WI-FI TECHNOLOGY
FUNDAMENTALS COURSE

Module 3: WLAN MAC Layer

Session 3a:

BASIC AP MANAGEMENT AND CONTROL FUNCTIONS

Thanushya Mothikivalasa
Rohini kaparapu
Nishtala Kiranmai
Jami Harika
Shiny Sayyad

The Multiple Access Problem

Single Transmitter and Receiver Model

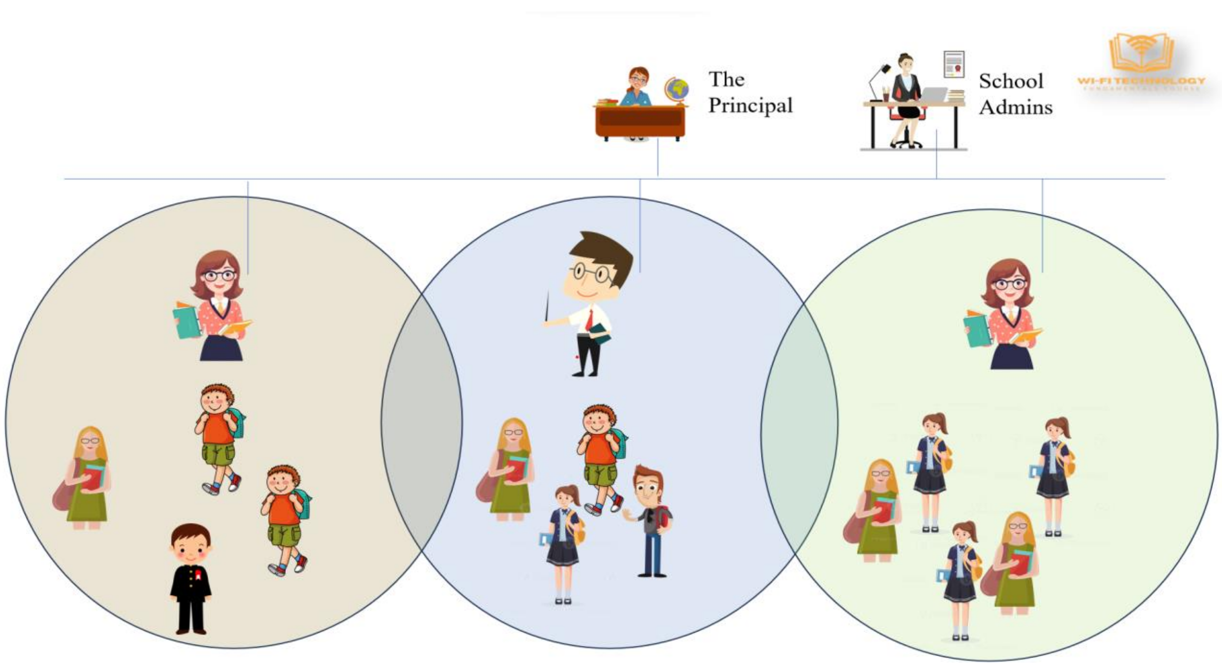
The basic communication model involves a single transmitter communicating with a single receiver over a wireless medium. This encompasses various concepts such as modulation, signal-to-noise ratio, coding mechanisms, and frequency spectrum.

Real-world Complexity

In the real world, the scenario extends beyond a single transmitter and receiver. Multiple transmitters (client devices) and receivers are connected to one access point, leading to what is known as the multiple access problem.

Classroom Analogy

To illustrate the complexity of multiple access, an analogy is drawn with a classroom setting. Imagine a teacher (access point) trying to teach multiple students (devices) simultaneously. This highlights the need for mechanisms to manage communication among multiple devices.



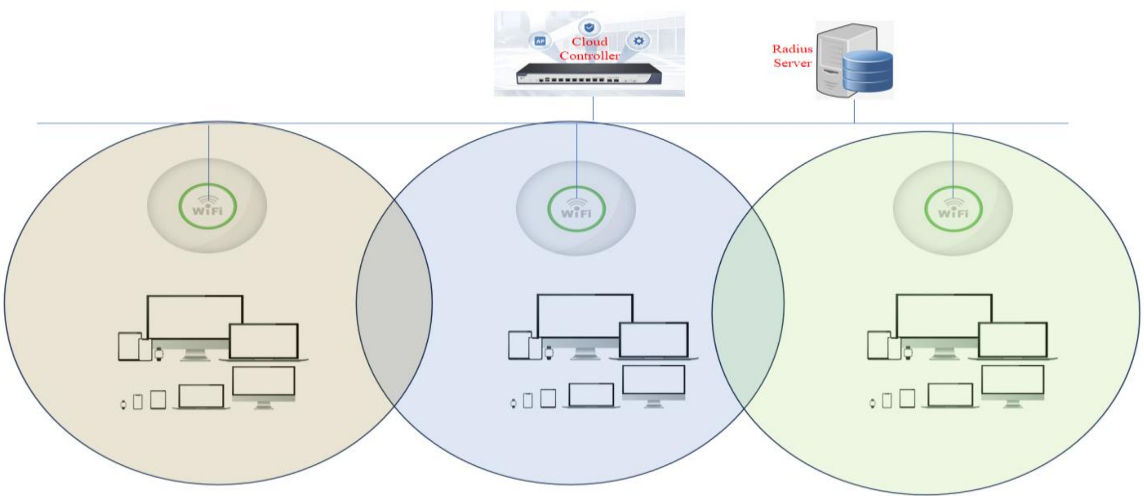
Challenges and Solutions

Addressing the multiple access problem involves solving challenges like interference, security, roaming, scheduling, and controls. Mechanisms akin to classrooms, such as time slot allocation or raising hands, must be established.

Multiple Access
Range
Interference
Security
Roaming
Scheduling
Management
Controls

Applying the Analogy to Wi-Fi

The analogy is extended to Wi-Fi, where the Wi-Fi router acts as the teacher, Wi-Fi stations as students, and cells as classrooms. Network elements like radius servers and controllers manage authentication, authorization, accounting, and configurations.



Extra Overhead in Multiple Access

In a multiple access scenario, additional overhead, including security, scheduling, controls, and management, is introduced to ensure successful communication between devices and access points.

What is a Beacon Frame?

Wi-Fi devices automatically scan for available networks.
Similar to scanning for restaurants, Wi-Fi devices search for Wi-Fi networks in the vicinity.

Beacon Frames:

Every access point sends out a "beacon frame" every 100 milliseconds.
This frame is broadcasted within the access point's wireless LAN cell.

