulation Technique	Frequency Band & Maximum Data Rate	Key Features
802.11 FHSS (BPSK)	Frequency Hopping Spread Spectrum **Spread the signal over multiple channels**	2.4 GHz Up to 2 Mbps	• Resilient to interference • Early standard
802.11 DSSS (BPSK)	Direct Sequence Spread Spectrum **Spreads the signal using a pseudo-random noise code** to enhance robustness	2.4 GHz 1 Mbps / 2 Mbps	• Robust against noise • Spreads signal over wider bandwidth
802.11a (QPSK)	Orthogonal Frequency Division Multiplexing (OFDM) **Divides the channel into multiple sub-carriers**, transmitting data simultaneously	5 GHz Up to 54 Mbps	• Better performance in high-density environments • Reduces multipath interference
802.11b (CCK)	High-Rate Direct Sequence Spread Spectrum (HR-DSSS)	2.4 GHz 1, 2, 5.5, and 11 Mbps	• Backward compatible with DSSS • Widely adopted
802.11g (QPSK, 16-QAM)	Orthogonal Frequency Division Multiplexing (OFDM)	2.4 GHz Up to 54 Mbps	• Combines features of 802.11a and 802.11b • Backward compatible with older standards

IEEE 802.11 - MAC Layer Specifications

- Key Functional Areas of the MAC Layer:

1. **Reliable Data Delivery**
    - Implements a frame exchange protocol where the source station transmits data and waits for an acknowledgment (ACK) from the destination.
    - If no ACK is received, the source retransmits the frame.
    - Utilizes a four-frame exchange process: Request to Send (RTS), Clear to Send (CTS), Data transmission & Acknowledgment (ACK)
2. **Access Control**
    - Employs both centralized and decentralized mechanisms to manage access to the wireless medium.
    - **Distributed Coordination Function (DCF):** A **mandatory access** method using **Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)**.
    - **Point Coordination Function (PCF):** An **optional method** for **time-sensitive transmissions**, using a **centralized polling mechanism**.
3. **Security**
    - Provides authentication and encryption services to ensure secure communication between devices.

IEEE 802.11 - MAC Layer Specifications



Feature	Distributed Coordination Function (DCF)	Point Coordination Function (PCF)
Overview	Mandatory MAC access method	Optional MAC access method
Access Method	Contention-based (CSMA/CA)	Centralized polling mechanism
Service Type	Asynchronous data service	Asynchronous and time-bounded service
Mechanism	- Device senses the medium before transmitting. - Waits for a clear channel. - Uses ACK for successful delivery.	- Access Point polls stations for transmission permission. - Grants time slots for data transmission.
Deployment	Used in both Infrastructure BSS and Independent BSS configurations	Primarily used in Infrastructure BSS only
Suitability	General data transmission	Time-sensitive applications (e.g., VoIP, video conferencing)
Features	- Resilient to collisions - Simple and flexible - Suitable for variable traffic loads	- Provides guaranteed bandwidth and latency - Reduces contention among devices

Medium Access Control Sublayer – DCF

- DCF protocol uses **CSMA** as access protocol.
- If station has frame to transmit, it listens to medium
- If medium idle, station may transmit
- Otherwise must wait until current transmission complete
- No collision detection
  - Not practical on wireless network
  - Dynamic range of signals very large
  - Transmitting station cannot distinguish incoming weak signals from noise and effects of own transmission
- DCF includes delays
    - Interframe space

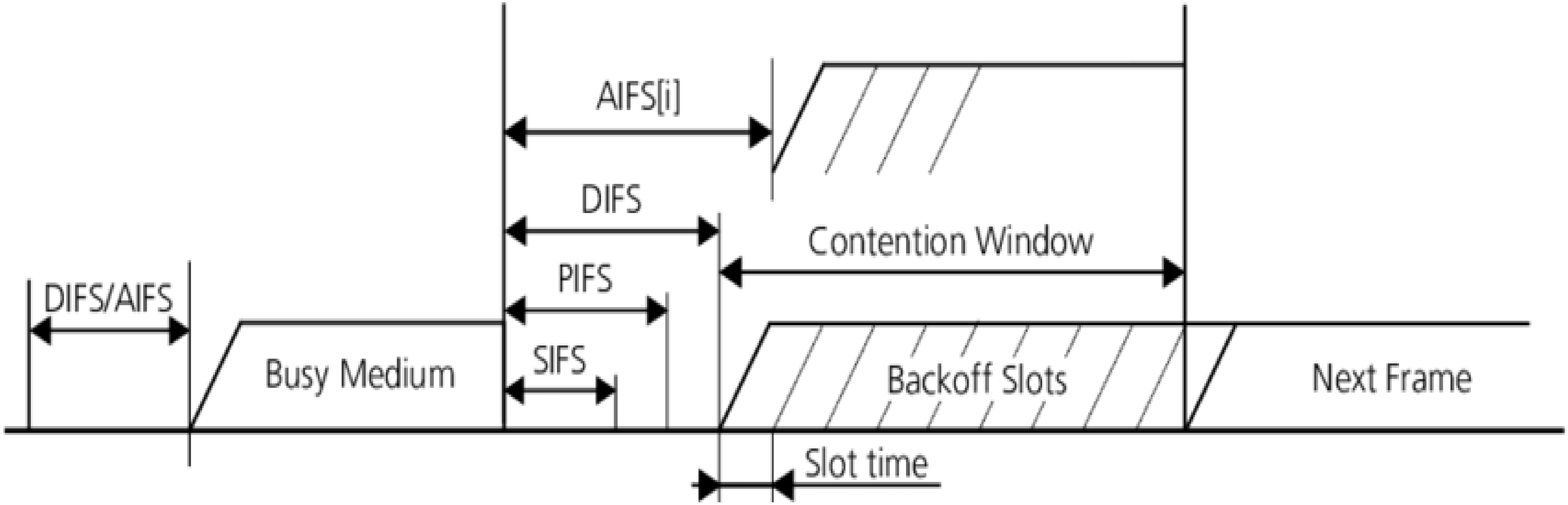
Medium Access Control Sublayer -Interframe Space

- Single delay known as interframe space (IFS)
- Using IFS, rules for CSMA:

1. Station with frame senses medium
2. If **busy station defers** (delays) transmission
    - Continue to monitor until current transmission is over
3. Once current transmission over, start another IFS
    - If remains idle, back off random time and again sense
    - If medium still idle, station may transmit
    - During backoff time, if becomes busy, backoff timer is halted and resumes when medium becomes idle

