WI-FI TECHNOLOGY
FUNDAMENTALS COURSE

Module 3: WLAN MAC Layer

Session 3c:

CARRIER SENSE AND MEDIUM ACCESS

Thanushya Mothikivalasa
Rohini kaparapu
Nishtala Kiranmai
Jami Harika
Shiny Sayyad

CSMA/CD and CSMA/CA:

CSMA/CD and CSMA/CA

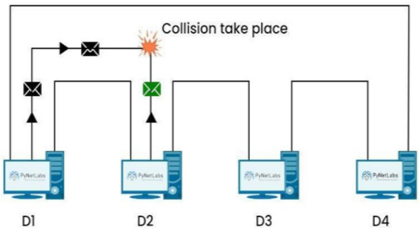
CSMA/CD and CSMA/CA are the media access methods that govern how a device can transmit data to the network.
CSMA/CD stands for Carrier Sense Multiple Access / Collision Detection. CSMA/CA stands for Carrier Sense Multiple Access/Collision Avoidance.

Both methods are used in a single collision domain. A single collision domain is a group of devices that share a collision. Since all devices share a collision, they use a method to avoid and remove the collision. Based on the media type used in the network, this method is known as either CSMA/CD or as CSMA/CA.

If the network uses wired media, this method is known as CSMA/CD. If the network uses wireless media, this method is known as CSMA/CA.

CSMA/CD

- This mechanism is only used in a single collision domain.
- All devices have equal priority.
- In this process, only one device can send data at a time.
- Before a device sends data, it will first sense the wire to ensure that no other device is currently sending data.
- If another device is currently using the media, it will have to wait till that transmission is over.
- If no device is currently using wire it can send the data.
- If two or more devices simultaneously sense wire and see no data in it, they could place their data on the wire at the same time.
- In this situation, a collision will occur.
- When a collision occurs, a special jam signal is created in the wire.
- Jam signal has a waiting time.
- All devices have to wait till the jam signal time is over.
- Once this time is over, devices can sense the wire again.
- If a device's data is lost in the collision, the device sends the same piece of data again.



CSMA/CA

- WLANs use a mechanism called Carrier Sense, Multiple Access/Collision Avoidance (CSMA/CA). Unlike Ethernet, it is impossible to detect collisions in a wireless medium. In a WLAN, a device cannot simultaneously send or receive data. It can only do one or the other. Because of this, it cannot detect a collision. To avoid collisions, a device will use virtual carrier sensing and random backoff mechanisms while accessing the medium.

Introduction to Multiple Access Problem:

The wireless communication challenge revolves around managing multiple devices seeking access to the same shared medium. Unlike scheduled methods, Wi-Fi networks often use a shared medium where multiple devices contend for access simultaneously.

CSMA/CD in Ethernet:
In the Ethernet realm, Carrier Sense Multiple Access with Collision Detection (CSMA/CD) is applied. Devices sense the carrier before transmitting, and if the medium is clear, they proceed. However, collisions may occur, leading to a backoff mechanism for retransmission.

CSMA/CA in Wi-Fi:
Wi-Fi employs Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). Due to challenges in detecting collisions over a wireless medium, CSMA/CA relies on preemptive measures. Devices sense the medium and wait for a clear window before transmission, aiming to minimize collision likelihood.

The Multiple/Medium Access Problem:

Shared Medium Dynamics:
In a shared medium scenario, like a Wi-Fi network, multiple devices attempt concurrent data transmission. This shared medium poses a challenge as only one device can transmit at a given moment, creating a collision domain.

Collision Implications:

Collisions occur when devices try to transmit simultaneously. Collisions lead to data corruption, necessitating a mechanism for resolution.

Solution1 – Use Scheduling:

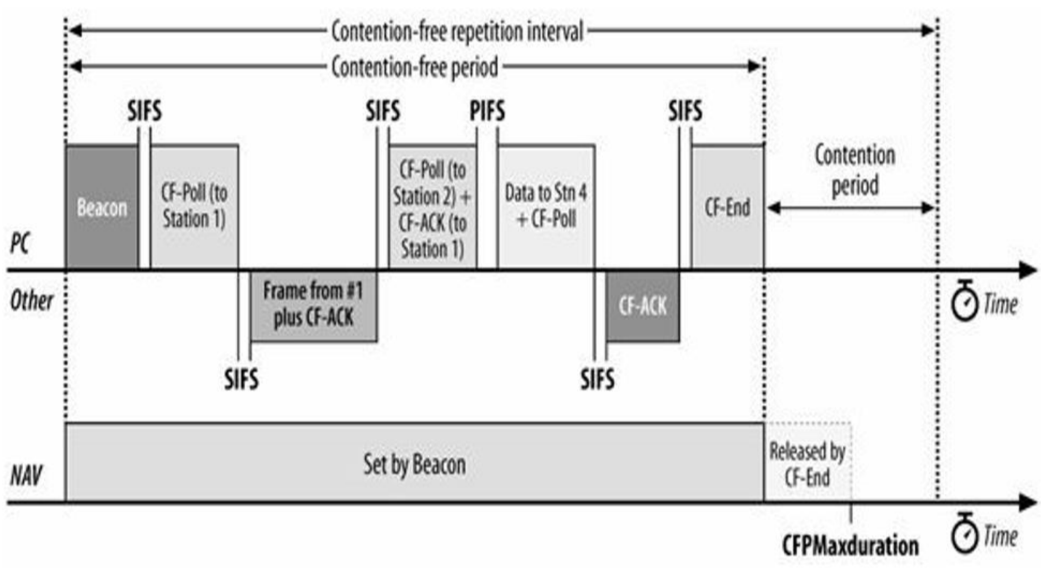
Introduction to Scheduling:
Scheduling offers a structured approach to handle multiple access. Devices, akin to students in a classroom or clients in a Wi-Fi network, receive allocated time slots for transmission. This method eliminates collisions by orchestrating a predetermined order of transmissions.