Purpose of Beacon Frames:

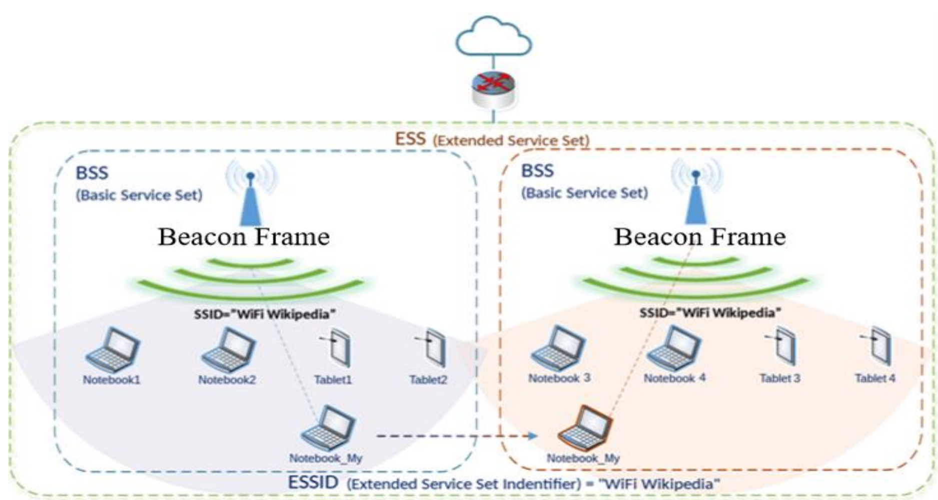
Beacon frames serve as a fundamental mechanism for devices to identify and list available Wi-Fi networks.
Comparable to a restaurant menu, the beacon frame contains information about the access point's capabilities.

Contents of Beacon Frame:

Includes details such as supported Wi-Fi standards (e.g., Wi-Fi 5, Wi-Fi 6), security mechanisms, QoS support, and load balancing capabilities.
Essentially, the beacon frame acts as an advertisement for the access point.

Scanning Process:

Devices, like phones, periodically tune to different frequencies (channels) to scan for beacons.
Upon detecting a beacon, the device reads the information, creating a list of available Wi-Fi networks.

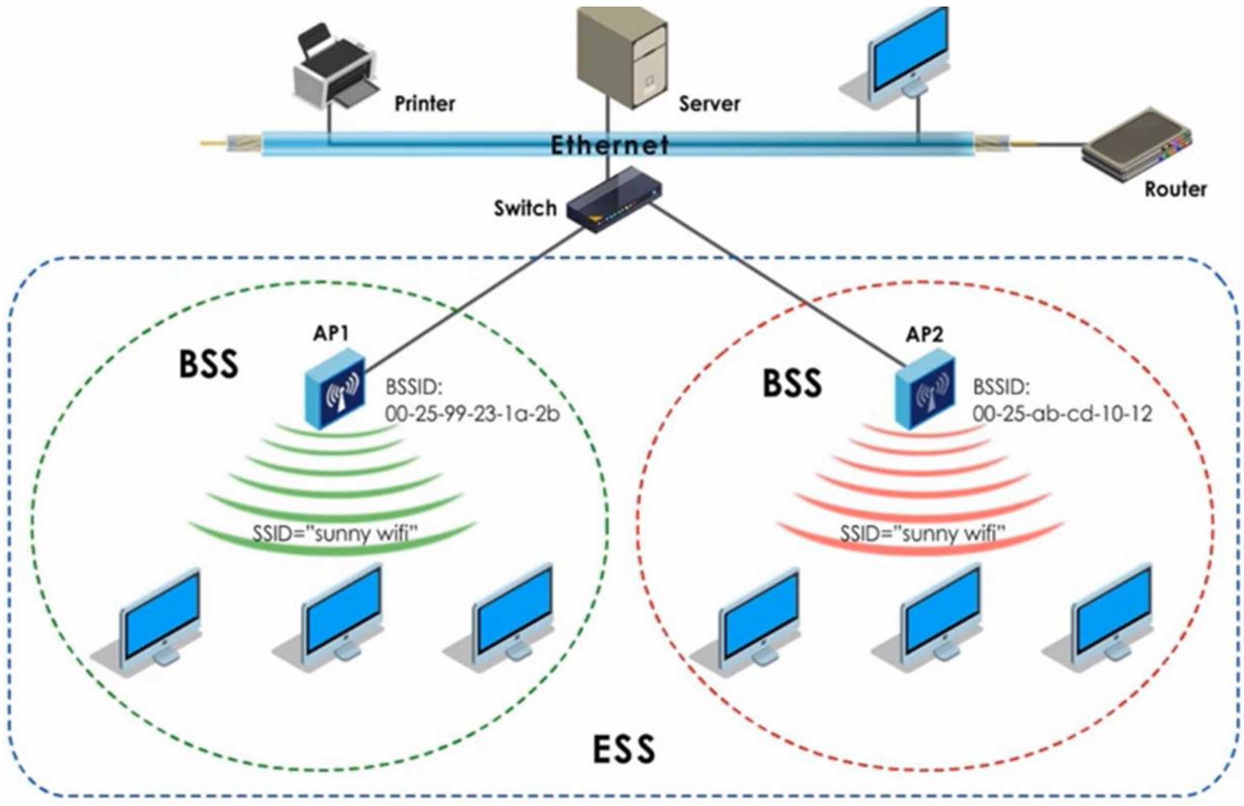


Analogy:

Analogous to surveying restaurants in a food court and creating a list of preferred options. The beaconing process allows devices to discover and compile a list of accessible Wi-Fi networks.

For a clearer understanding, you can check out the example explained in the video starting from the timestamp(16:05) available on YouTube.

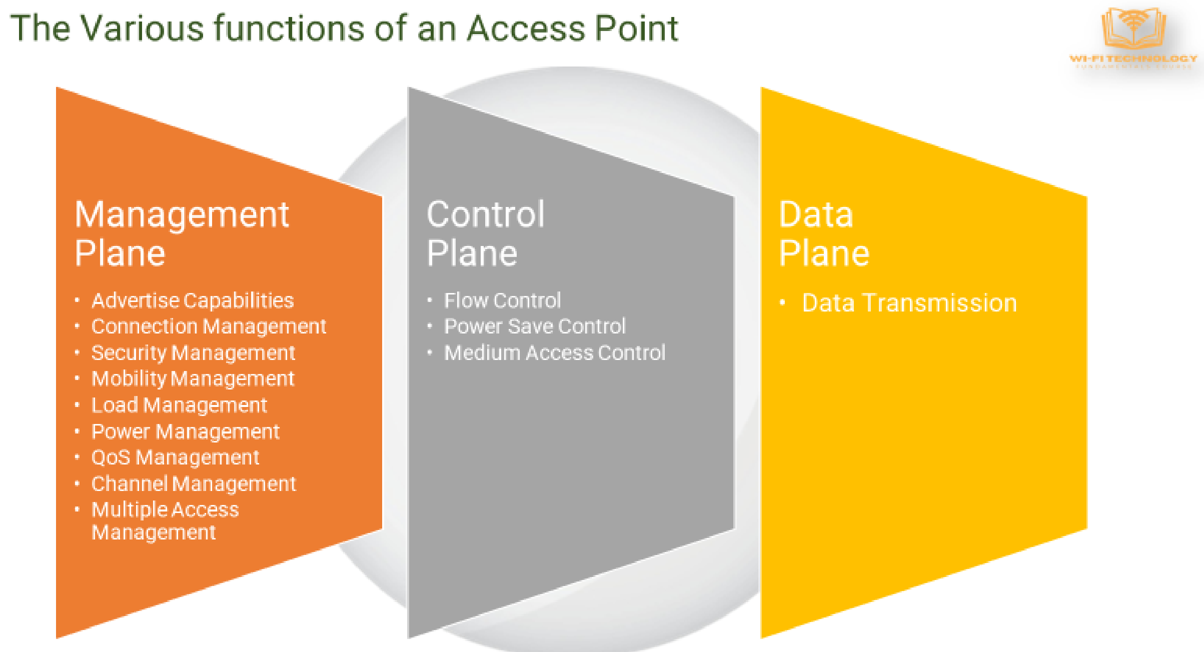
SSID and BSSID



SSID (Service Set Identifier): The SSID is essentially the name of a Wi-Fi network. When an access point broadcasts its SSID, it allows devices to recognize and connect to that particular network. It serves as a logical identifier. For instance, in the context of your explanation, if an access point advertises the SSID "Sunny Wi-Fi," devices looking to connect to that network will recognize it by this name.