- To ensure stability, **binary exponential backoff** used

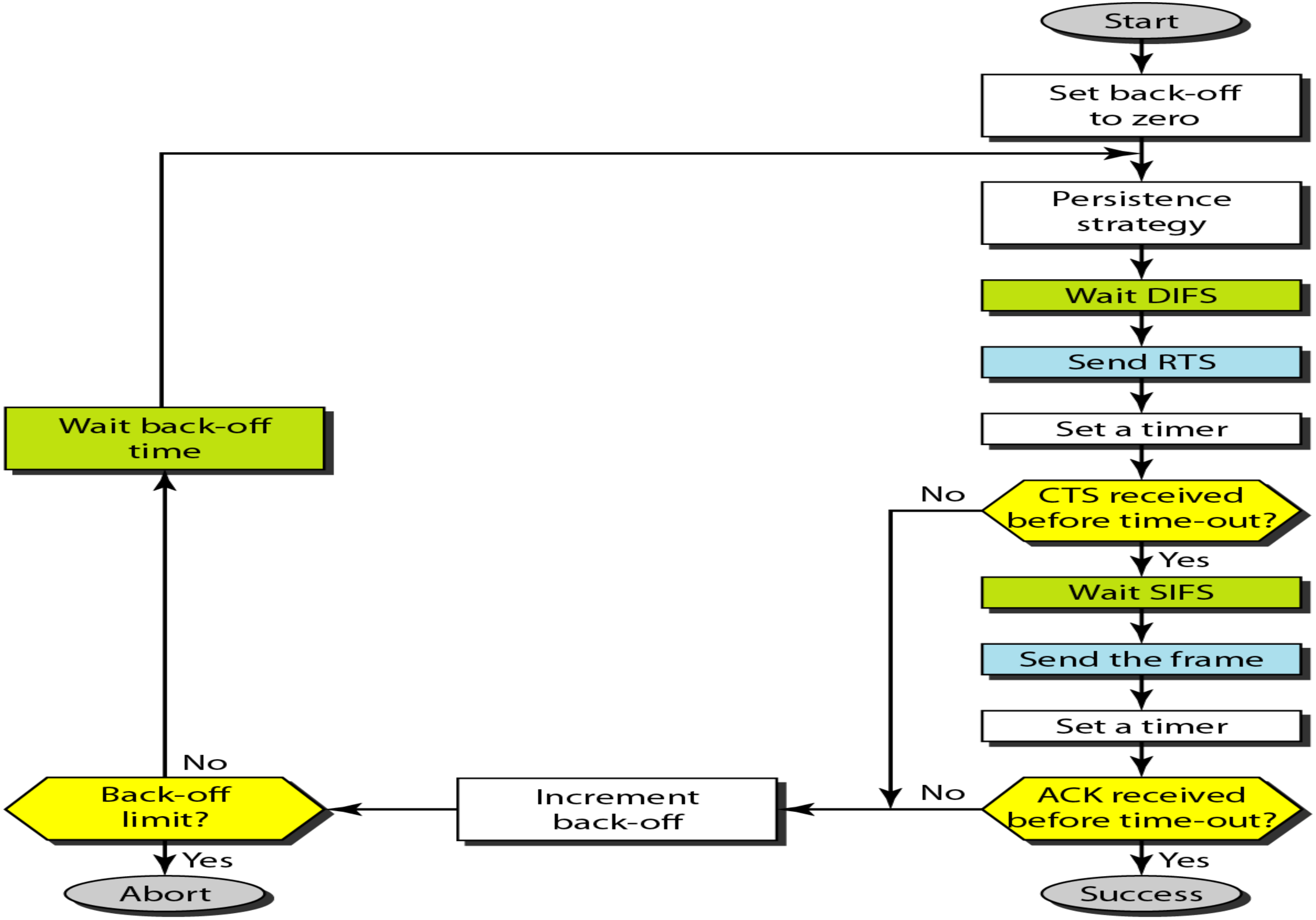
CSMA/CA – Inter Frame Space



- **SIFS (Short Inter-Frame Space)**
- **PIFS (Point Coordination Function Inter-Frame Space)**
- **DIFS (Distributed Coordination Function Inter-Frame Space)**
- **AIFS (Arbitration Inter-Frame Space)**

Shorter the frame space, shorter the distance

CSMA/CA


Start
Set back-off to zero
Persistence strategy
Wait DIFS
Send RTS
Set a timer
CTS received before time-out?
No
Yes
Wait SIFS
Send the frame
Set a timer
ACK received before time-out?
No
Yes
Success
Increment back-off
Back-off limit?
No
Yes
Abort
Wait back-off time

CSMA/CA – Key Steps

1. Carrier Sensing (Check if the Medium is Idle):

- The device (station) listens to the communication medium to check if it is idle (no ongoing transmission).
- If the medium is **busy**, the station waits for it to become idle before proceeding.

2. Inter-Frame Space (IFS) Waiting:

- After the medium becomes idle, the station waits for an appropriate inter-frame space (e.g., **DIFS**, **SIFS**, or **AIFS**) based on the type of traffic.
- The IFS ensures priority for certain frame types:
  - **SIFS**: Used for high-priority frames like ACKs.
  - **DIFS**: Used for standard data frames.

3. Backoff Mechanism:

- If multiple stations want to access the medium, each station enters a **contention phase**.
- A random **backoff timer** is selected within a specified **contention window**.
- The backoff timer is decremented in **time slots** only when the medium is idle. If the medium becomes busy during this time, the countdown pauses and resumes when the medium is idle again.

CSMA/CA – Key Steps

4. Transmission:

- The station whose backoff timer reaches **zero first** gains access to the medium and begins transmitting its data frame.

5. Acknowledgment (ACK):

- The receiver sends an acknowledgment (ACK) frame after a successful transmission. This ensures that the sender knows the data was received correctly.
- The ACK is sent after a **SIFS** period, giving it priority over other transmissions.

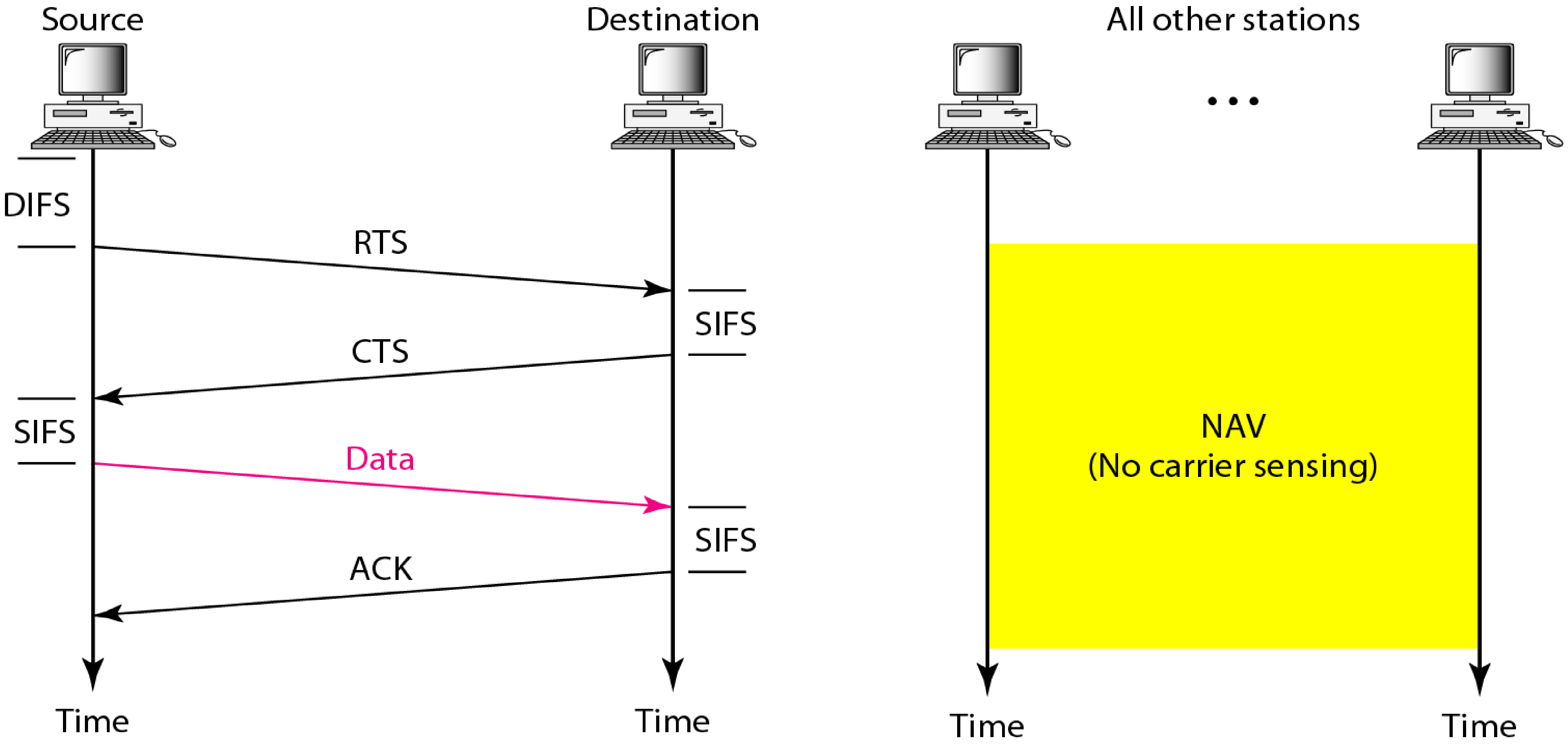
6. Collision Avoidance:

- If two stations select the same backoff timer, a collision can still occur.
- To minimize repeated collisions, the contention window is doubled (exponential backoff) for the retransmission attempt.

Network Allocation Vector (NAV)

- **Virtual timer** maintained **by each device** in a wireless network
- It **indicates the amount of time that the medium is reserved** for **another device's transmission**.
- During this time, **other devices refrain from attempting** to access the medium.

Network Allocation Vector (NAV)

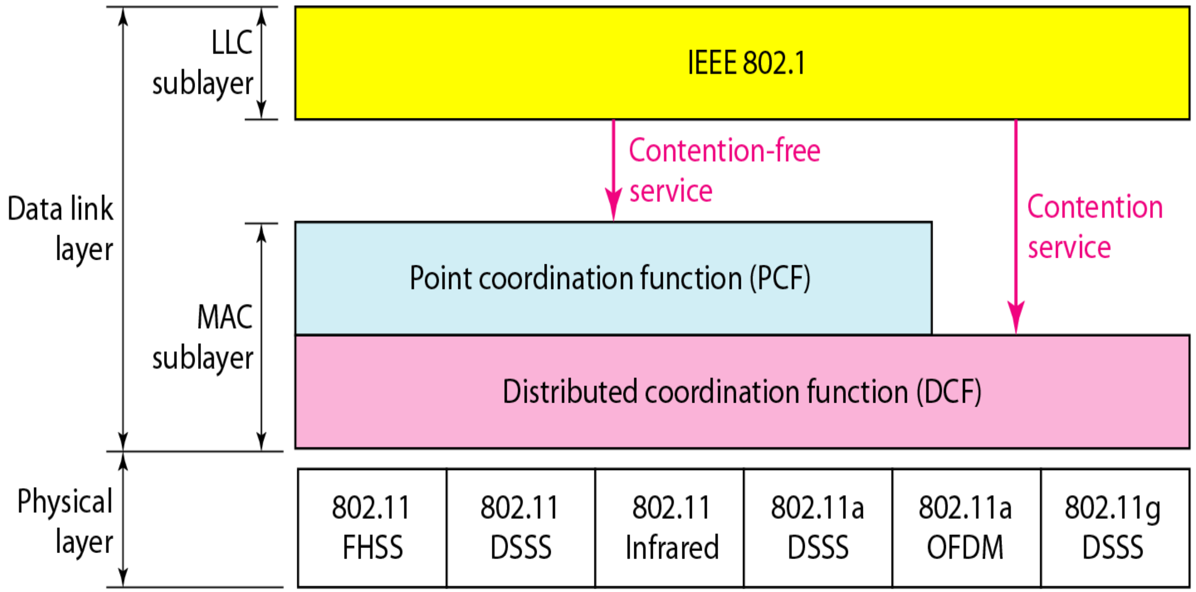


Network Allocation Vector (NAV)

1. **Transmission Reservation**:
   - When a device sends a frame (e.g., RTS, CTS, or DATA), it includes a **Duration Field** specifying how long the medium will be occupied for the ongoing transmission, including any acknowledgments.
2. **Setting NAV**:
   - Devices that overhear the frame update their NAV with the value in the Duration Field. This ensures that these devices do not attempt to access the medium for the specified duration.
3. **Waiting Period**:
   - While the NAV timer is running, the device assumes the medium is busy, even if it is idle physically (no carrier signal detected).
4. **Medium Access After NAV**:
   - Once the NAV timer expires, the device checks the physical medium. If idle, it proceeds with its own transmission after waiting the required inter-frame space (IFS).