Application in Cellular Networks:
Cellular networks leverage scheduling to allocate time slots for different devices. Each device knows its designated transmission time, ensuring a deterministic and collision-free communication process.

Challenges and Alternatives:
While scheduling provides efficiency, challenges emerge in dynamic environments. Wi-Fi networks often choose CSMA/CA, emphasizing proactive measures to avoid collisions. This approach enhances adaptability in scenarios where scheduling may be impractical or inefficient.

Point Coordination Function (PCF) - AP Scheduling

The Point Coordination Function (PCF) is a method in Wi-Fi where the Access Point (AP) takes control of the medium's scheduling.



Connection-Free Period:

During PCF, there's a defined "connection-free period" where the AP asserts control over the medium.
Clients are instructed to refrain from transmitting during this period.

Beacon and Control:

The AP communicates its control through a beacon, specifying the duration of the connection-free period.
Within this period, the AP sends connection-free poll messages to specific stations.

Polling Process:

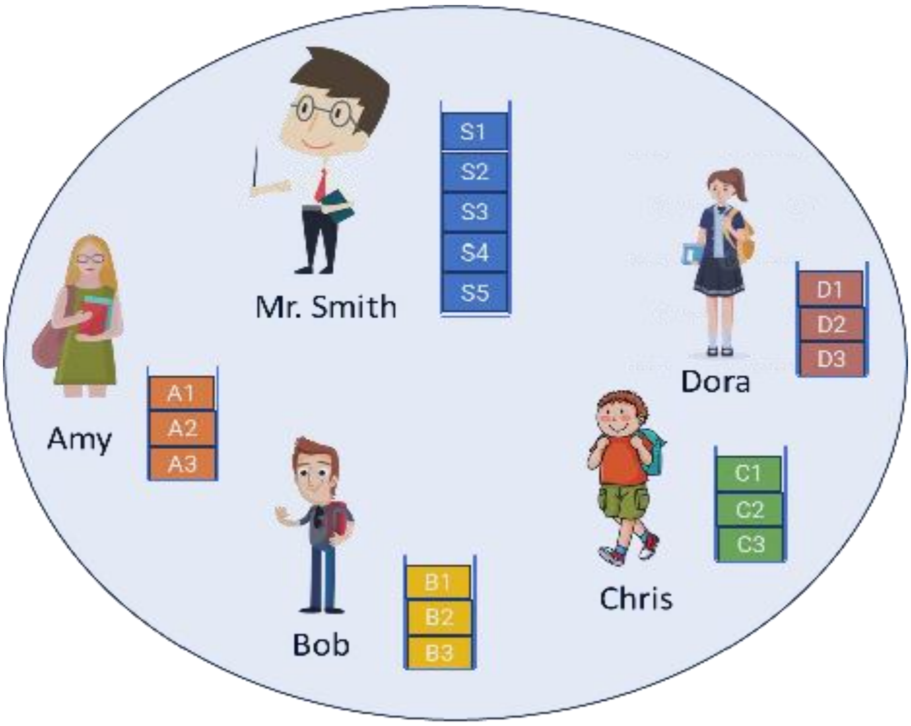
The AP individually polls stations, allowing them to transmit data in a controlled manner.
Stations respond with their frames, and the AP acknowledges each response before polling the next station.

Deprecation of PCF:

PCF has been deprecated in modern Wi-Fi protocols.
Wi-Fi predominantly utilizes a connection-free or contention-based protocol, where all stations contend for the medium without explicit scheduling.

Distributed Coordination Function (DCF) – Random Backoff

DCF is a protocol where coordination is distributed among all devices in contrast to a centralized point.



Example Illustration:

1. Pick Random Number:
Each student picks a random number between 0 and 5.

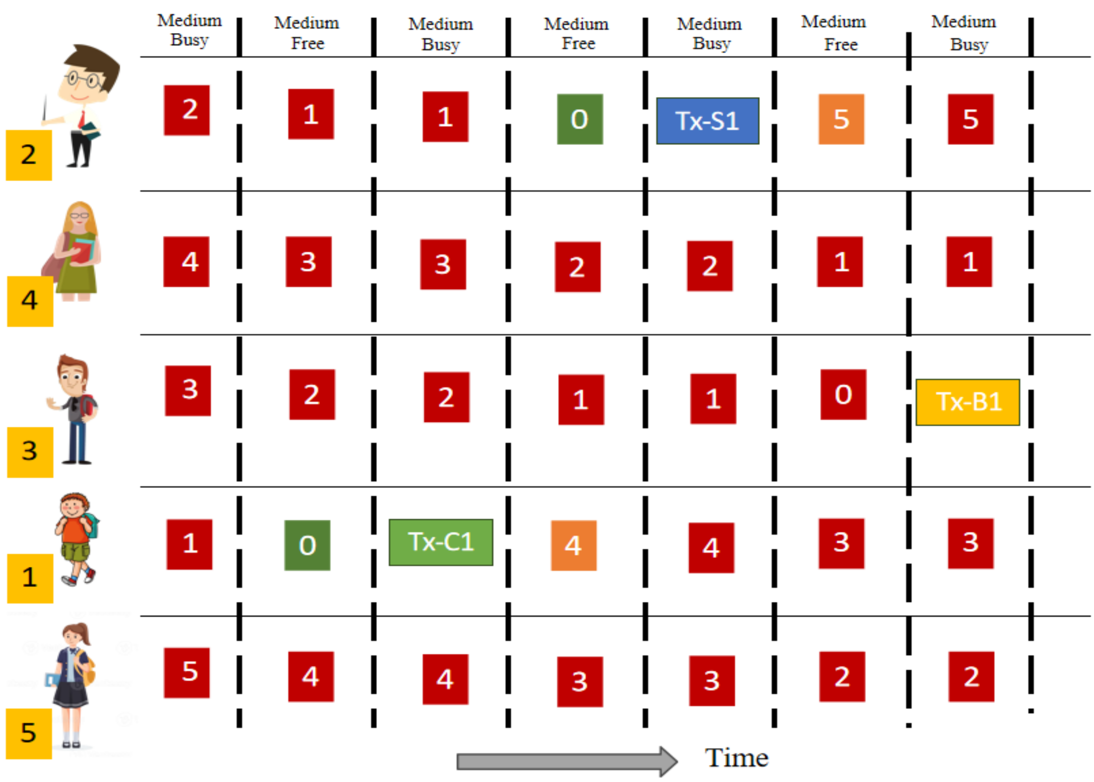
2. Transmission Criteria:
No one transmits until their randomly picked number reaches 0.
Countdown occurs only when the medium is free.

