Wi-Fi Technology Fundamentals

WI-FI TECHNOLOGY
FUNDAMENTALS COURSE

Module-3

WLAN MAC Layer

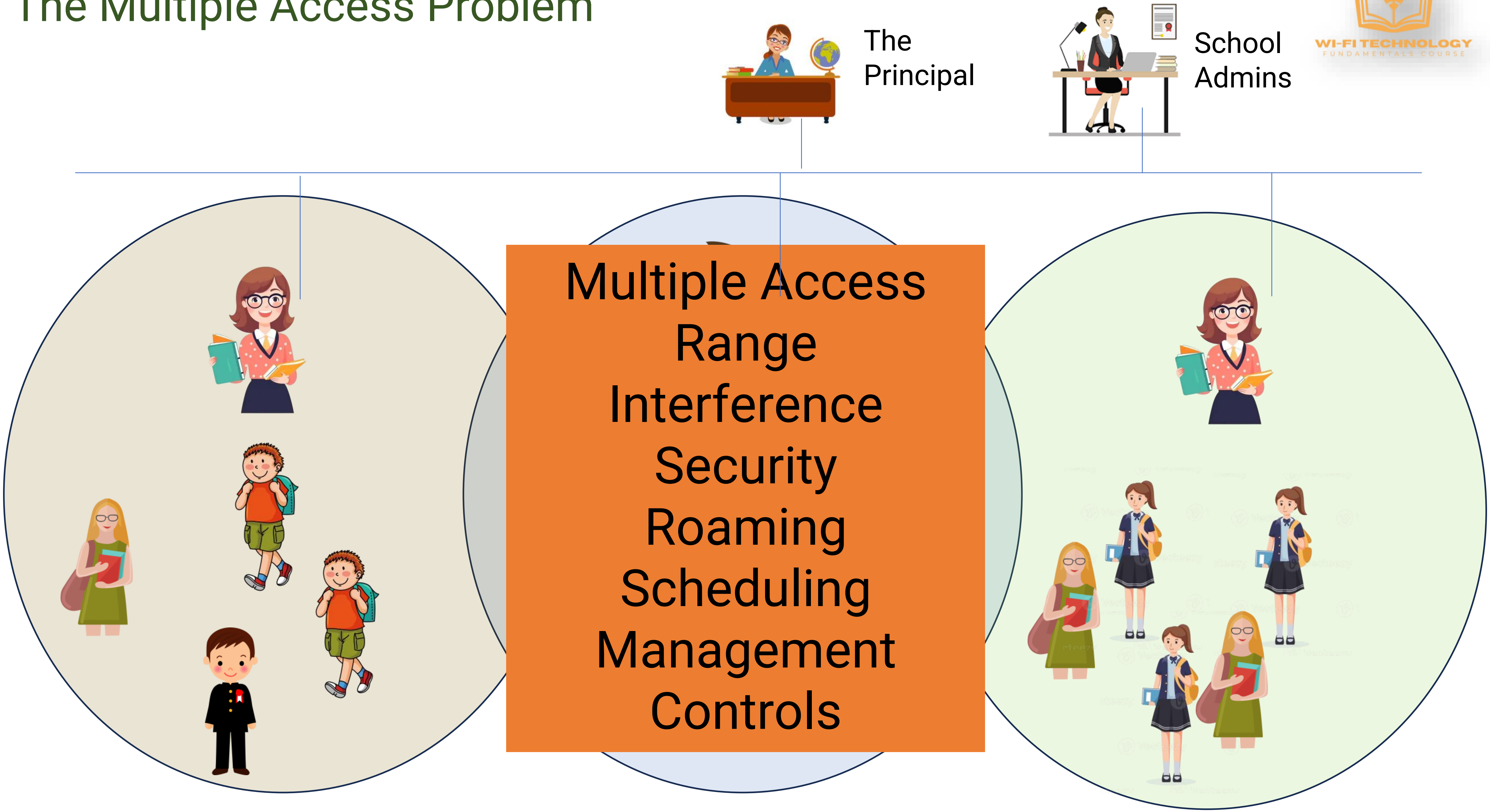
Session-3a

Basic AP Management and Control Functions

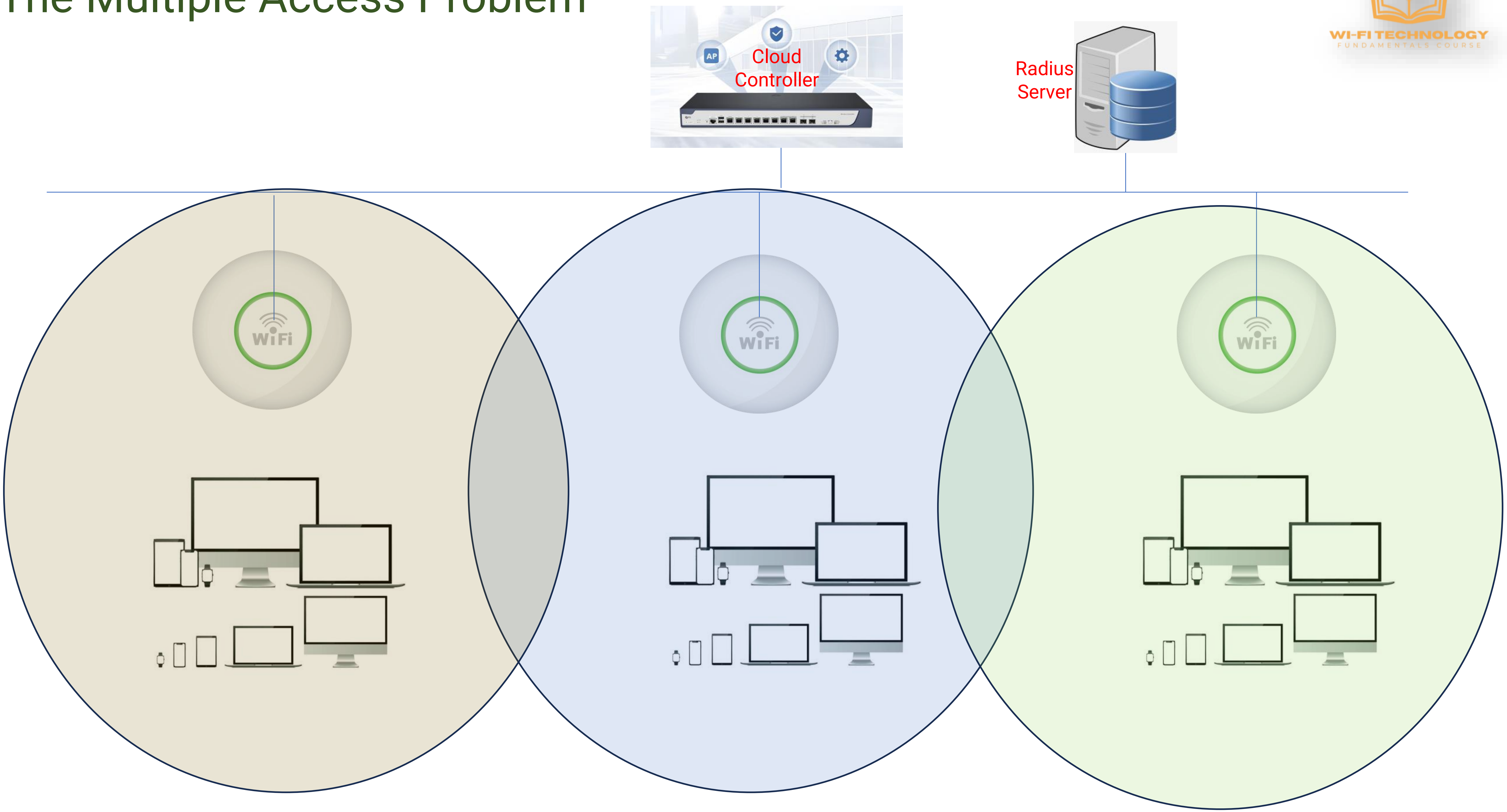
Recap …..
Module 2: WLAN Physical Layer

- Frequency Allocation and Modulation Basics
  - ISM and UNII Bands, unlicensed spectrum allocation, channels, Channel BW, Spread spectrum, OFDM