Medium Access Control Sublayer - PCF

- Alternative access method implemented on top of DCF
- Implemented only in infrastructure n/ws (not in AD Hocs)
- Used in time sensitive transactions
- Has a **centralized contention free polling access method**
- **AP** performs polling of stations
- Uses PIFS (PCF IFS) when issuing polls
- Point coordinator polls in **round-robin** to stations configured for polling



PCF – Key Features

1. **Contention-Free Period (CFP)**:
   - Ensures that only polled stations communicate, avoiding medium contention.

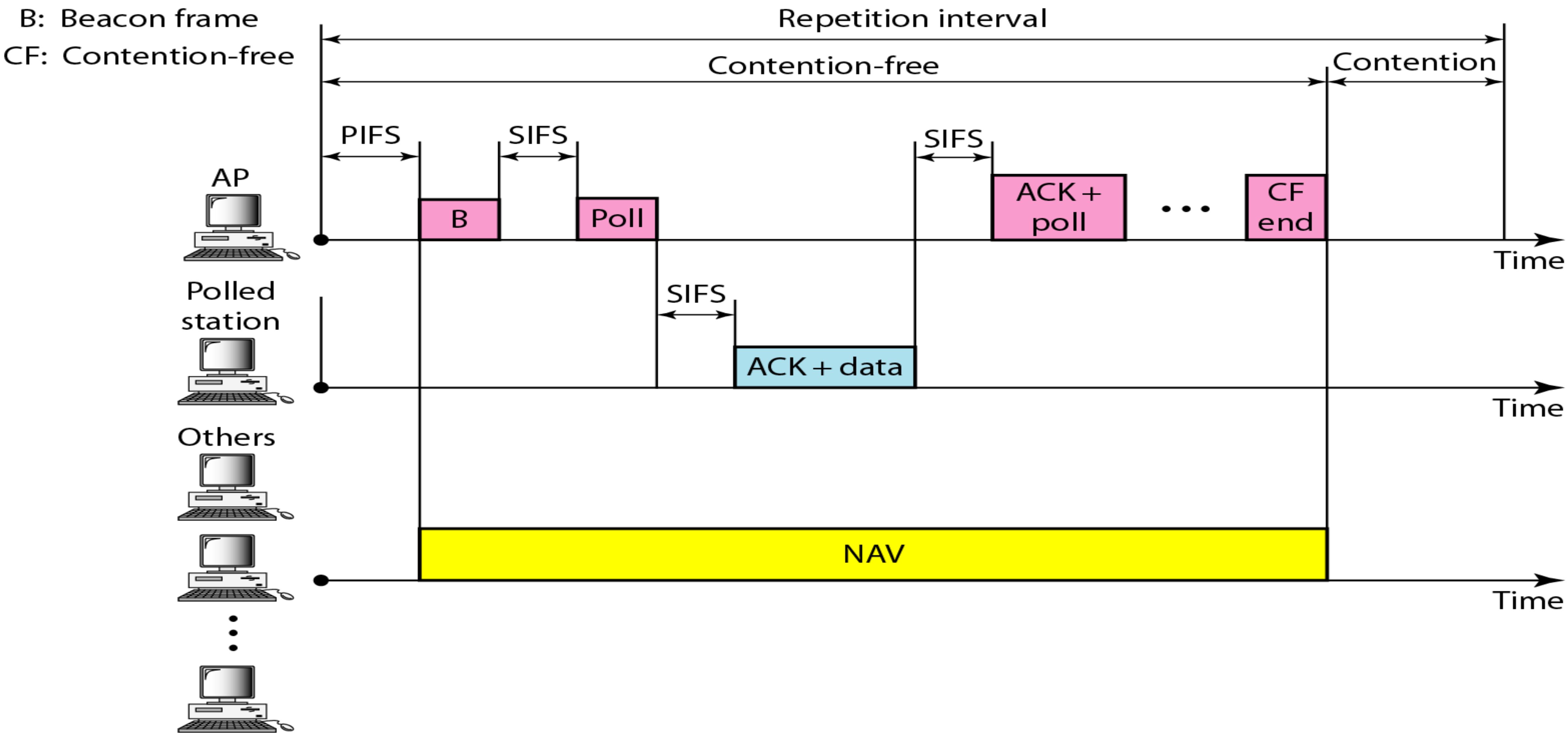
2. **Network Allocation Vector (NAV)**:
   - Other stations set their NAV to the duration of the CFP and refrain from accessing the medium.

3. **Integration with DCF**:
   - After the CFP, the medium reverts to contention-based access using DCF.

Medium Access Control Sublayer - Priority

- Use three values for IFS
- **SIFS (short IFS):**
  - Shortest IFS
  - For all immediate response actions
- **PIFS (point coordination function IFS):**
  - Mid-length IFS
  - Used by the centralized controller in PCF scheme when issuing polls
- **DIFS (distributed coordination function IFS):**
  - Longest IFS
  - Used as minimum delay for asynchronous frames contending for access

Medium Access Control Sublayer - PCF



Medium Access Control Sublayer - PCF

1. **Beacon Frame (B)**:
   - The Access Point (AP) begins the **Contention-Free Period (CFP)** by broadcasting a **Beacon Frame**.
   - The beacon contains information such as the duration of the CFP, allowing other stations to set their **Network Allocation Vector (NAV)**.
2. **Contention-Free Period (CFP)**:
   - A period where the AP controls the medium and prevents contention among stations.
   - Stations communicate only when polled by the AP.
3. **Polling**:
   - The AP sends a **Poll Frame** to a specific station, granting it permission to transmit.
   - The polled station can send its data during this time without competing for the medium.

Medium Access Control Sublayer - PCF

4. Acknowledgment and Data (ACK + Data):

- After sending data, the station can receive an acknowledgment (ACK) from the AP.
- The AP may include another Poll Frame along with the ACK to allow the next station to transmit.

5. CF End:

- The AP sends a **Contention-Free End Frame**, signaling the end of the CFP and the start of the **Contention Period (CP)**.

6. Contention Period (CP):

- After the CFP, stations use the Distributed Coordination Function (DCF) mechanism to contend for medium access, following the CSMA/CA protocol.

Medium Access Control Sublayer - PCF

7. Inter-Frame Spaces (IFS):

- **PIFS (Point Inter-Frame Space)**:
  - Used by the AP for high-priority access to the medium during the CFP.
- **SIFS (Short Inter-Frame Space)**:
  - Used for immediate responses, such as ACKs or polling responses, ensuring quick transmission without contention.

How the PCF Process Works?

1. **Start of Contention-Free Period**:
    - The AP broadcasts a beacon to initiate the CFP, reserving the medium for contention-free access.
    - Stations set their NAV to the duration of the CFP, ensuring they do not attempt to access the medium during this time.
2. **Polling Stations**:
    - The AP sequentially polls stations on its polling list.
    - Each polled station transmits its data and receives an ACK from the AP.
3. **Medium Access**:
    - Stations only transmit when polled by the AP, ensuring there are no collisions during the CFP.
4. **End of CFP**:
    - The AP sends a **CF End Frame**, releasing the medium for contention-based access.
5. **Contention Period (CP)**:
    - After the CFP, stations use DCF to access the medium through the CSMA/CA protocol.