3. Countdown Process:
Every time the medium is free, everyone counts down by one number.
The first student reaching 0 will transmit if the medium is free at that time.

4. Medium Busy:
If the medium is busy, everyone stops counting down.

5. Post-Transmission:
After a successful transmission, the student picks a new random number and repeats the process.

6. Collision Handling:
Collision occurs if two students pick the same random number simultaneously.
In case of collision, students retransmit, picking a random number between 0 and 10 to reduce collision probability.



Comparison with Point Coordination Function (PCF):
PCF involves a single point (Access Point) controlling the medium.
DCF distributed coordination among all devices in the network.

Basic Principle:
Collision avoidance mechanism in Wi-Fi.
Devices individually pick random numbers during contention.

Random Number Picking:
Example with students randomly picking numbers between 0 and 5.
Statistically, they should avoid picking the same number, ensuring fairness.

Medium Status Sensing:
Devices sense the medium's status: busy or free.
If busy, they freeze their back-off counters; if free, they start counting down.

Transmission Criteria:
Transmission occurs when both the medium is free and the back-off counter reaches zero.

Fair Access:
Ensures fair access to the medium without centralized control.

Even if a device successfully transmits, it picks a new back-off counter and re-enters the queue.

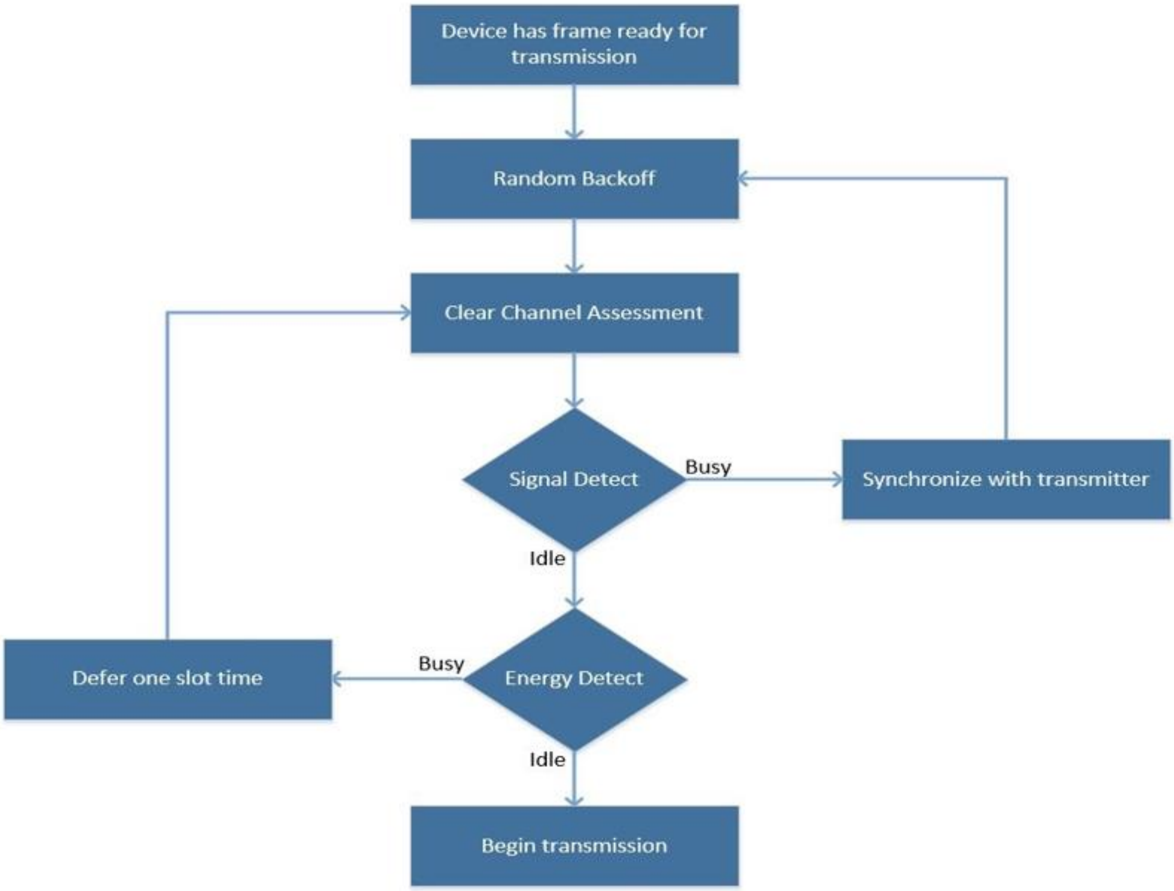
Handling Collisions:
If two devices pick the same number (collision), an exponential back-off mechanism is introduced.
Devices pick random numbers from an extended range, reducing the probability of collisions.

Statistical Fairness:
Over numerous cycles, statistical fairness is achieved, ensuring equal access to the medium.
Exponential Back-Off:
Introduced in case of collisions to reduce the likelihood of repeated collisions.

Distributed Coordination Function Essence:
No central scheduling; devices cooperate in a distributed manner.
Ensures collision avoidance and fair access to the communication medium.