- Modulation/Coding, MIMO Basics
  - Modulation and Coding Rates, Multipath, MIMO, OFDM, RSSI, SNR, EVM, Spectral Efficiency
- MCS Table, PHY Data Rates
  - PHY Data rates, MCS Table, Theoretical Throughput
- PHY Headers and key functions
  - PHY Headers, PCLP and PMD Sub Layers, Key PHY later functions

The Multiple Access Problem



The Multiple Access Problem



The Food Court Experience

1. Rough scan all the restaurants in the food court
2. More detailed scan, check the menus.
3. Check how long it will take food to arrive and how busy the restaurant is.
4. Figure out which restaurant you like.
5. Place the order and pay the money
6. Enjoy the food and leave

What is a Beacon Frame?

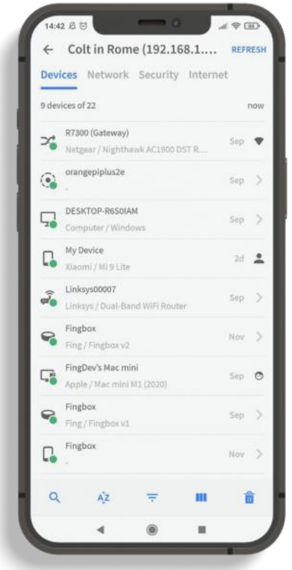
A periodic Message Broadcast
once every 100mses

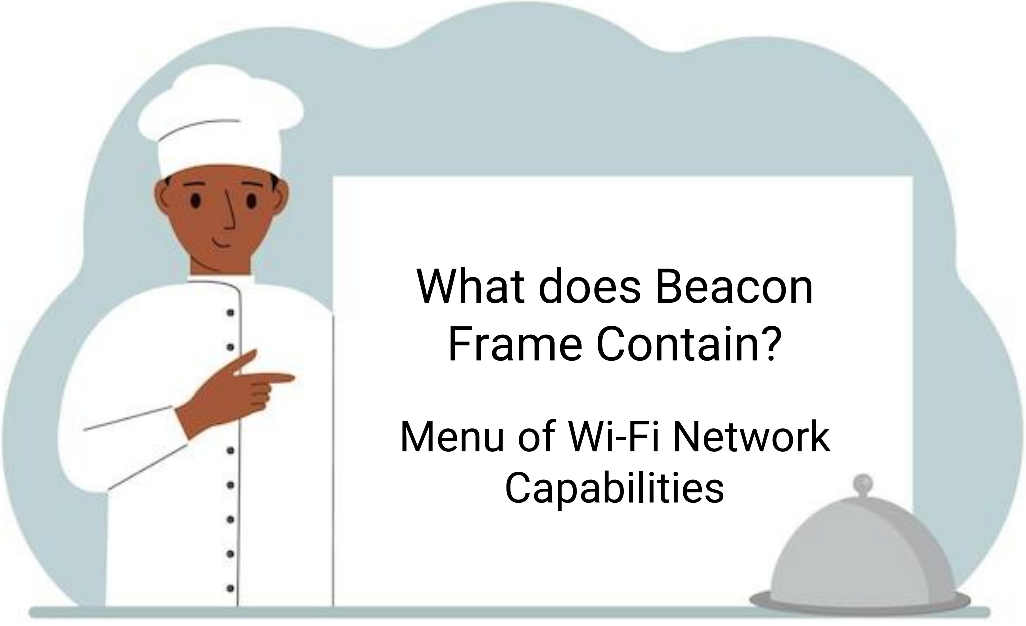
WNIC
(No WiFi)