BSSID (Basic Service Set Identifier): On the other hand, the BSSID acts as the physical identifier or MAC address of a specific access point. Every access point has a unique BSSID, even if they are part of the same SSID. This address is crucial for distinguishing between different access points, ensuring that devices connect to the intended point.

The Various Functions of an Access Point:



Management Plane: In the management plane, the access point handles crucial administrative tasks. This includes managing client connections, ensuring network security, handling mobility between access points (as devices move within the network), load balancing to distribute connections evenly, power management for efficient energy use, and the implementation of QoS (Quality of Service) to prioritize certain types of data.

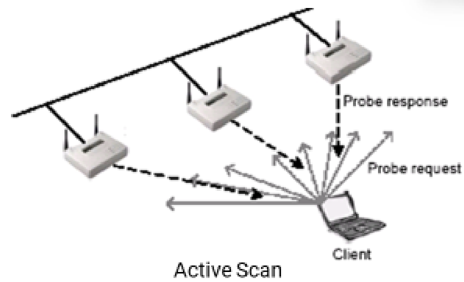
Control Plane: The control plane is responsible for overseeing flow control, power-saving mechanisms to conserve energy, medium access control to regulate how devices share the network, and various other control-related functions. It ensures the efficient management of network resources and communication.

Data Plane: The data plane's primary function is to handle the actual transmission of data between devices connected to the Wi-Fi network. It ensures that data packets are efficiently routed between the source and destination devices, facilitating effective communication.

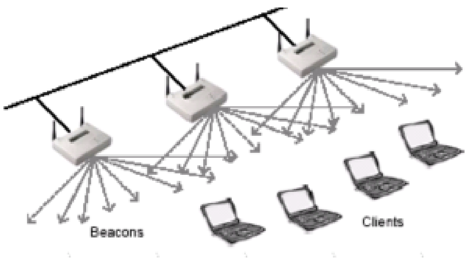
Scanning

Scanning

1. Scanning is the first step for the station to join an AP's network.
2. In the case of passive scanning the client just waits to receive a beacon frame from the AP
3. Station searching for a network by just listens for beacons until it finds a suitable network to join.



Active Scan



Passive Scan

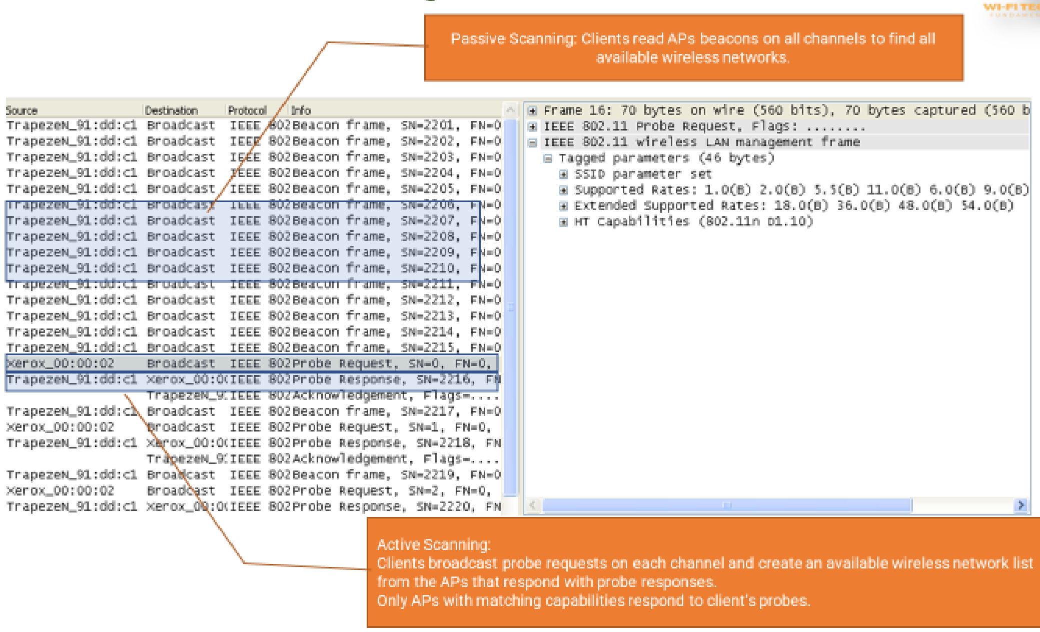
1. The Station tries to locate an AP by transmitting probe request frames, and waits for a probe response frame from the AP.
2. The probe request frame can be a directed or a broadcast probe request.
3. The probe response frame from the AP is similar to the beacon frame.
4. Based on the response from the AP, the client makes a decision about connecting to the AP

Note: These scanning procedures are used by wireless LAN clients (such as laptops and smartphones) to find a list of available wireless networks

Scanning: Scanning is a fundamental process in Wi-Fi networks that involves discovering and identifying available networks. This is particularly crucial when a device wants to join a Wi-Fi network or roam between different access points within the same network. The scanning process helps devices gather information about nearby networks, including their SSIDs, signal strength, and security protocols.

Active and Passive Scanning:

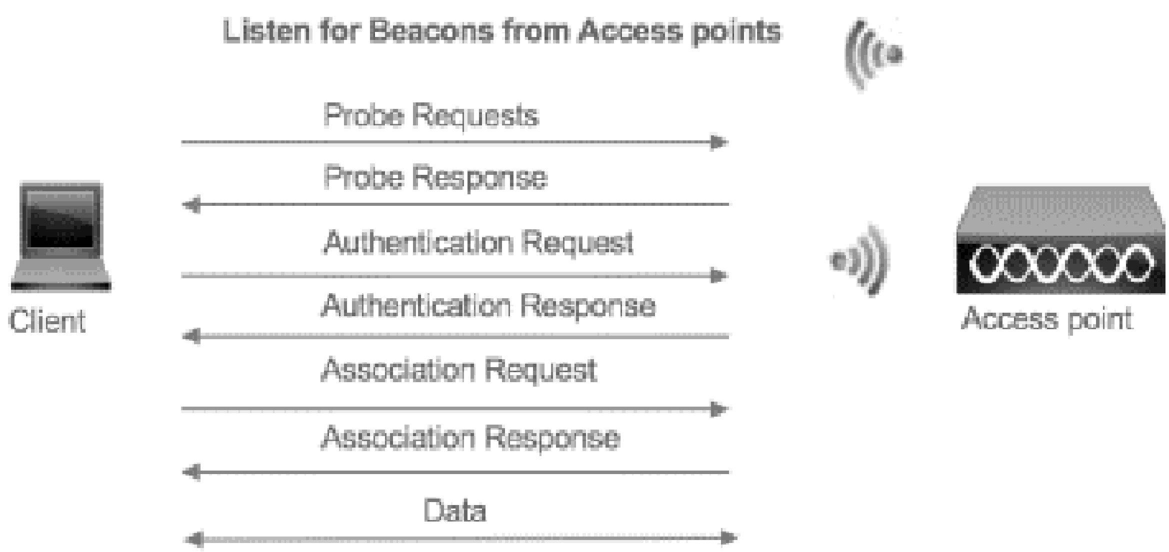
Active and Passive Scanning



Active Scanning: In active scanning, the client device takes a proactive role in discovering networks. It does so by sending out probe requests to potential access points. These probe requests essentially inquire about the presence of specific networks. Active scanning is more power-intensive for the client device, as it actively participates in seeking available networks.