PCF – Advantages & Limitations

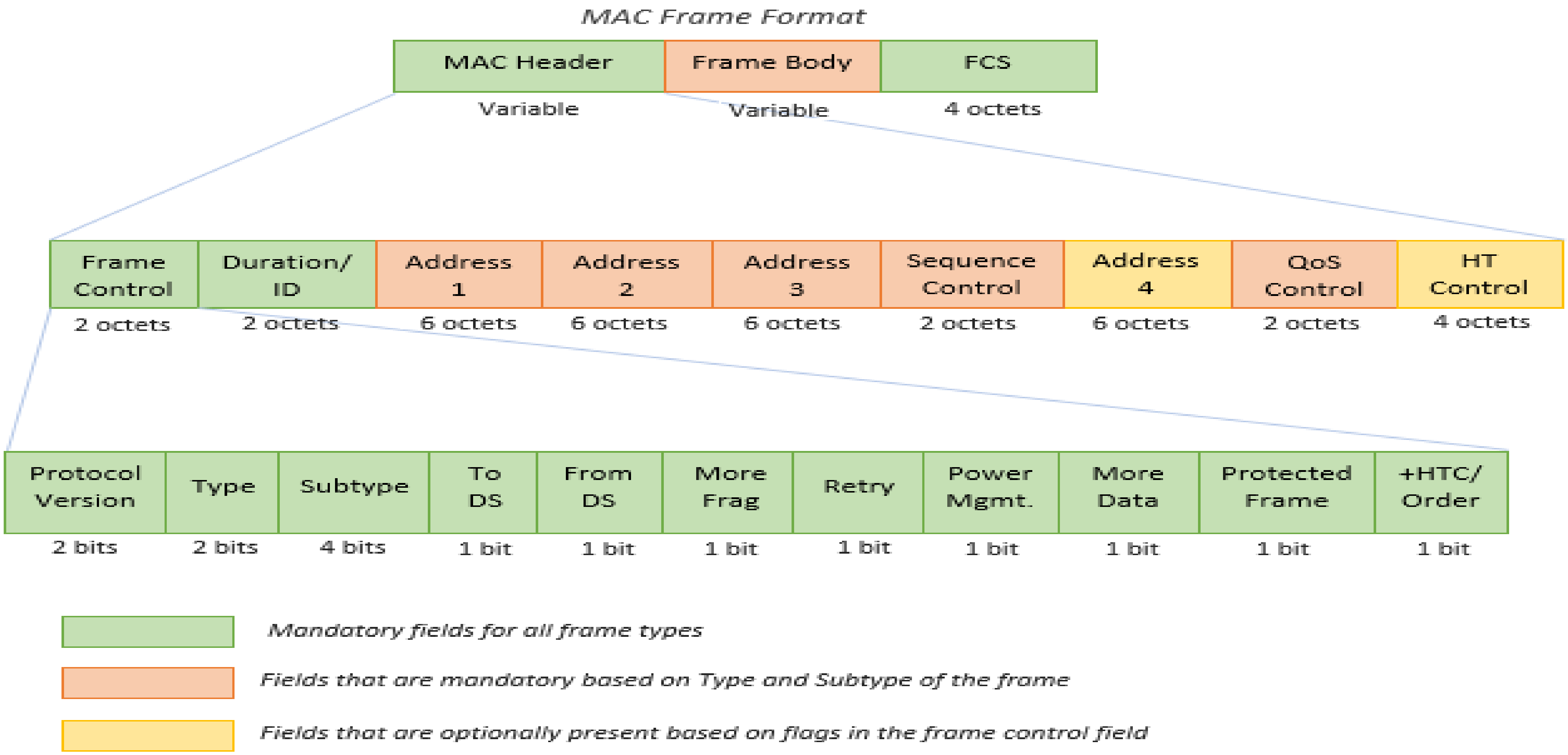
Advantages

1. **Deterministic Access**:
   - Guarantees medium access for polled stations, reducing delays for time-critical traffic.
2. **Collision-Free**:
   - Eliminates collisions during the CFP through centralized coordination.
3. **Real-Time Communication**:
   - Ensures smooth communication for applications requiring real-time data transfer.

Limitations

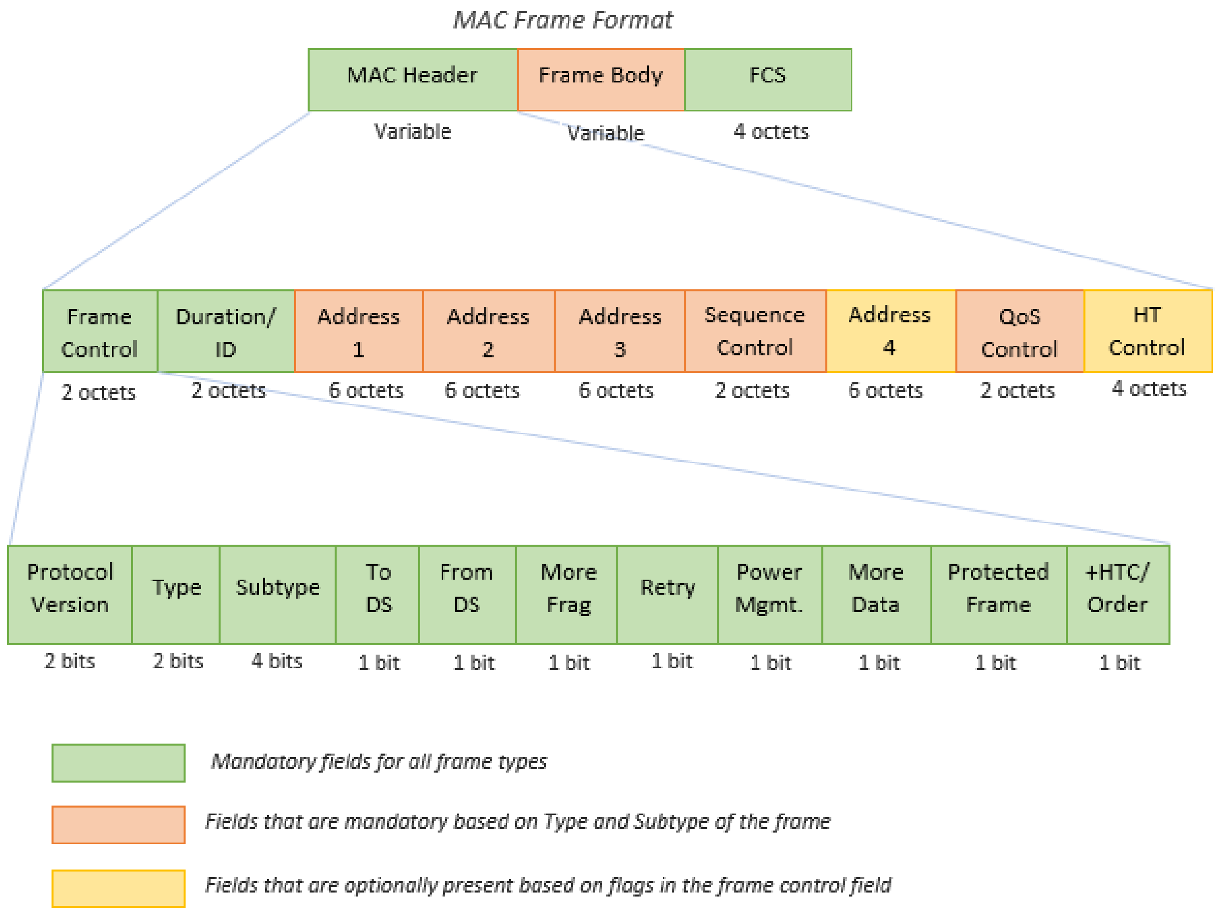
1. **Polling Overhead**:
   - The polling mechanism introduces additional latency and reduces efficiency for non-real-time traffic.
2. **Limited Scalability**:
   - As the number of stations increases, polling each station becomes time-consuming.

MAC Frame Fields



MAC Frame Fields

- **MAC Header:**
  - Contains control and addressing information.
  - Includes fields like **Frame Control**, **Duration/ID**, **Address Fields**, **Sequence Control**, **QoS Control**, and **HT Control**.
- **Frame Body:**
  - Variable in size, it carries the actual data or payload of the frame.
- **Frame Check Sequence (FCS):**
  - A 4-byte field used for error detection, ensuring the integrity of the transmitted frame.



MAC Fields – Frame Control

Frame Control (2 Octets):
- Contains critical control information about the frame.