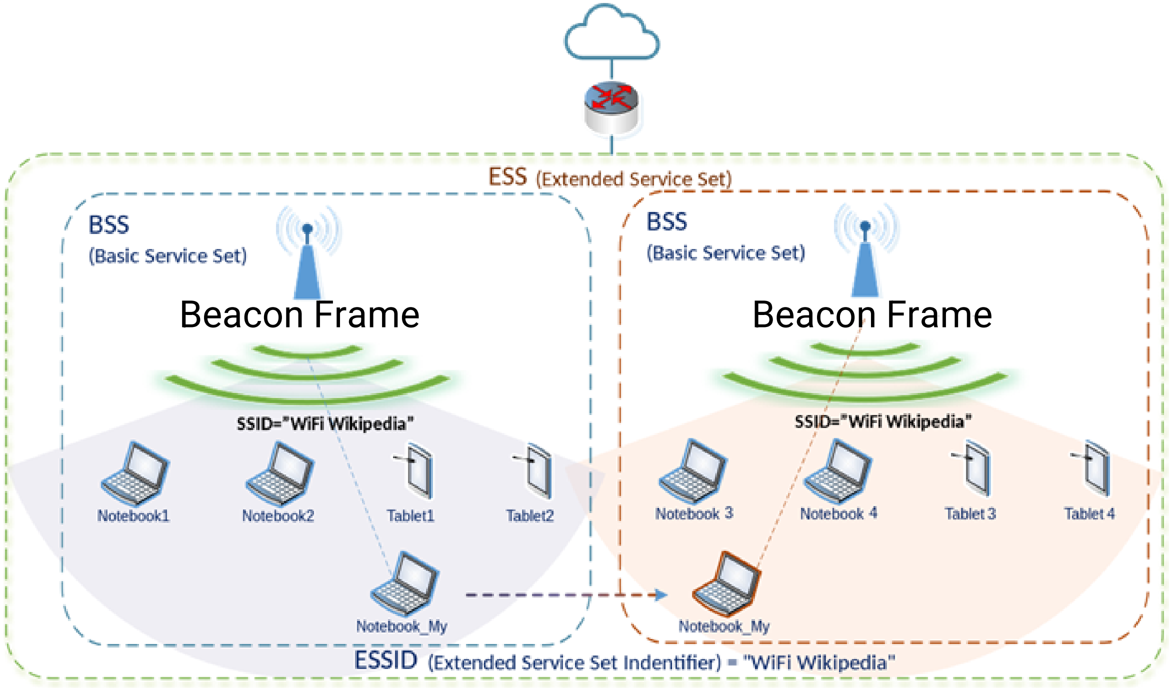
WNIC
(No WiFi)

AP

WNIC
(No WiFi)