Clear Channel Assessment (CCA)

Devices use two methods to determine whether the channel is clear. One is used to detect other Wi-Fi transmissions, signal detect (SD), and the other is used to detect any sources of interference that are affecting the medium, energy detect (ED).
Signal detect – Device detects an 802.11 preamble in range. The threshold is a signal that is about 4dB above the noise floor. This means that the device will defer transmissions if a nearby device is starting to transmit.
Energy detect – Device listens for any energy in the medium that is 20dB above the signal detect value. These devices could be Bluetooth, microwaves, baby monitors, or any other device that primarily operates in 2.4GHz or causes interference in the 2.4GHz range as a byproduct to its primary function.
The flowchart represents a simplified version of the CCA process.



Clear Channel Assessment (CCA) is crucial for Carrier Sense Multiple Access (CSMA) protocols.

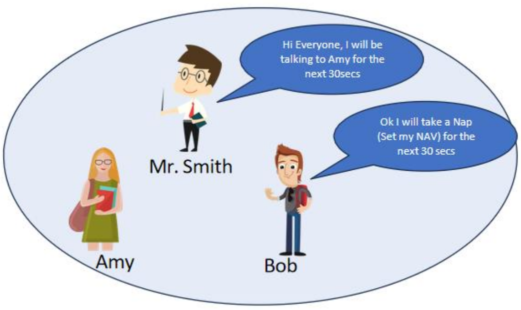
Signal Detect vs. Energy Detect:
Signal Detect: Identifying other valid frames being transmitted.
Energy Detect: Detecting energy or interference from other devices.

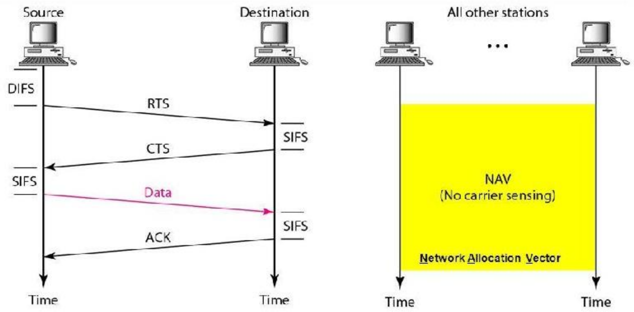
CCA Methods Flowchart:
Device with Frames to Transmit:*
Initiates a random back-off for collision avoidance.

During Random Back-Off:
Periodically checks the channel for activity.
If Channel is Busy (Signal Detected):
Returns to random back-off to avoid collision.
If Channel is Idle:
Checks for energy/interference.
If energy is present, the device freezes its back-off counter and rechecks.

If both signal and energy are absent, the device can transmit when the back-off counter reaches zero.

Network Allocation Vector (NAV)





- The network allocation vector (NAV) is a virtual carrier-sensing mechanism.
- The virtual carrier-sensing is a logical abstraction which limits the need for physical carrier-sensing at the air interface in order to save power.
- The MAC layer frame headers contain a duration field that specifies the transmission time required for the frame, in which time the medium will be busy.
- The stations listening on the wireless medium read the Duration field and set their NAV, which is an indicator for a station on how long it must defer from accessing the medium.
- The NAV may be thought of as a counter, which counts down to zero at a uniform rate.
- When the counter is zero, the virtual carrier-sensing indication is that the medium is idle; when nonzero, the indication is busy.
- The medium shall be determined to be busy when the station (STA) is transmitting.
- The NAV represents the number of microseconds the sending STA intends to hold the medium busy (maximum of 32,767 microsecs).

The primary purpose of the NAV is to prevent hidden node problems and reduce the likelihood of collisions in wireless communication. Hidden nodes occur when two or more stations cannot hear each other but are within the communication range of a common station. Without coordination, simultaneous transmissions from hidden nodes can lead to collisions and degraded network performance.

Operation:

- When a station wants to transmit a frame, it first listens to the channel to check if it is idle. If the channel is busy, the station will set its NAV to the duration of the busy period, preventing other stations from transmitting during that time.
- The NAV value is included in the control field of the frame and is broadcasted to other stations in the network.
- Stations receiving a frame with a NAV value will defer their transmission until the NAV timer expires, indicating that the channel is clear.

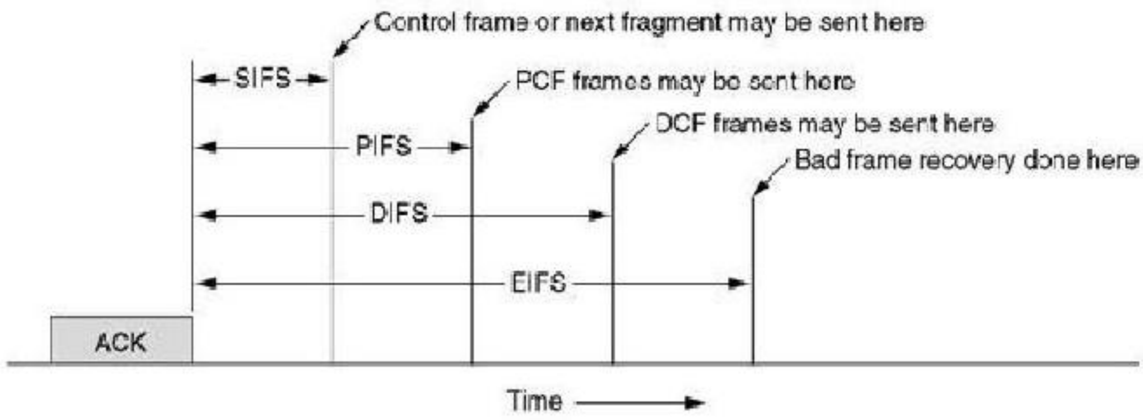
NAV Components:

- Duration Field: This field in the control frame indicates the duration for which the channel will be reserved. The NAV value is calculated based on the duration field and is set by the station initiating the transmission.
- Updating NAV: As control frames traverse the network, each station updates its NAV based on the received frames. The NAV is decremented as time progresses, and when it reaches zero, the channel is considered idle.