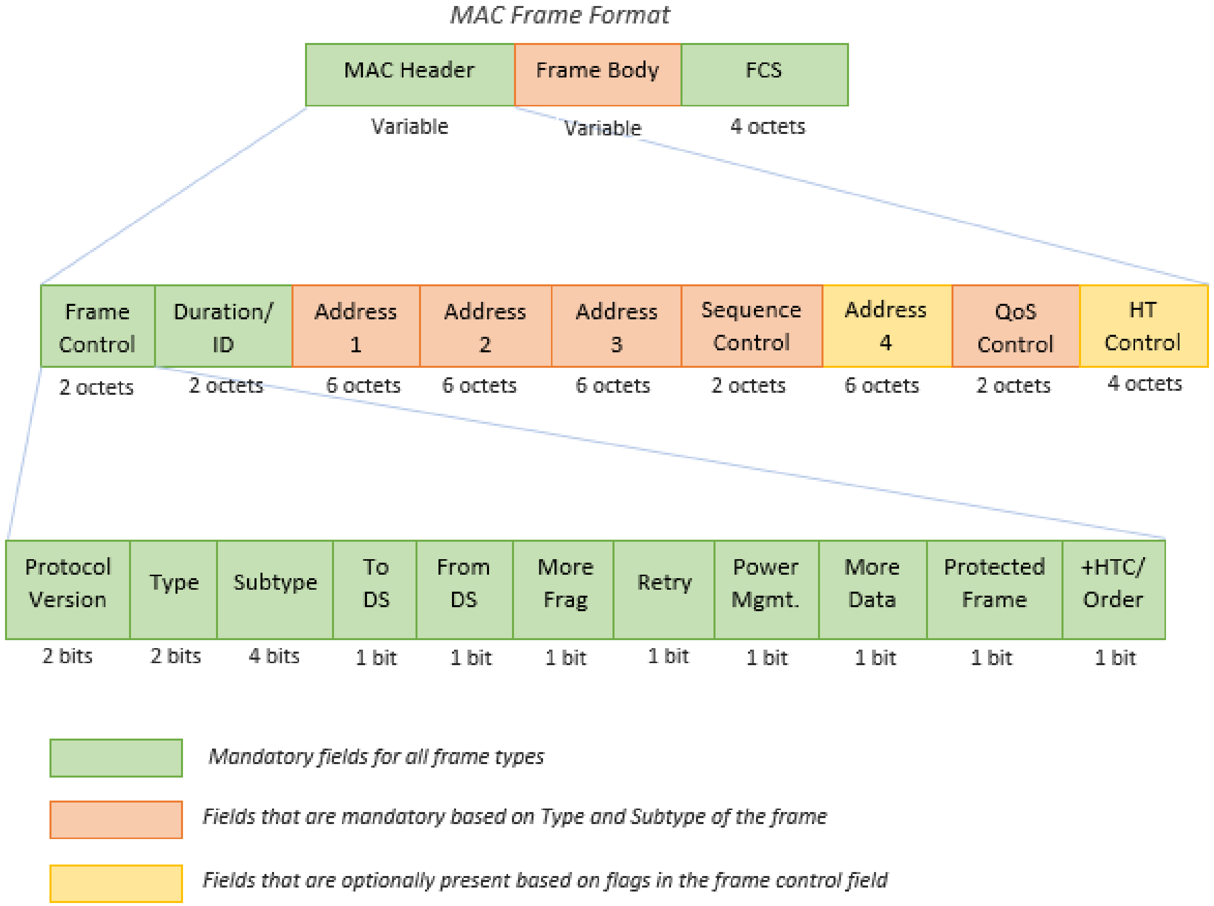
- Subfields:
  - **Protocol Version (2 bits)**:
    - Identifies the version of the 802.11 protocol being used.
  - **Type (2 bits)**:
    - Indicates the type of frame (Management, Control, Data).
  - **Subtype (4 bits)**:
    - Specifies the specific function of the frame (e.g., RTS, CTS, Beacon).
  - **To DS (1 bit) / From DS (1 bit)**:
    - Indicates whether the frame is going to or coming from the Distribution System.
  - **More Fragments (1 bit)**:
    - Indicates if the frame is fragmented.

- **Retry (1 bit)**:
  - Indicates if the frame is a retransmission.
- **Power Management (1 bit)**:
  - Shows if the device is in power-saving mode.
- **More Data (1 bit)**:
  - Indicates that more data frames are buffered for the same receiver.
- **Protected Frame (1 bit)**:
  - Specifies if the frame is encrypted.
- **+HTC/Order (1 bit)**:
  - Indicates if the frame contains High Throughput Control information.

MAC Fields – Duration

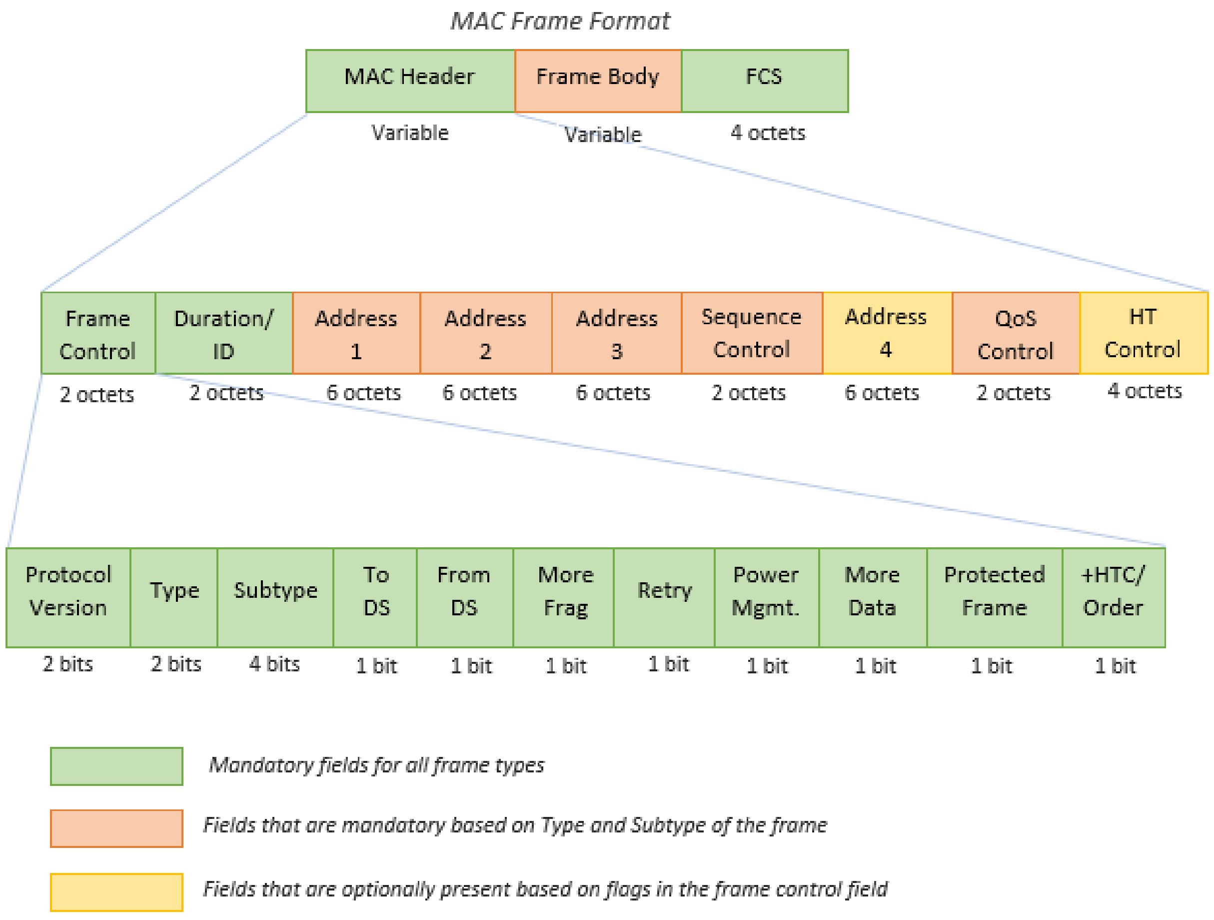
Duration/ID (2 Octets):

- **Duration**:
  - Specifies the time (in microseconds) the medium is reserved for this frame's transmission.
- **ID**:
  - Used in Power Save mode to indicate a station's association ID (AID).