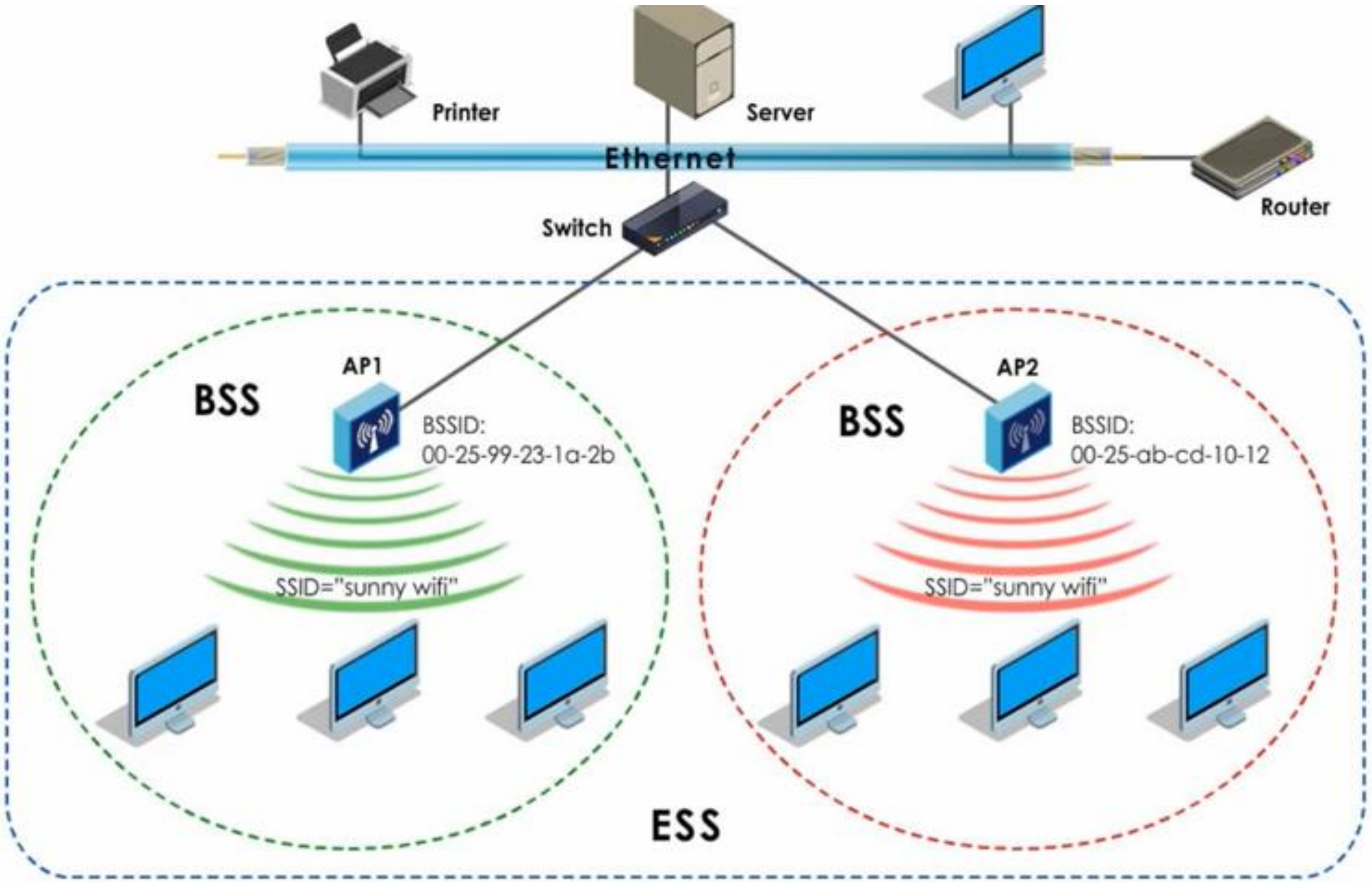
SSID and BSSID

SSID (Service Set Identifier)

- Name of a wireless network
- Can exist on several physical APs
- Device identifies network by this name

BSSID(Basic Service Set Identifier)

- Unique identifier for a specific access point within a wireless network.
- Distinguishes between multiple access points sharing the same SSID.
- BSSID helps devices pinpoint the exact access point to connect to.



The Various functions of an Access Point

Management Plane

- Advertise Capabilities
- Connection Management
- Security Management
- Mobility Management
- Load Management
- Power Management
- QoS Management
- Channel Management
- Multiple Access Management

Control Plane

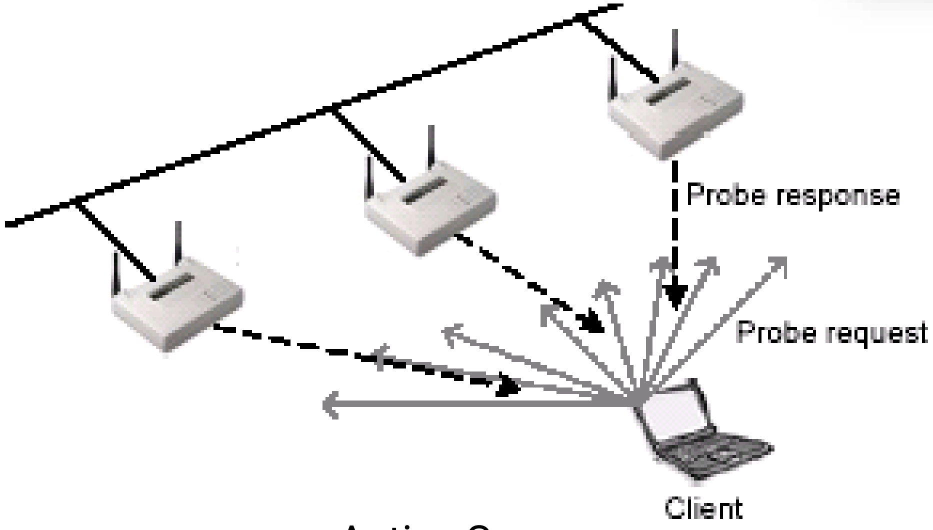
- Flow Control
- Power Save Control
- Medium Access Control