Passive Scanning: On the other hand, passive scanning is a less power-consuming method. Here, the client device listens for beacon frames that are periodically broadcasted by nearby access points. These beacon frames contain essential information about the network, such as SSID, BSSID, and supported data rates. Passive scanning allows devices to create a list of available networks without actively transmitting probe requests.

Simple Client Connection



Introduction to Client Connection Process:

The initial step involves understanding how a client connects to an access point. The basic connection process includes the following steps.

Beacons: The access point (AP) sends out beacons to announce its presence in the network.

Probe Request:The client creates a list of available networks and sends a probe request.

Probe Response:The access point responds to the probe request with a probe response.

- **Authentication:**

Following the probe process, authentication becomes crucial, akin to a student entering a campus requiring ID verification.

Basic Authentication: In the basic Dole standard, a simple exchange of authentication request and response occurs.

Authentication Methods: Mention of more complex authentication methods to be covered in the next module.

- **Frame Formats and Headers:**

Detailed information on frame formats, headers, and the intricacies of the exchange will be covered in the next session.

- **Association Request:**

Once authentication is complete, the client decides to connect and sends an association request.

Unicast Frame:The association request is a unicast frame, specifically directed to the chosen access point.

- **Association Response:**

The access point responds to the association request with an association response.

Issuance of Association ID:The association response includes the issuance of an association ID, similar to receiving a token in a restaurant scenario.

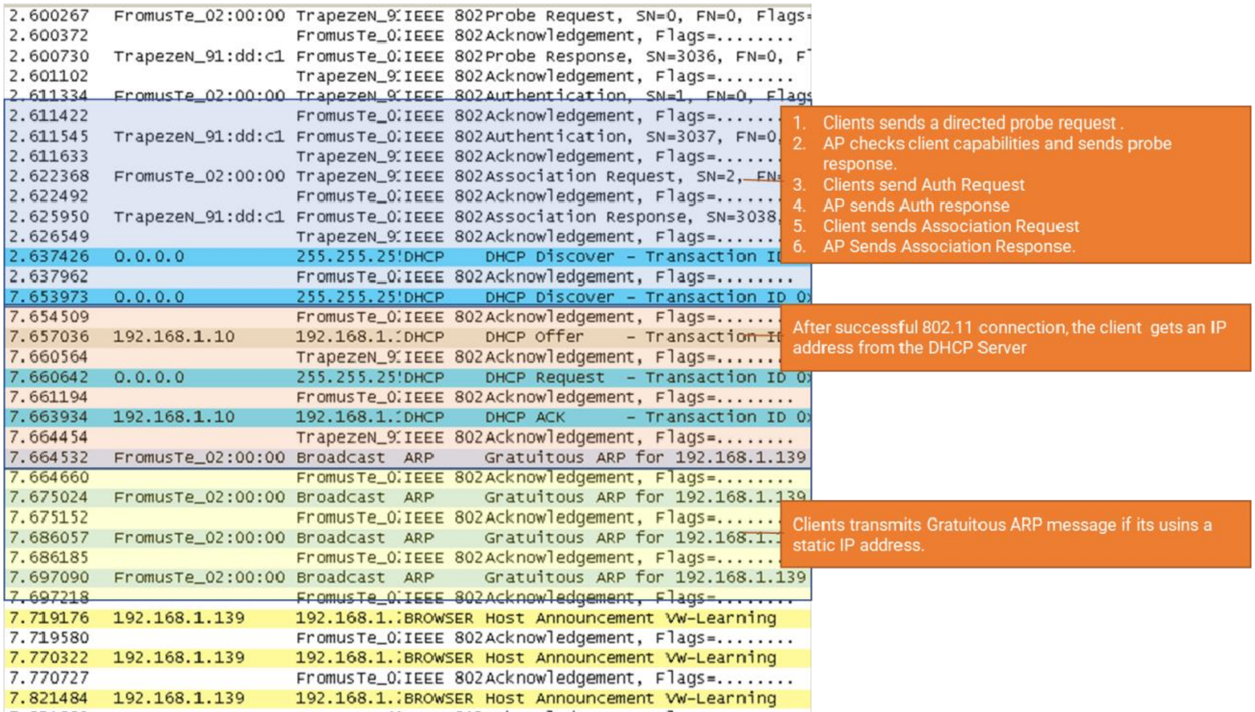
- **Commitment and Connection**:

After receiving the association response, the client commits to connecting to the access point.

- **Session Token Analogy:**

Drawing an analogy to a restaurant scenario, where paying money results in receiving a token for the specific session.

Simple Client Connection and Data Transfer:



Overview of Basic Client Connection Process:

Observed steps in the Wireshark capture, including:

Probe Request and Acknowledgment: Client initiates a probe request, and the access point acknowledges it.

Probe Response: The access point sends a probe response in reply to the client's request.

- **Authentication Phase:**

The authentication phase is highlighted as a crucial step in the connection process.

Authentication Request and Response:Explanation of the authentication request and response frames exchanged between the client and the access point.

- **Association Phase:**

Detailing the association phase, where the client officially associates with the access point.

Association Request and Response:Description of the frames involved in the association request and response, leading to the client being associated with the access point.

- **Connection Status:**

Clarification that when the client is associated with the access point, it signifies a connection at the Wi-Fi level, but not necessarily internet connectivity.

- **Transition to Internet Connectivity:**

Explaining that after the basic connection, there is a subsequent process for internet connectivity.

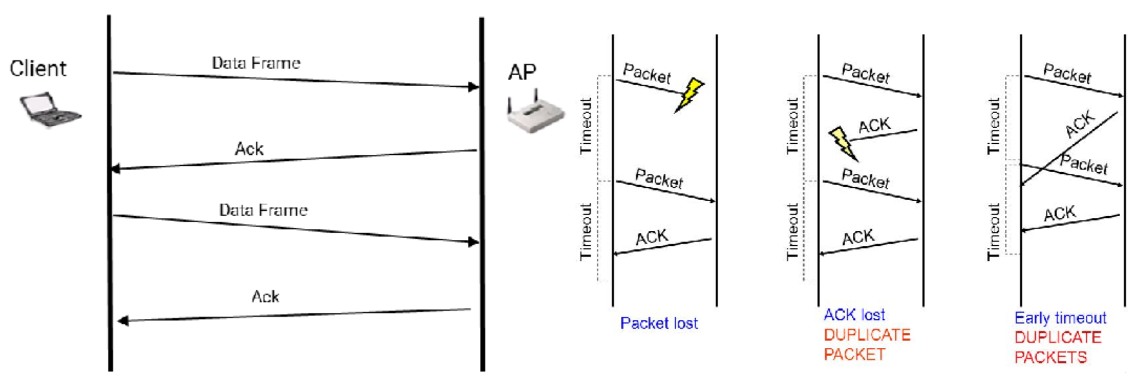
Obtaining IP Address:The client, having no IP address after association, connects to the DHCP server to obtain one.