Frame Types:

- Clear-to-Send (CTS): When a station sends a CTS frame as part of the Request-to-Send (RTS)/CTS exchange, it includes a duration field that sets the NAV for the duration of the upcoming transmission.
- Acknowledgment (ACK): Similar to CTS, an ACK frame also includes a duration field, allowing the sender to reserve the channel for a short period.

Interframe Spaces



What is an Interframe Space (IFS) : It is a period of time that every Wi-Fi device (station) must wait before it transmits an 802.11 frame. IFS is used to avoid collisions and to prioritize medium access for transmissions.

There are 6 types of IFS and each one is used at different times and/or for different purposes.

- SIFS : Once a station has already been given the right to communicate, the SIFS is used between frames of an individual communication stream. SIFS is one of the shortest in length. This means that if a station already has an active communication stream, after having waited a DIFS or an AIFS, then waiting only a SIFS means that it will be able to continue that communication stream until it is through because every other station will have to wait at least a DIFS or AIFS which are both longer than a SIFS.
- PIFS : The Point Coordination Function (PCF) Interframe Space (PIFS) was for use specifically in PCF implementations. According to the 802.11-2016 standard, "The PCF mechanism is obsolete
- DIFS :The Distributed Coordination Function (DCF) Interframe Space (DIFS) is used as part of the process to determine who has the right to transmit. In other words, it is used when contending for the RF medium.
- EIFS : The Extended Interframe Space (EIFS) is used when a station receives a frame which fails the Frame Check Sequence (FCS), in which case it waits for an EIFS to give the sending station an opportunity to retransmit. The EIFS is the longest of all IFS and so is called "Extended".

Short Interframe Space (SIFS):

- SIFS is the shortest interframe space and is used between certain frames that require immediate acknowledgment, such as Acknowledgement (ACK) frames.
- Frames requiring SIFS include ACK frames, CTS (Clear-to-Send) frames, and the response to a polled frame in Point Coordination Function (PCF) mode.

Point Coordination Interframe Space (PIFS):

- PIFS is longer than SIFS but shorter than DIFS (Distributed Interframe Space).
- It is used by the Point Coordinator in PCF mode to contend for access to the medium.

Distributed Interframe Space (DIFS):

- DIFS is the longest interframe space and is used by stations to contend for access to the medium in the Distributed Coordination Function (DCF) mode, which is the default contention mechanism in WLANs.
- DIFS is used before transmitting data frames and management frames that are not immediate-response frames.

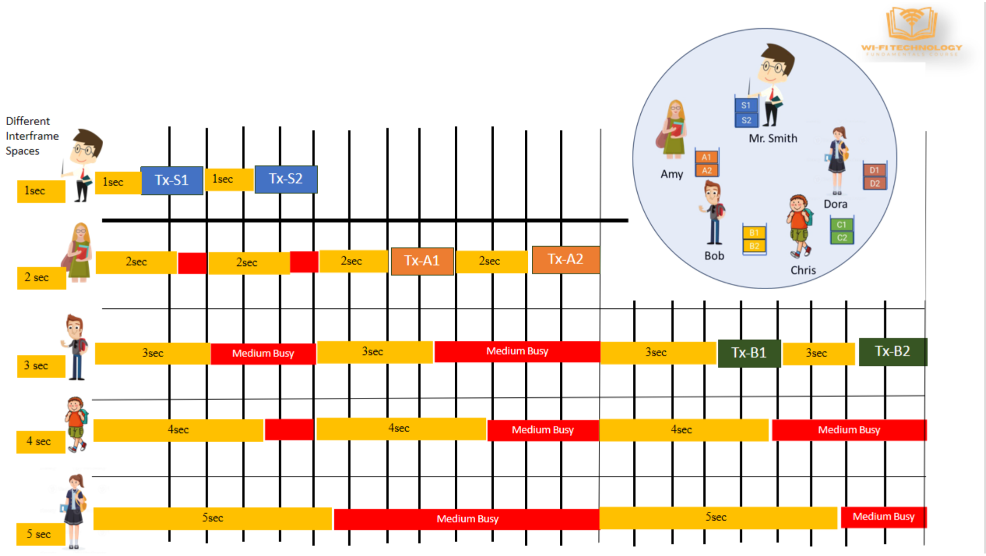
Extended Interframe Space (EIFS):

- EIFS is used after a station detects a frame with errors. The station waits for EIFS before attempting to transmit a new frame.
- This extended space allows time for potential retransmissions or recovery from errors before attempting to access the medium again.

The use of different interframe spaces helps in prioritizing access to the medium based on the urgency and nature of the frames being transmitted. For example, frames requiring immediate acknowledgment (such as ACK frames) are given the shortest interframe space (SIFS) to ensure prompt acknowledgment. On the other hand, the longer DIFS is used for regular data frames, allowing for a more extended contention window.

These interframe spaces contribute to the overall efficiency and fairness of the WLAN by providing a structured and prioritized approach to accessing the shared wireless medium.

Inter Frame Spaces used for Preferential Access



Inter-Frame Spaces (IFS):

- Definition: Inter-Frame Spaces are time intervals between the transmissions of frames, and different frame types or users may have different IFS durations.
- Example: Mr. Smith (the teacher) has a shorter IFS of 1 second, while Amy has 2 seconds, Bob has 3 seconds, Chris has 4 seconds, and Dora has 5 seconds.
- Purpose: Shorter IFS durations grant higher priority access to the medium.

Preferential Access Scenario:

- All users see the medium as free at Time Zero.
- The rule is that users need to see the medium free for at least their IFS duration before transmitting.
- Example: Mr. Smith only needs to see the medium free for 1 second before transmitting, giving him preferential access over others.