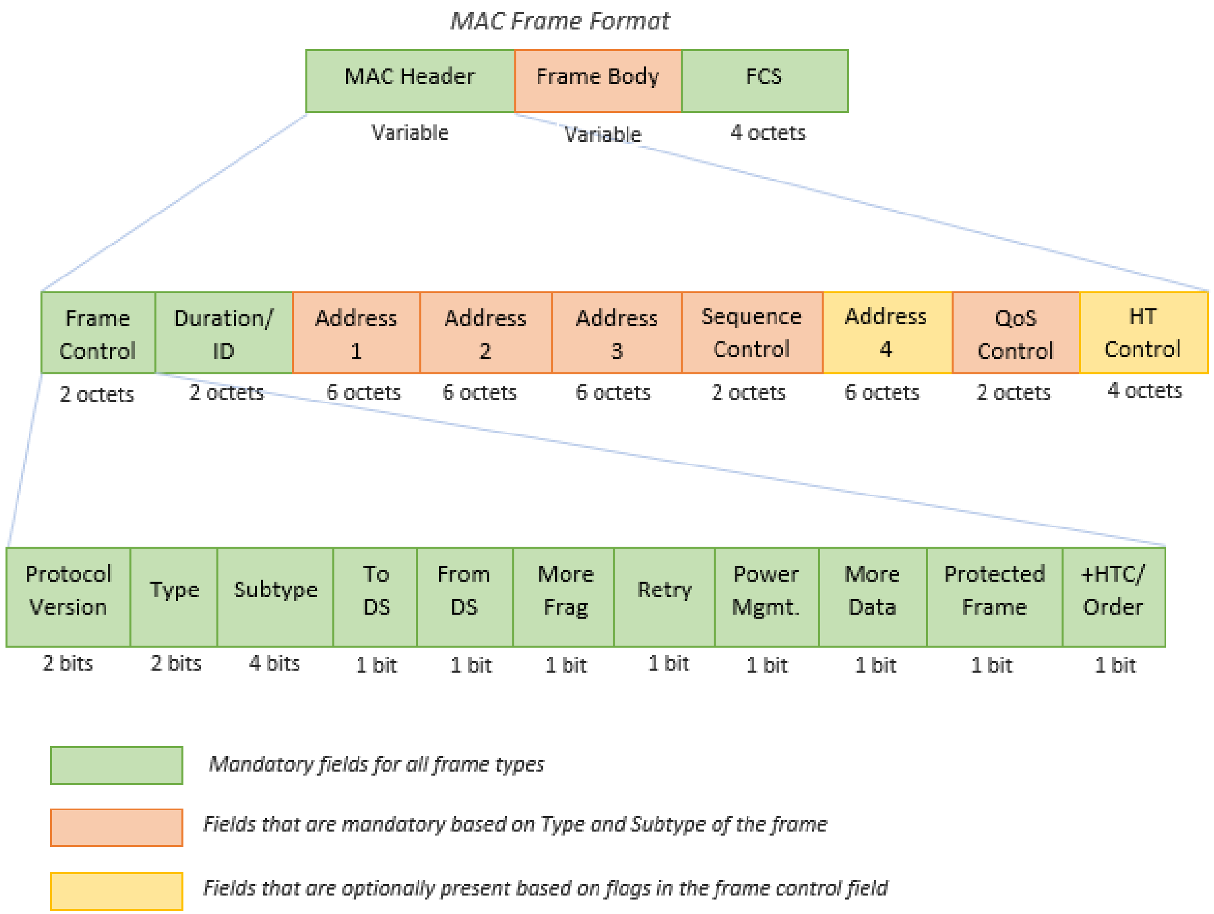
MAC Fields – Address Fields

- **Address Fields:**
- Each address field is 6 octets (48 bits) long, representing MAC addresses.
- **Address 1**:
  - Receiver's address.
- **Address 2**:
  - Transmitter's address.
- **Address 3**:
  - BSSID (Basic Service Set Identifier) in infrastructure networks.
- **Address 4**:
  - Used in Wireless Distribution System (WDS) to specify additional routing information.



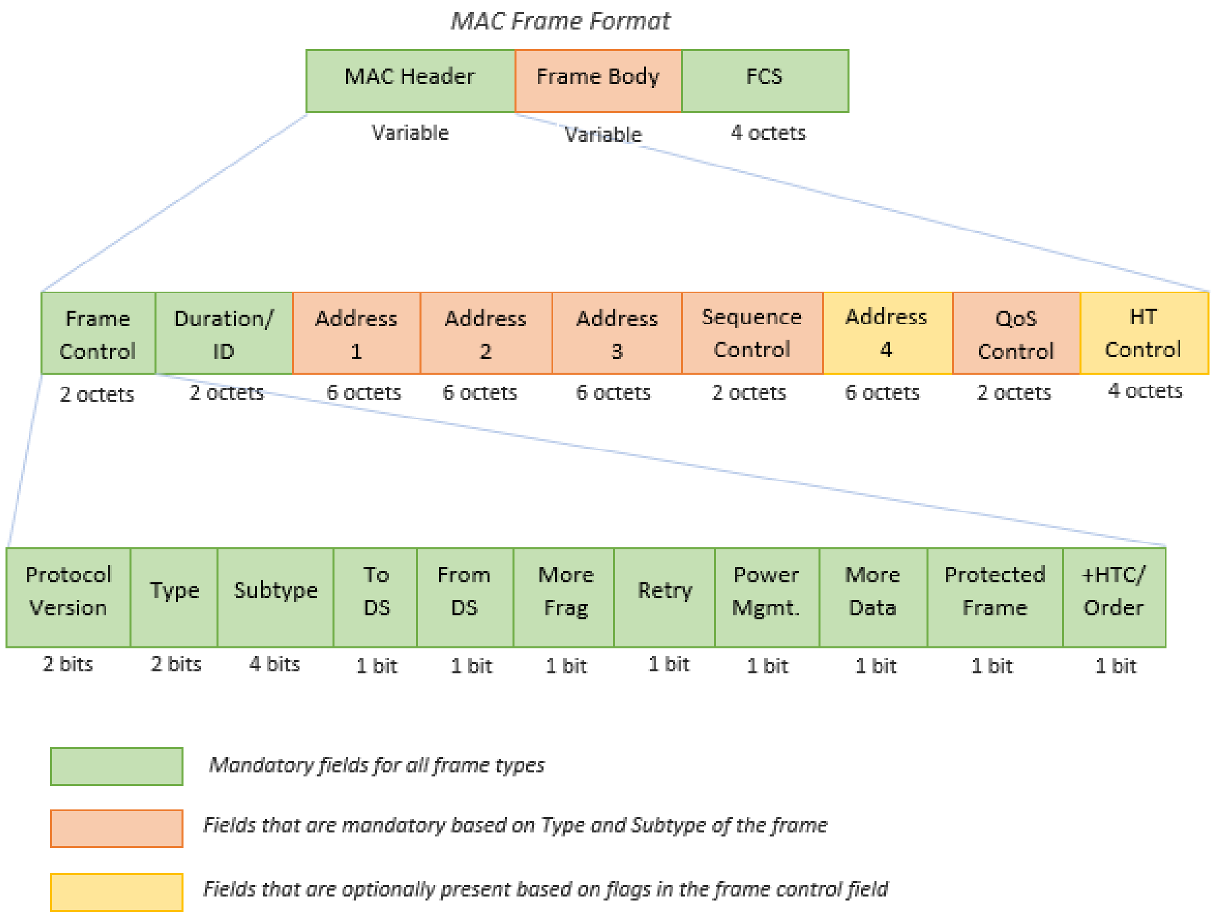
MAC Fields – Sequence Control

- **Sequence Control (2 Octets):**
- Ensures proper ordering and reassembly of fragmented frames.
- Subfields:
  - **Sequence Number**: Identifies the frame in a sequence.
  - **Fragment Number**: Specifies the fragment order for the frame.



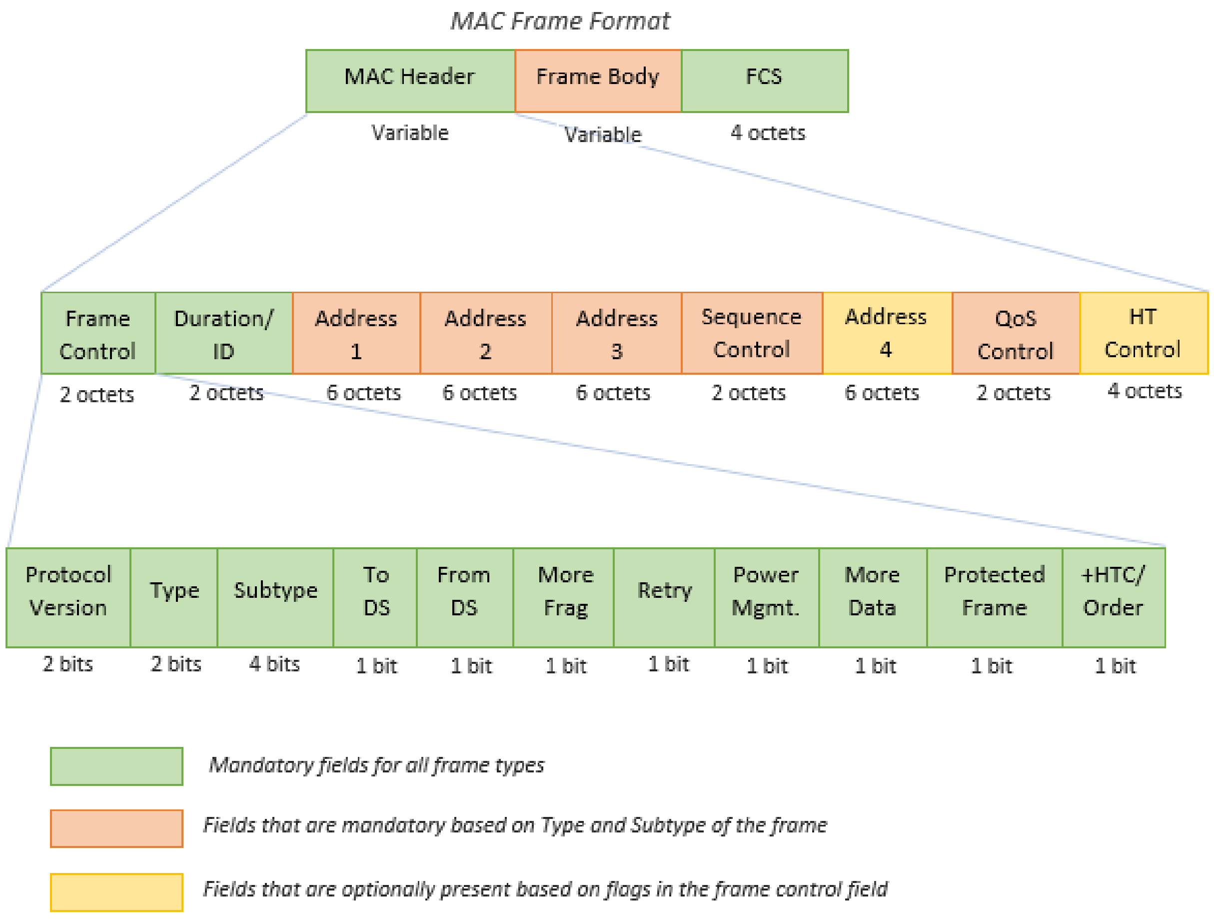
MAC Fields – QoS & HT Control

- **QoS Control (2 Octets) (Optional):**
  - Provides Quality of Service (QoS) support for prioritized traffic.
  - Used in 802.11e to manage multimedia traffic.
- **HT Control (4 Octets) (Optional):**
  - Used in High Throughput (HT) environments (802.11n) for advanced control and signalling.