DHCP Server Location:Highlighting that the DHCP server can exist on the Wi-Fi access point or elsewhere in the network, depending on the network setup.

- **Data Transfer:**

After obtaining an IP address, the client can send and receive data.

Data Transfer and Retries



Introduction to Data Transmission:

The transition from the client connection process to the actual data transmission, comparing it to a teacher starting to teach after enrollments and security handshakes are completed.

- **Wireless Medium Challenges:**

The challenges in a Wi-Fi medium, including potential issues like range, interference, multipath, modulation, and Signal-to-Noise Ratio (SNR).

- **Stop and Wait Protocol:**

Explaining the concept of the stop and wait protocol, an acknowledgement-based protocol used in Wi-Fi for reliable data transmission.

Packet Transmission and Acknowledgement:Describing how the client sends a data packet to the access point and waits for an acknowledgement.

Timeout and Retransmission:The presence of a timeout, and if an acknowledgement is not received within a specified time, the client assumes packet loss and retransmits.

Retransmission Limit:Highlighting that there is a limit on the number of retransmissions before giving up on a particular data frame.

- **Analogy to Postal System:**

Drawing an analogy to the postal system, where letters with acknowledgments are used to explain the stop and wait protocol.

- **Reasons for Retries:**

Exploring various reasons why retries may occur in the stop and wait protocol.

Packet Loss:The basic scenario where the transmitted packet doesn't reach the receiver due to channel conditions or SNR issues.

Lost Acknowledgement:Acknowledgement is sent by the receiver but gets lost, leading to retransmission.

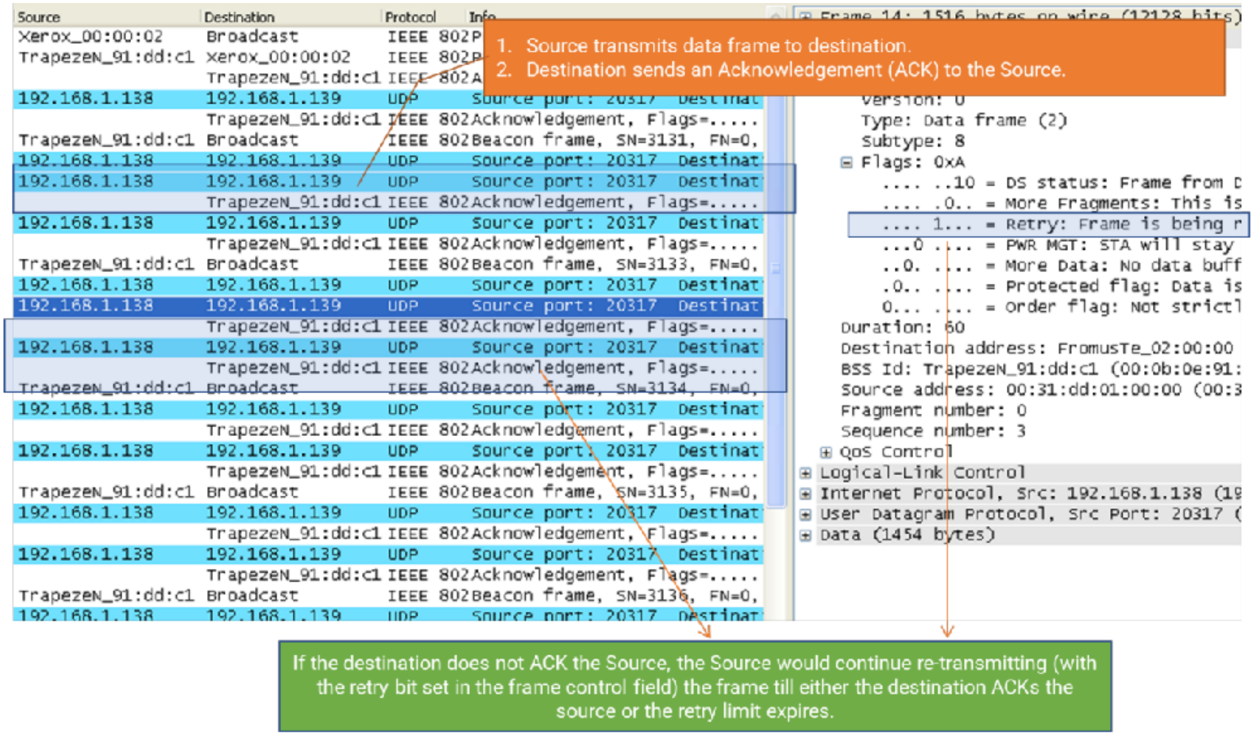
Delayed Acknowledgement:Acknowledgement arrives at the sender after the timeout, causing retransmission.

- **Retransmission Handling:**

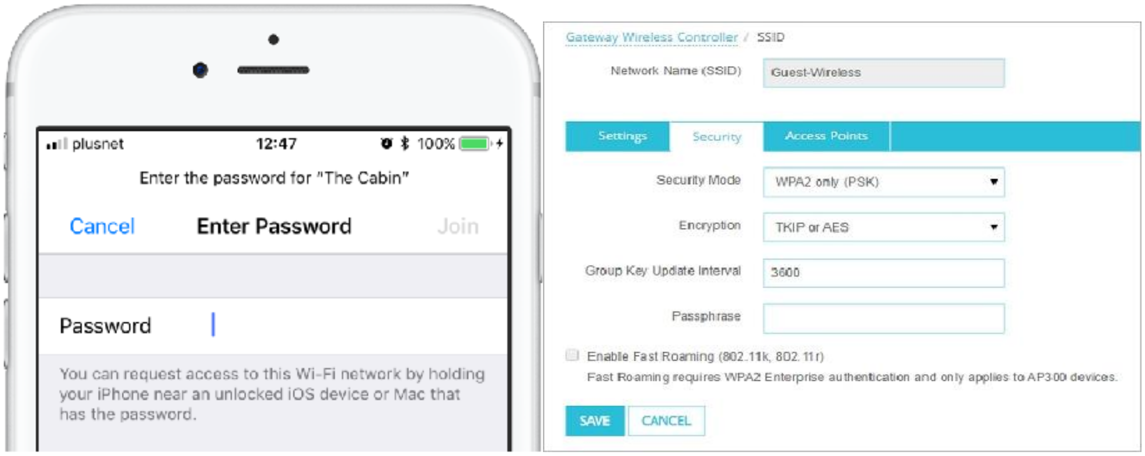
An explanation of how retransmissions are handled, including setting a "retrive" flag to identify duplicate packets.