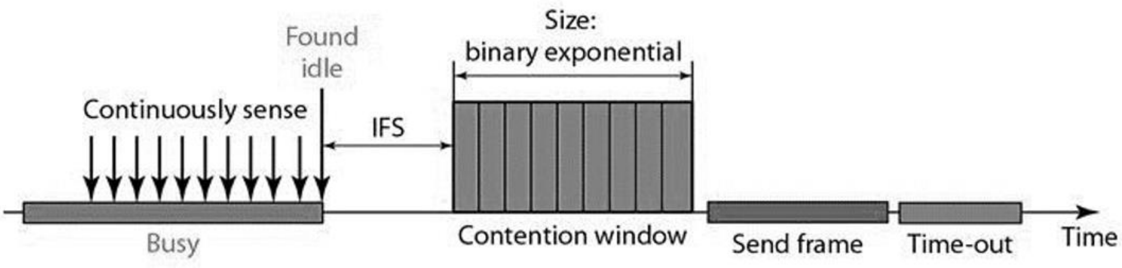
Transmission Scenario:

- Mr. Smith transmits after waiting 1 second (his IFS duration).
- Amy has to wait 2 seconds (her IFS duration) before she can transmit.
- This process continues, and each user must wait their specified IFS duration before accessing the medium.

Preferential Access Impact:

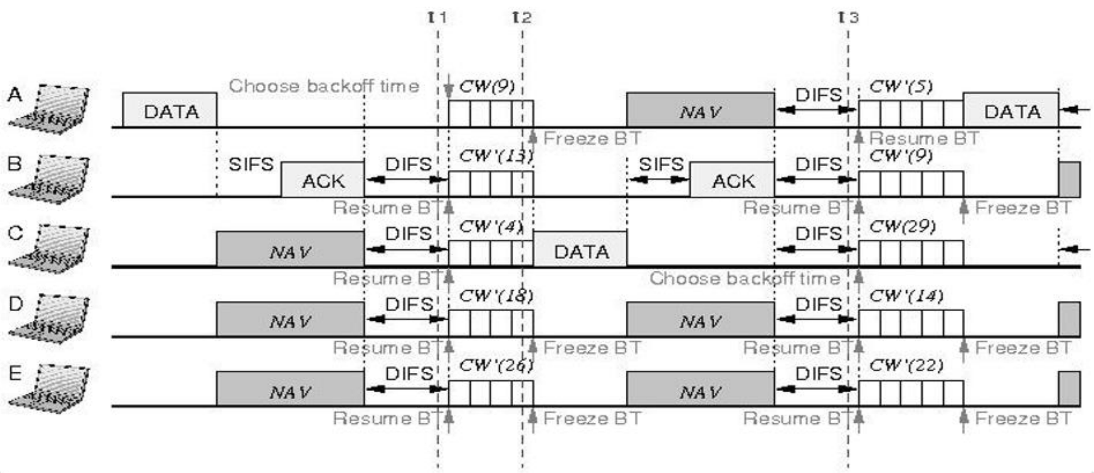
- Users with shorter IFS durations get statistically more opportunities to transmit.
- Mr. Smith, with a 1-second IFS, gets preferential access over Amy (2 seconds), Bob (3 seconds), and so on.

Contention Window



- The contention window in Wi-Fi is like a range of numbers you can pick from when deciding how long to wait before transmitting data. Imagine you're in a crowded room, and there's a rule that everyone has to wait a random amount of time before talking. This "window" is the range of numbers you can choose from.
- For example, if the contention window is from 0 to 5, you can pick any number between 0 and 5. Let's say you pick 3. That means you'll wait for 3 time units before trying to talk again. If someone else picks the same number, they'll also wait for 3 units.
- Now, if the window is larger, say from 0 to 20, you have more numbers to choose from. This reduces the chance of two devices picking the same number, which is good because it avoids collisions (when two devices try to talk at the same time and clash).
- However, here's the trade-off: with a larger window, you might end up waiting longer before speaking because you're picking from a larger range of numbers. So, while it reduces collisions, it might slow down access to the network.
- In simpler terms, the contention window is like the range of numbers you can pick to decide how long to wait before talking on a busy Wi-Fi network. It's a balancing act between reducing clashes and waiting time for a chance to talk.

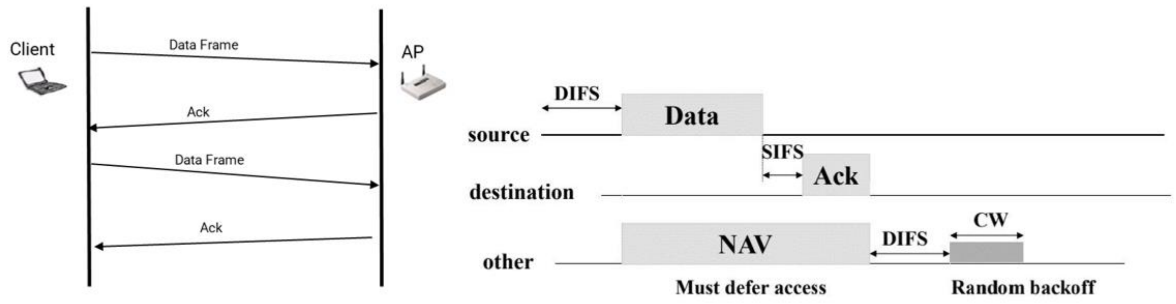
Backoff Algorithm



In Wi-Fi, before a device can transmit data, there's a process to ensure the network isn't too crowded. This involves several steps:

- Channel Sensing: Before transmitting data over Wi-Fi, a device 'listens' to the channel to check if it's busy or free. After detecting a silent channel, the device waits for a minimum duration called DIFS (Distributed Interframe Space). If the channel remains quiet for this duration, the device extends its wait randomly to ensure the channel is genuinely clear.
- Transmission Decision: If the channel remains idle after this additional random wait, it's like receiving a green light to start transmitting data. This step ensures no other devices are using the network at that moment.
- Controlling Wait Time: Each device has a 'CW' (Contention Window), determining how long it should wait before attempting to transmit. The 'CW' acts like a range of numbers from which the device chooses its waiting time. The larger the 'CW,' the longer the potential wait time.
- Counting Down: Devices randomly pick a number within their 'CW' range and begin counting down. This countdown decides when they can start transmitting. Each 'slot' of time during the countdown is a unit of measurement.
- Adjusting Countdown: If a device detects the channel is clear during a slot, it continues counting down. But if it senses any transmission during a slot, it pauses the countdown. This freezing prevents collisions with other devices attempting to transmit.
- Initiating Transmission: When the countdown reaches zero, the device starts transmitting data. However, if this attempt fails, the device begins a new countdown with an increased 'CW.' This adjustment reduces the chance of colliding with other devices attempting to access the network.
- This process continues, with devices adjusting their 'CW' and countdowns based on the channel status. It's like a controlled waiting game, ensuring fair and efficient access to the Wi-Fi network for all devices without causing interference or collisions.