MAC Fields – Frame Body & FCS

- **Frame Body (Variable Length):**
  - Contains the payload or data being transmitted.
  - Size can vary depending on the type of frame and the application.
- **Frame Check Sequence (FCS) (4 Octets):**
  - Contains a Cyclic Redundancy Check (CRC) to detect errors during transmission.
  - Ensures the integrity of the received frame.



MAC – Frame Types

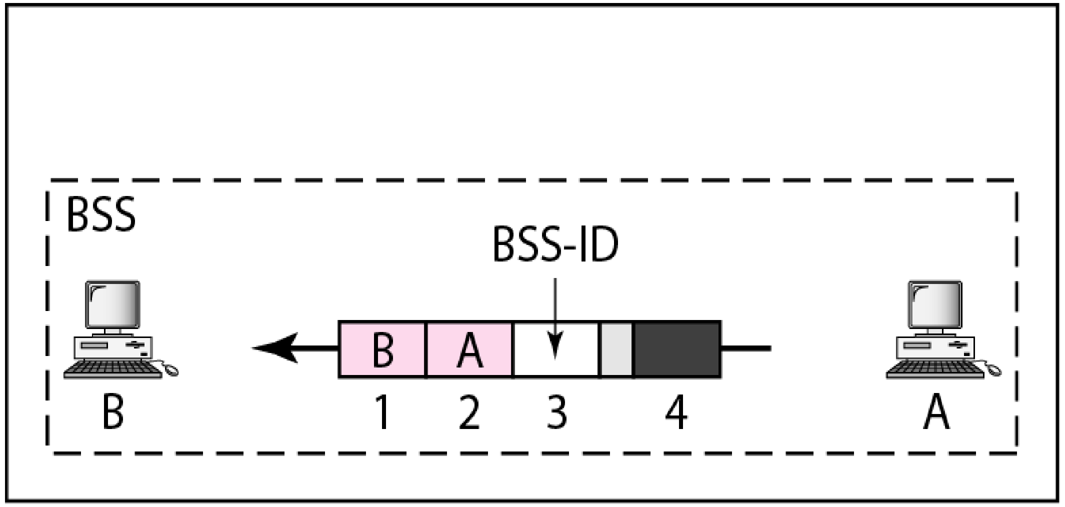
1. **Management Frames**:
   - Fields used for establishing and maintaining wireless connections (e.g., Beacons, Authentication).
2. **Control Frames**:
   - Fields used for managing access to the medium (e.g., RTS/CTS, ACK).
3. **Data Frames**:
   - Fields used to carry user data across the network.

MAC – Addressing Mechanisms

- **Case 1:** Communication Within the Same Basic Service Set (BSS)
- **Case 2:** Communication from a Device in One BSS to an External Device Through an AP
- **Case 3:** Communication from the Distribution System (DS) to a Device in a BSS
- **Case 4:** Wireless Distribution System (WDS) Communication

MAC – Addressing Mechanisms

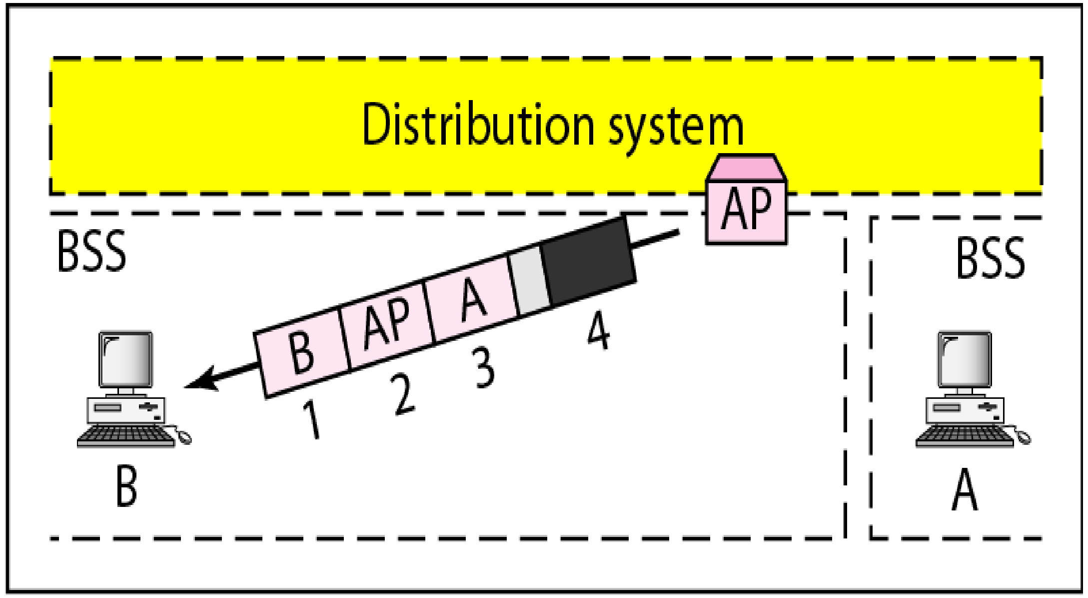
- **Case 1: Communication Within the Same Basic Service Set (BSS)**
- **Description**:
  - Two devices (stations A and B) communicate within the same BSS without involving a Distribution System (DS) or Access Point (AP).
- **Address Fields**:
  - **Address 1**: Destination address (B).
  - **Address 2**: Source address (A).
  - **Address 3**: BSSID (identifies the BSS to which the devices belong).
  - **Address 4**: Not used (set to null).
- **Key Point**: Direct communication between devices in the same BSS.



a. Case 1

MAC – Addressing Mechanisms

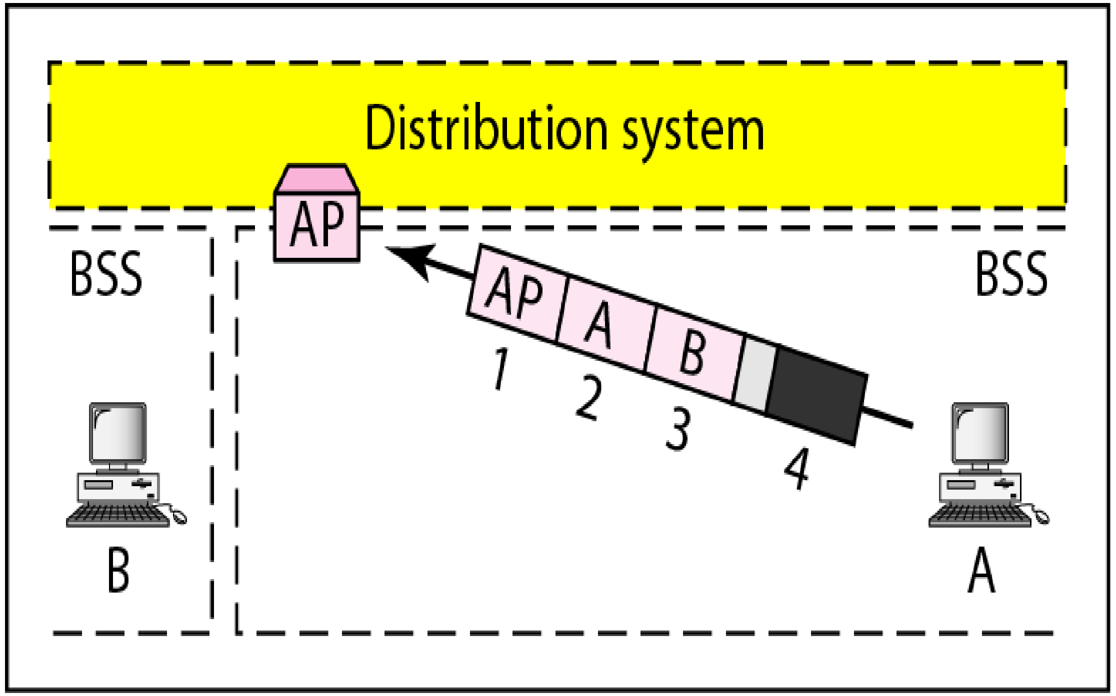
- **Case 2: Communication from a Device in One BSS to an External Device Through an AP**
- **Description**:
  - Device B sends data to device A through the AP and a Distribution System (DS).
- **Address Fields**:
  - **Address 1**: Destination address (A).
  - **Address 2**: Source address (B).
  - **Address 3**: BSSID of the AP connected to the DS.
  - **Address 4**: Not used (set to null).
- **Key Point**: The AP serves as the intermediary for forwarding data between the devices.