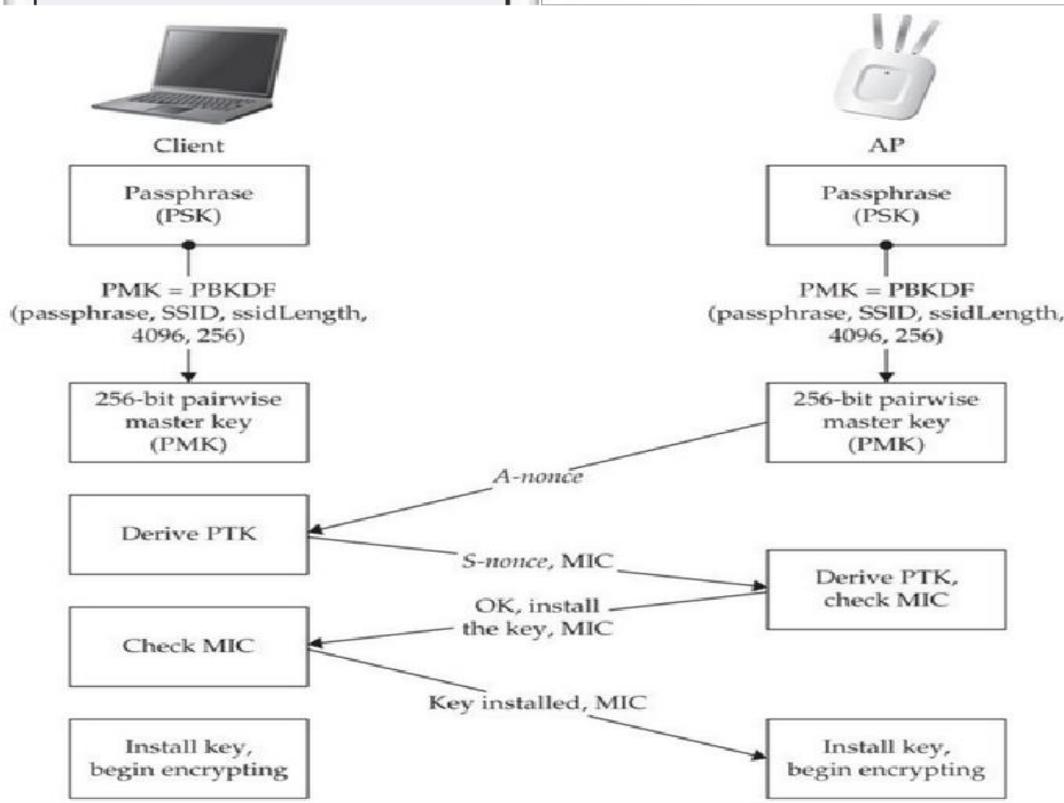
- **Packet Capture:**

Mentioning a quick packet capture illustrating the process of retransmissions.


Source
Destination
Protocol
Info
1. Source transmits data frame to destination.
2. Destination sends an Acknowledgement (ACK) to the Source.
Type: Data frame (2)
Subtype: 8
Flags: 0xA
.... ..10 = DS status: Frame from D
.... .0.. = More Fragments: This is
.... 1... = Retry: Frame is being r
...0 .... = PWR MGT: STA will stay
..0. .... = More Data: No data buff
.0.. .... = Protected flag: Data is
0... .... = Order flag: Not strictl
Duration: 60
Destination address: FromusTe_02:00:00
BSS Id: TrapezeN_91:dd:c1 (00:0b:0e:91:
Source address: 00:31:dd:01:00:00 (00:3
Fragment number: 0
Sequence number: 3
QoS Control
Logical-Link Control
Internet Protocol, Src: 192.168.1.138 (19
User Datagram Protocol, Src Port: 20317 (
Data (1454 bytes)
If the destination does not ACK the Source, the Source would continue re-transmitting (with the retry bit set in the frame control field) the frame till either the destination ACKs the source or the retry limit expires.

Connection with Basic Personal Security





Security in Wi-Fi Networks:

The common scenario where Wi-Fi networks have security enabled, emphasizing that most networks are not open.

Open Networks:Acknowledging that open networks are less common, and connecting to them means immediate internet access without a password.

Password-Protected Networks:Describing the more common scenario where networks require a password for access.

- **Password Entry and Authentication:**

The process of connecting to a password-protected network, involving obtaining and entering the network's password.

Access Point Configuration:Noting that the access point's user interface allows users to enable security features and set a password.

Mutual Authentication:Emphasizing the importance of mutual authentication, ensuring both the client and access point authenticate each other.

- **Key Generation for Encryption:**

The concept of key generation for encryption once mutual authentication is established.

Secondary Keys or Session Keys: Describing the process of using the entered password to generate secondary keys or session keys for encrypting the traffic.

- **Dual Aspects of Security:**

Highlighting the dual aspects of security in Wi-Fi connections: authentication and encryption.

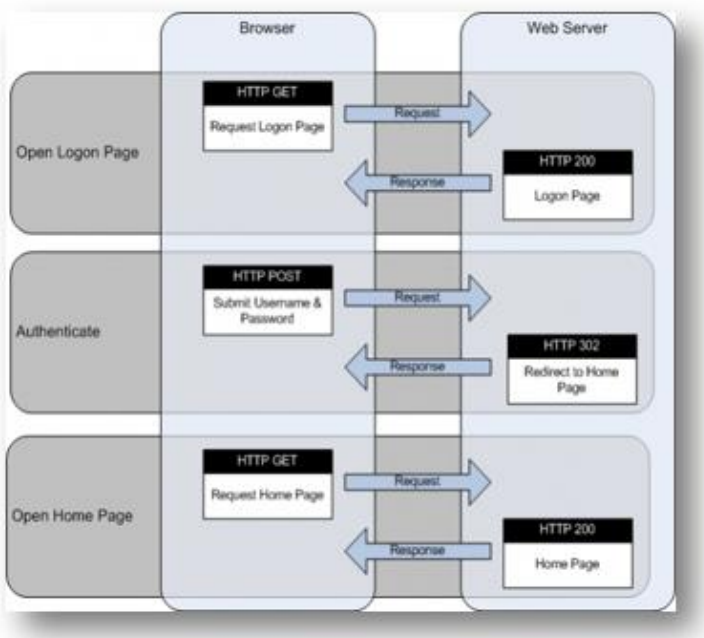
Authentication:Briefly mentioning that authentication ensures the legitimacy of the client and access point.