Basic Data Transmission



basic data transmission process in Wi-Fi:

1. **Data Transmission and Acknowledgement:** Imagine a client sending data to an access point (AP), followed by the AP sending an acknowledgment (ACK). For Wi-Fi communication to work smoothly, these transmissions need to be continuous or "atomic." After the data is sent, the medium becomes free for a moment.
2. **Ensuring Sequential Access:** However, it's crucial that only the AP accesses the medium after the data transmission to send the ACK. If another device tries to transmit, it might block the ACK, causing the client to assume the data wasn't received, leading to unnecessary retransmissions.
3. **Maintaining Order:** To prevent this, a short Inter-Frame Space (SIFS) time is designated for the AP to send the ACK. Other devices must wait a longer Distributed Inter-Frame Space (DIFS) time before attempting transmission.
4. **Atomic Data-ACK Combination:** This setup ensures that only the ACK immediately follows the data frame. If multiple devices detect the free medium, the AP can quickly send the ACK due to its shorter wait time (SIFS), while others must wait longer (DIFS) before sending their frames.
5. **Prioritizing Frame Transmission:** Wi-Fi uses different Inter-Frame Space times for various frame types, prioritizing critical frames like acknowledgments or control frames (e.g., RTS, CTS, beacon). Shorter spaces give these high-priority frames preferential access to the medium.
6. **Enhanced Medium Access Control:** By assigning shorter wait times for crucial frames, Wi-Fi networks ensure that essential transmissions like acknowledgments have higher priority, preventing interruptions or delays caused by other devices trying to access the medium simultaneously.
7. This system helps maintain order and priority in transmitting different types of frames over Wi-Fi, allowing essential frames, especially acknowledgments, to access the medium quickly after data transmissions, thereby ensuring efficient and reliable communication.

Exponential Backoff

Binary Exponential Backoff (BEB) is like a traffic cop for Wi-Fi devices trying to talk on a busy road. When two or more devices try to communicate at the same time (like trying to cross an intersection together), BEB steps in to avoid chaos.

Here's how it works:

Retry and Double: If a device fails to communicate, it doesn't give up right away. Instead, it waits for a bit, then tries again. If it still doesn't work, the waiting time doubles. This prevents a rush of devices trying to talk all at once.

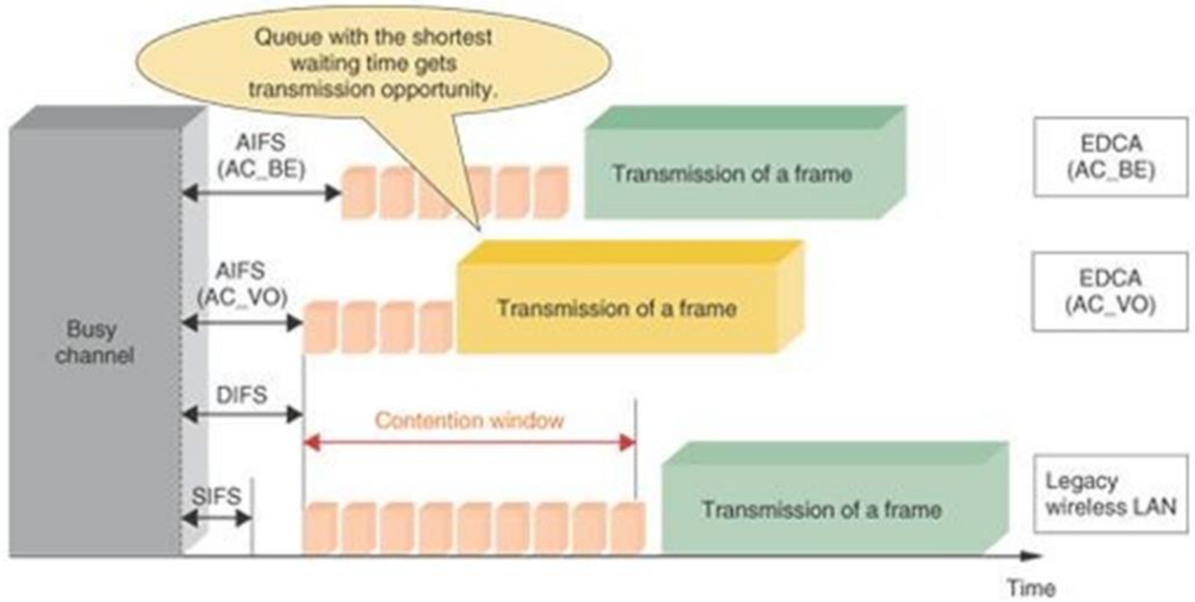
Preventing Congestion: BEB is like telling devices, "Hey, if it's crowded out there, wait a bit longer before trying again." This prevents everyone from attempting to talk at the same time, reducing the chance of a traffic jam in Wi-Fi land.

Improving Efficiency: In systems where many devices are vying for the same Wi-Fi 'road,' BEB helps manage the chaos. Without it, everyone might try to grab the road when it's free, causing confusion when it's time to move.

Optimizing Resource Use: In scenarios where devices need to share a common resource (like a specific Wi-Fi channel), BEB ensures a smoother flow. It helps prevent a stampede when the resource becomes available, making sure devices take turns instead of all rushing at once.