b. Case 2

MAC – Addressing Mechanisms

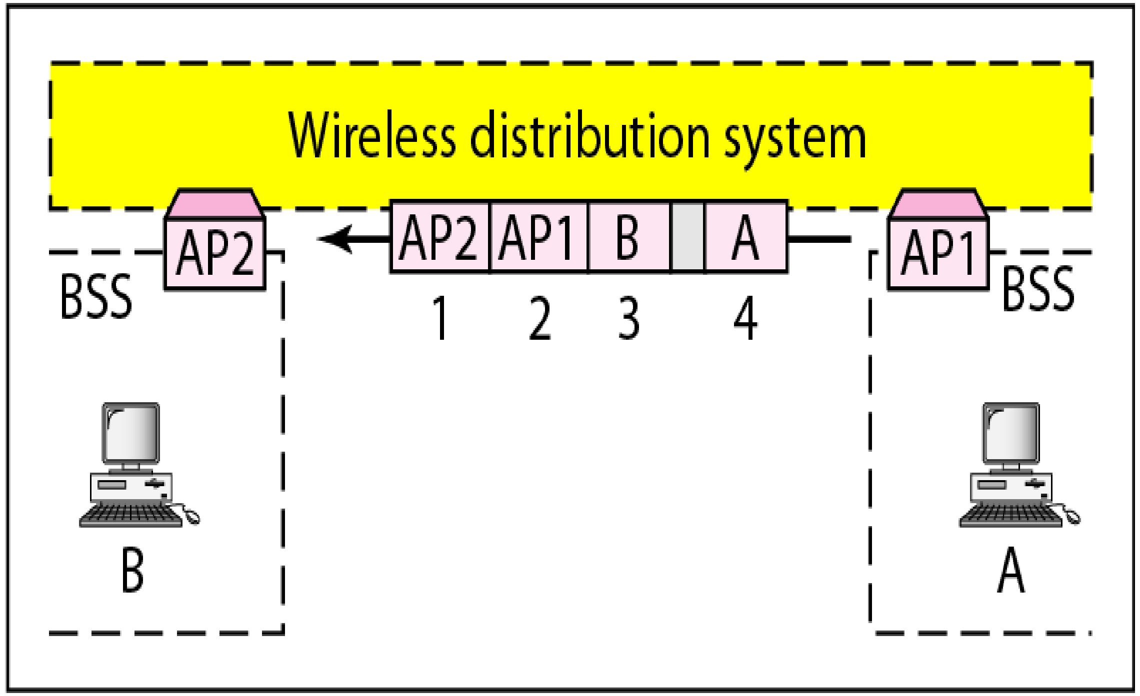
- **Case 3: Communication from the Distribution System (DS) to a Device in a BSS**
- **Description**:
  - Data from the DS is delivered to device B in the BSS via an AP.
- **Address Fields**:
  - **Address 1**: Destination address (B).
  - **Address 2**: Source address (A) from the DS.
  - **Address 3**: BSSID of the AP managing the BSS.
  - **Address 4**: Not used (set to null).
- **Key Point**: The AP relays data from the DS to a device in its BSS.



c. Case 3

MAC – Addressing Mechanisms

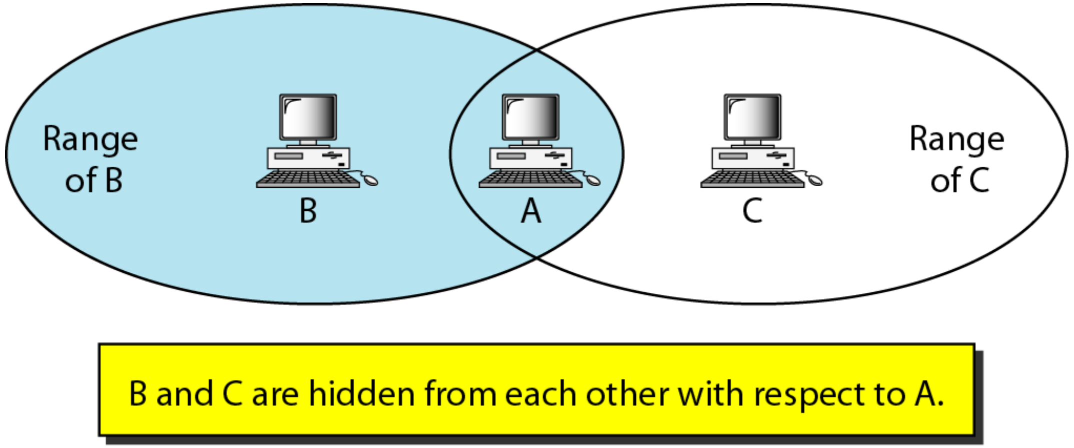
- **Case 4: Wireless Distribution System (WDS) Communication**
- **Description**:
  - Data is sent from device A in one BSS to device B in another BSS through two APs connected via a Wireless Distribution System (WDS).
- **Address Fields**:
  - **Address 1**: Final destination address (B).
  - **Address 2**: Source address (A).
  - **Address 3**: Address of the sending AP (AP1).
  - **Address 4**: Address of the receiving AP (AP2).
- **Key Point**: The frame uses all four address fields to route data through intermediate APs in the WDS.



d. Case 4

Hidden Station Problem

- **Problem Description**
- **Scenario**:
  - Device B is transmitting data to A, and device C starts transmitting simultaneously, unaware of B's activity.
  - Since A is within range of both B and C, it receives overlapping signals, causing a collision.
- **Cause**:
  - The hidden node problem arises because B and C cannot sense each other's transmissions, so they unknowingly transmit at the same time, leading to data corruption at A.

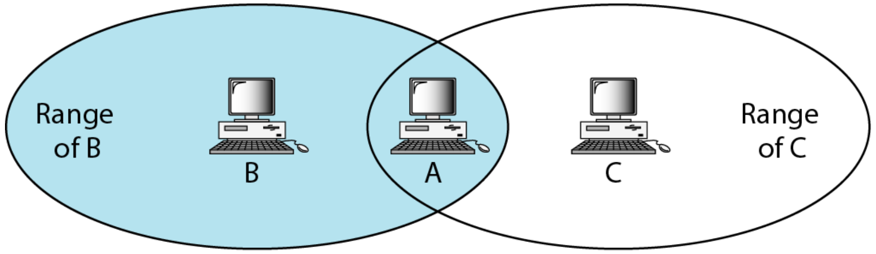


Impact:

- Collision of packets
- Reduced throughput
- Increased latency

Hidden Station Solution

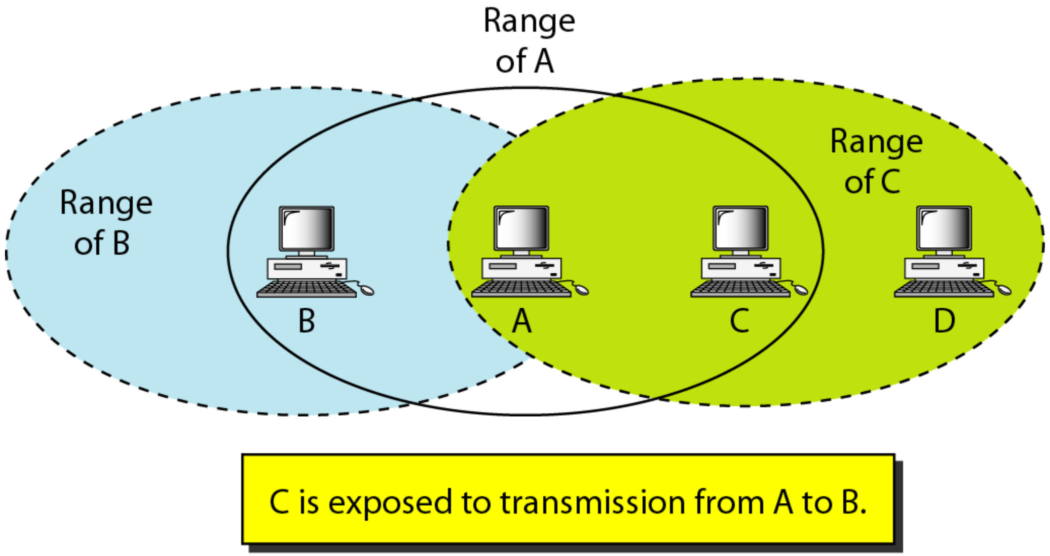
RTS/CTS (Request to Send / Clear to Send)	- B sends RTS to A. - A sends CTS to B. - C hears CTS and defers transmission, avoiding collisions.
CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)	- Devices sense the medium. - Use backoff timers to avoid simultaneous transmissions.
Power Control	Adjust transmission power to reduce communication range and minimize hidden nodes.
Directional Antennas	Use antennas that focus signals in specific directions to reduce interference and improve communication.



B and C are hidden from each other with respect to A.

Exposed Node - Problem

- **Scenario**:
  - Device A is transmitting data to B.
  - Device C, which is within the range of A, detects this transmission and refrains from transmitting to D, fearing a collision.
  - However, the transmission from C to D would not interfere with the communication between A and B because D is outside the range of A and B.
- **Cause**:
  - Device C cannot differentiate between transmissions that would cause interference and those that would not.



Impact:

- Bandwidth underutilization
- Reduced throughput
- Increased latency

Exposed Node - Solution

RTS/CTS	Ensures safe transmission by exchanging RTS/CTS signals.
Directional Antennas	Focuses signals to limit overlap.
Power Control	Adjusts transmission range to reduce overlap.
Enhanced MAC Protocols	Identifies non-interfering transmissions.