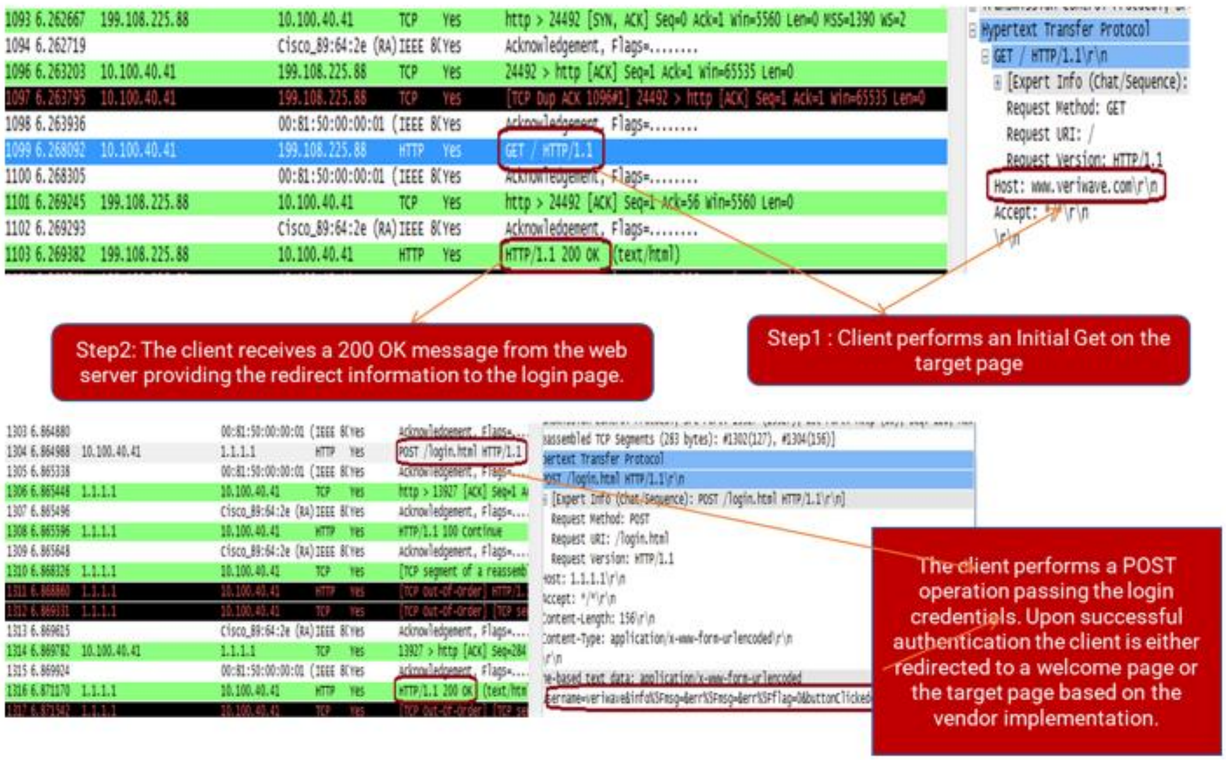
Encryption:Discussing the need for encryption to secure the communication between the client and access point.

Connection using Browser

This can be understood through an example. Suppose we are attempting to connect to the Wi-Fi provided by a hotel. Initially, we select the access point SSID and click on 'Connect.' However, instead of our usual browser, we get redirected to a captive portal page. This redirection occurs because, at first, we are only connected to the Wi-Fi service, not the network itself. To establish a connection with the network, we must fill in the details on the displayed captive portal.


HOTEL WiFi
Login
Signup
Please choose a plan
Check Email
High Speed Access
One Month Unlimited Access
One Week Internet Access
Type your details
Room
Last Name
I accept the terms of use
Signup


Browser
Web Server
Open Logon Page
HTTP GET
Request Logon Page
Request
Response
HTTP 200
Logon Page
Authenticate
HTTP POST
Submit Username & Password
Request
Response
HTTP 302
Redirect to Home Page
Open Home Page
HTTP GET
Request Home Page
Request
Response
HTTP 200
Home Page

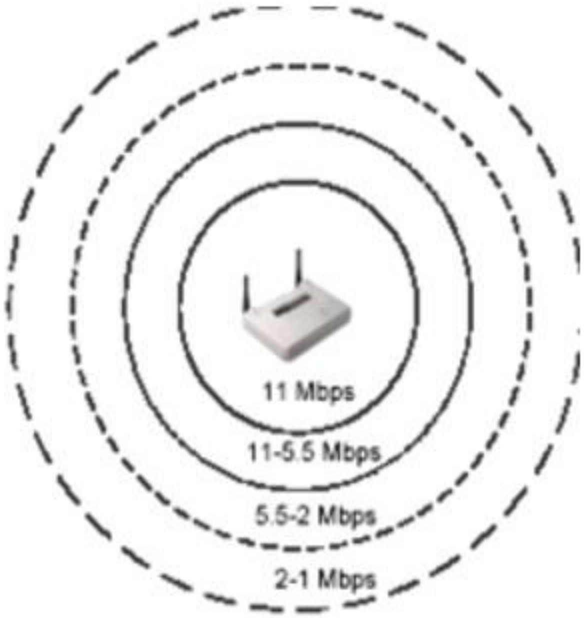


Rate Adaptation

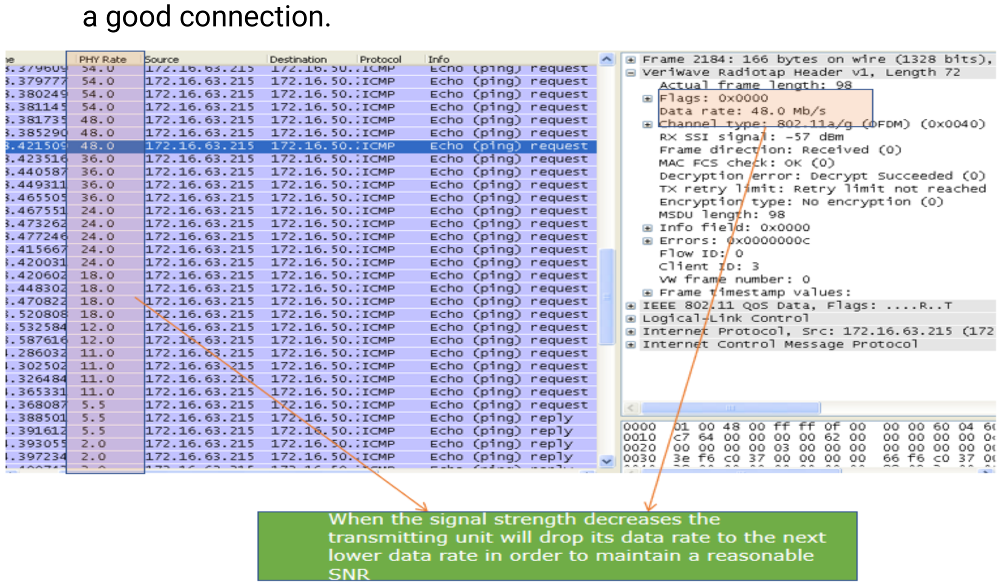
- As we know , rate adaptation involves how the access point maintains a connection to the station at various distances. When the station is very close, the access point aims to transmit at the highest possible data rate (MCS rate) to maximize throughput while ensuring a reliable connection.

- However, as the distance increases, the signal-to-noise ratio drops, making it challenging to sustain higher modulation rates. This is where a rate adaptation algorithm comes into play. The transmitter decides when to drop to a lower data rate based on the channel conditions.

- For instance, if the transmitter sends a data packet and receives an acknowledgment, indicating a good channel, it continues at the current rate. However, if acknowledgments are not received, suggesting a possible distance increase or channel problem, the transmitter adapts by trying a lower MCS rate. It iteratively adjusts the data rate until it finds a reliable connection with optimal throughput.