Probabilistic Systems: BEB shines in situations where it's hard to predict who gets access next. It's like saying, "Okay, whoever gets there first gets the chance to talk." Others have to patiently wait for their turn.

Wi-Fi QoS (WMM) Basics



1. Distributed QoS in Wi-Fi:
- QoS in Wi-Fi operates in a distributed fashion.
- Different devices may have varying priorities for sending traffic, such as voice or data.

2. Arbitrary Interframe Space (AFS):
- Higher-priority traffic uses a shorter interframe space (AFS) to access the medium.
- Lower-priority traffic uses a longer interframe space, ensuring a longer wait time.

3. Connection Window Size:
- Random back-off involves picking a random number from a connection window.
- For higher-priority traffic, a smaller connection window is used, increasing the chances of quicker access.

4. Access Categories:
- Wi-Fi has access categories (access categories include Best Effort, Background, Voice, and Video).
- Different access categories have different AFS and connection window values.

5. Prioritizing Traffic:
- Access categories have different AFS values and back-off counter ranges.
- For example, voice traffic may have a shorter AFS and a smaller back-off counter range than background traffic.

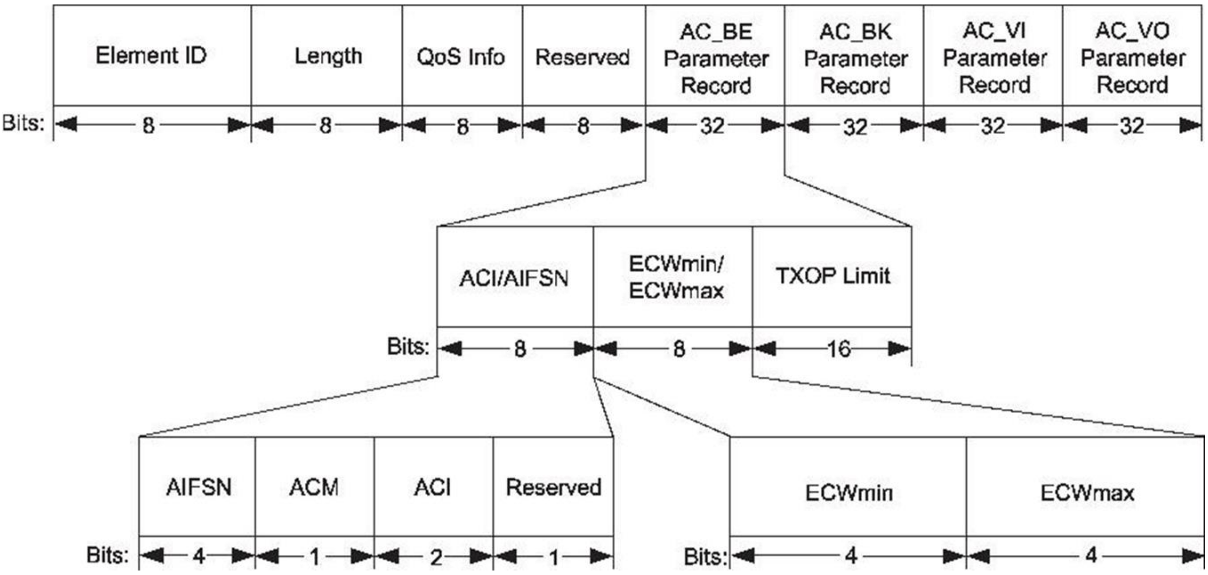
6. Statistical Access:
- Even with lower priority, there's a statistical possibility for lower-priority traffic to gain access over time.
- The protocol ensures fairness over the long term, allowing all priorities to transmit.

7. Preferential Access:
- The protocol creates preferential access by assigning different AFS and connection window values to each access category.

8. WM QoS Protocol:
- WM QoS protocol involves different queues (access categories) with specific AFS and connection window values.
- This protocol ensures preferential access to the medium based on the priority of the traffic.

9. QoS Algorithm:
- QoS is achieved through the selection of AFS and connection window values for each access category when transmitting frames.

EDCA Parameter Set



Let us know how the Access Point (AP) implements QoS through the EDCA (Enhanced Distributed Channel Access) parameter set in Beacon frames:

1. Beacon Frames and Information:

- The AP regularly sends out Beacon frames, sort of like a signal to all devices in the area, announcing its presence and sharing important information.

2. EDCA Parameter Set:

- Inside the Beacon frame, there's a part called the EDCA Parameter Set. This is where the AP spills the beans on how it wants devices to access the communication space.

3. Instructions for Different Traffic:

- The EDCA Parameter Set provides instructions for different types of traffic. For example:
- "Hey, if you've got important voice traffic, use this specific connection window size and AFS value."
- "Background traffic, you use a different set of values."

4. Broadcasting to All Devices:

- These instructions are like a broadcast to all devices in the network. So, every device knows how to behave based on the type of data it has to send.

5. Controlling Quality of Service:

- By tweaking these EDCA parameters a bit, the AP can control the quality of service (QoS).
- For instance, if the AP sets large values for connection windows and AFS for background traffic, and small values for voice traffic, it creates a big gap in priority.
- If the values are closer for both types of traffic, the priority levels are more similar.

6. Degree of Control:

- The AP can fine-tune how much priority it gives to different types of traffic by adjusting these EDCA parameters.

7. User Control:

- In some cases, certain APs might even allow users to manually set these parameters. So, you could potentially have some control over how your device's data is treated within the network.

In simple terms, the AP is like the boss of the network, and it uses Beacon frames to tell all devices how to play nice and take turns in talking. By adjusting the EDCA parameters, the AP decides who gets to talk sooner, and this helps in controlling the quality of service for different types of data.

Note:You can see a practical demonstration of how EDCA parameters and QoS work in the course playlist on YouTube (https://www.youtube.com/watch?v=53L6oINQZdE).Check it out for better understanding.