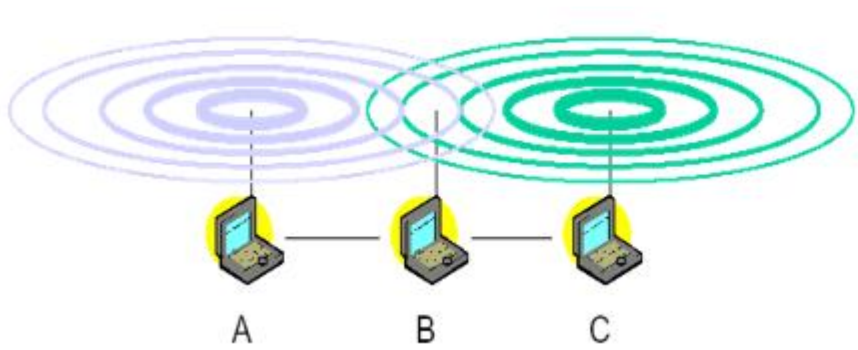


- In the picture, you can see a situation where the access point is having some difficulty keeping a good connection. It starts by trying to send data at a fast speed of 54 megabits per second (Mbps), but it's not getting acknowledgments, which are like signals saying, "I got your message." Since it's not getting these signals, it thinks there might be a problem, maybe the device it's trying to connect with moved farther away.
- So, to figure out the best way to communicate, the access point decides to slow down how fast it's sending data. It keeps trying slower and slower speeds—like going from a fast car to a slower one—to see if it can find a speed where it gets those acknowledgments, ensuring a stable connection. This process is what we call rate adaptation, and it shows how the system adjusts to the changing conditions to maintain a good connection.



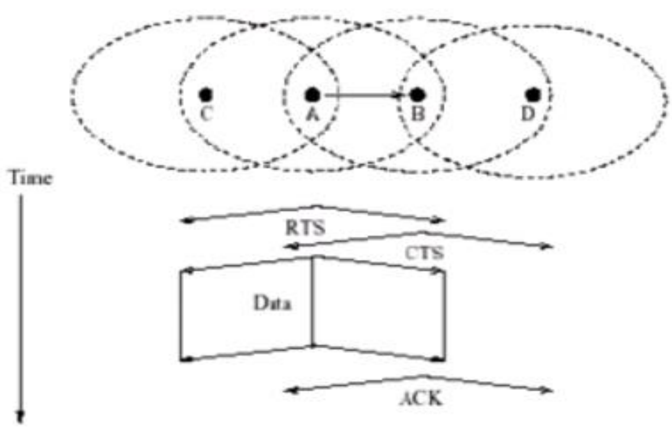
Carrier Sensing

Physical Carrier Sensing



- Uses CSMA/CA scheme
- Each station detects activity on the channel by analyzing the signal from other clients in the network
- All the clients connected to the same AP are considered to be in a common contention zone
- If a station is not able to detect any signal then it assumes that none of the other stations are transmitting and starts transmitting
- This scheme faces hidden terminal problem

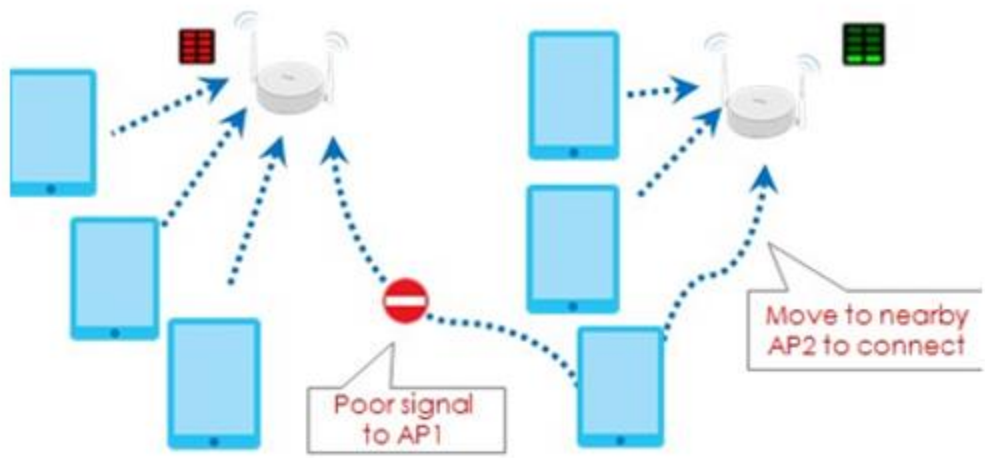
Virtual Carrier Sensing



- This scheme uses CTS and RTS
- When a MS wants to transmit data, it sends an RTS packet which includes the source, destination and the duration of the following transaction
- Destination responds with CTS which includes the same duration information
- All stations receiving either CTS or RTS set their NAV for the given duration and don't try to transmit for that time
-

Load Balancing and Band Steering

Load Balancing



- Imagine a college facing a scheduling challenge; they have a rule that each classroom can only accommodate 30 students per teacher, creating a student-to-teacher ratio of 30 to 1. Now, let's say an additional 10 students enroll. This situation poses a management problem – they must figure out how to handle this exceeding capacity. They might need to place the extra 10 students in a different classroom or even create a new one. This process of organizing and distributing students to maintain an optimal learning environment is akin to what we call "load balancing."

- Now, in the realm of Wi-Fi and access points, there's a similar concept of load balancing. If there are too many devices connected to a particular access point, it might become overloaded. To address this, the access point can refuse to connect new devices and instead encourage them to connect to a neighboring access point with less traffic. This process helps distribute the load more evenly across different access points, ensuring better performance for all connected devices.

- Load balancing, in essence, is about efficiently managing the distribution of devices across multiple access points to prevent overcrowding and maintain a smooth network experience. It's a critical aspect of network management, just like the college managing its classrooms to ensure an effective learning environment.

Band Steering

- In Wi-Fi networks, there are different frequency bands, like 2.4 GHz, 5 GHz, and 6 GHz. Each band offers a varying amount of radio spectrum. For instance, 2.4 GHz has a limited spectrum with fewer non-overlapping channels, typically using 20 MHz channel bandwidth. On the other hand, 5 GHz provides more flexibility, allowing for 40 and 80 MHz channel bandwidths. The 6 GHz band offers even more spectrum.

- Now, when devices connect to an access point, the access point can analyze the situation. If a device supports the 5 GHz band and there aren't many devices connected in that band, the access point might decide to steer that device from the 2.4 GHz band to the 5 GHz band. This steering action is known as "band steering."

- Band steering is a function that helps optimize the use of available spectrum and manage the connection of devices across different frequency bands. The access point's decision on when and how to perform band steering depends on the algorithms and metrics it uses.

Legacy Protection and Greenfield Mode

- Legacy protection helps new and older Wi-Fi devices to communicate with each other.
- It ensures that when fast Wi-Fi devices are using a network, the slower devices are told to wait for their turn.
- This makes sure that the network works smoothly for all devices, whether they're fast or slow.

Green Field Mode:

- Green field mode is like creating a special lane on a road only for fast cars.
- In Wi-Fi, it means the network is set up only for the newest devices to use.
- This allows the fastest devices to use the network without being slowed down by the older, slower devices.

These features in Wi-Fi networks help ensure that all devices, new and old, can use the network without causing any problems for each other.

Power Management:

- Power management helps Wi-Fi devices save their battery so they can work for longer without needing a recharge. It's like putting your phone on power-saving mode to make the battery last longer.

Dynamic Frequency Selection (DFS):

- DFS helps Wi-Fi devices avoid interfering with radar systems that use the same radio frequencies. It's like making sure your Wi-Fi doesn't disrupt other important communication happening nearby.

WLAN Roaming

Wireless Local Area Network (WLAN) Roaming is the process through which a device shifts its connection from one wireless access point to another as it moves within a network. This mechanism ensures continuous connectivity without interruptions, enabling devices to maintain a seamless connection to the network while in motion. During roaming, the device constantly searches for the best available signal strength to ensure a stable connection throughout its movement within the network.
A lot more detail about WLAN roaming will be covered in the next sessions.