Data Plane

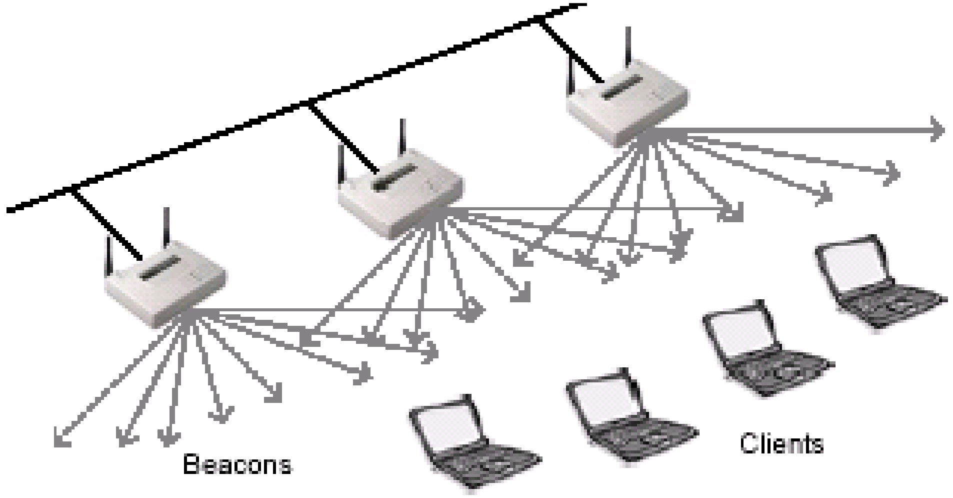
- Data Transmission

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



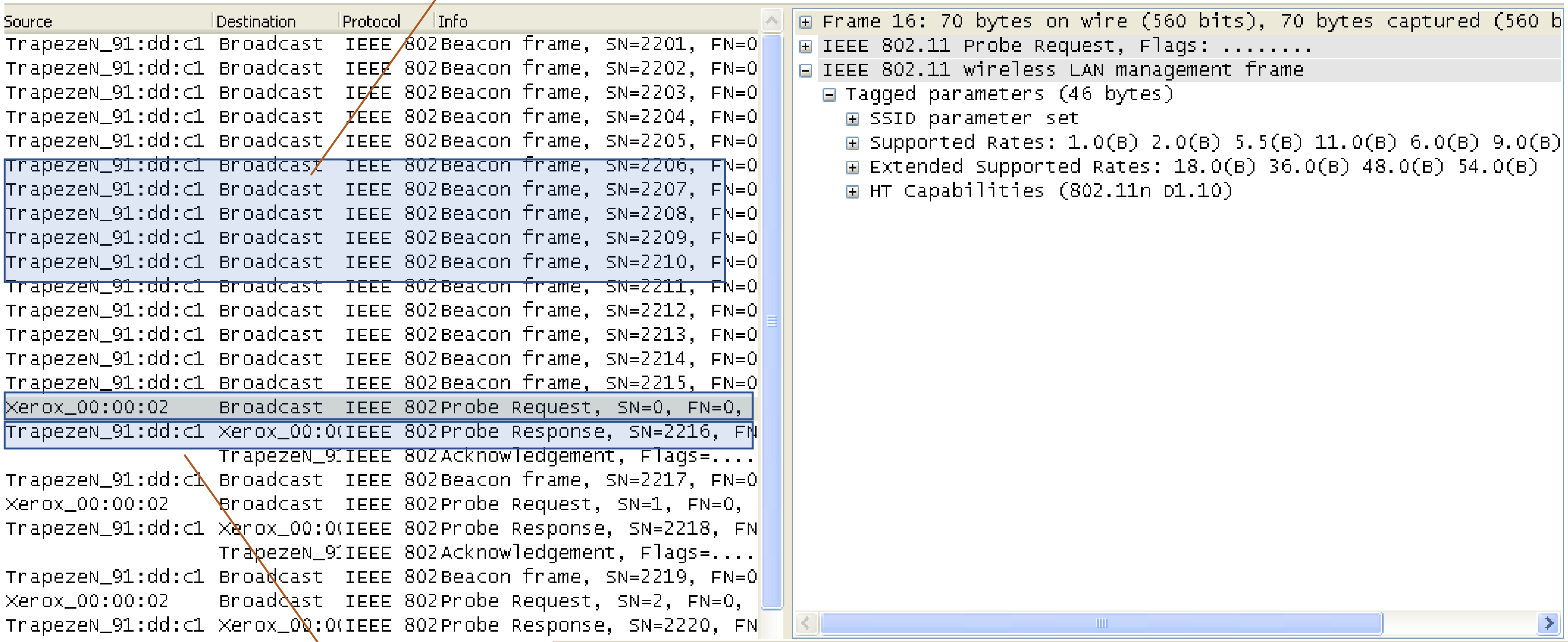
Passive Scan

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

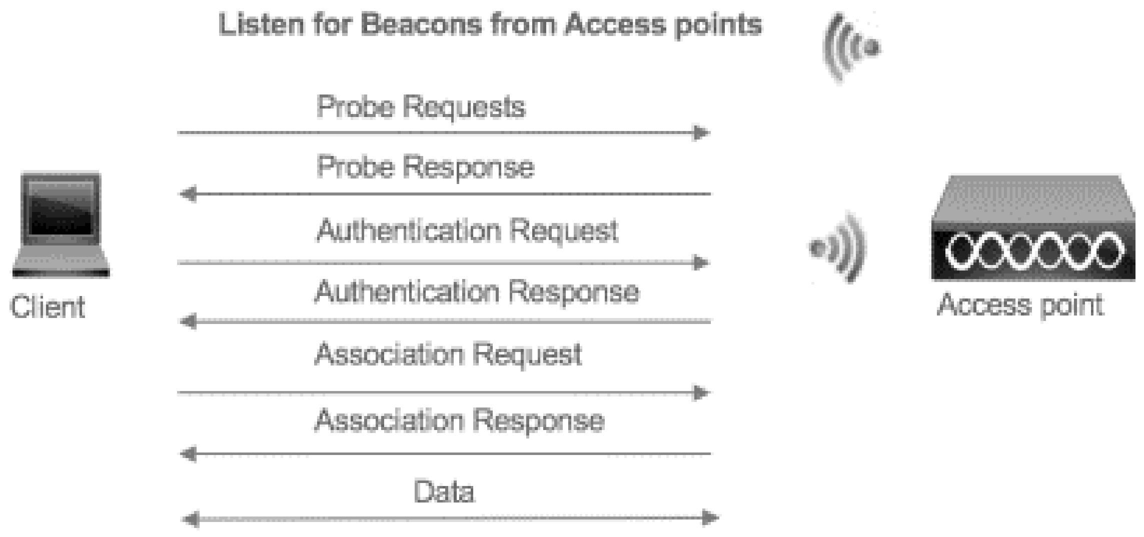
Active and Passive Scanning

Passive Scanning: Clients read APs beacons on all channels to find all available wireless networks.



Active Scanning:
Clients broadcast probe requests on each channel and create an available wireless network list from the APs that respond with probe responses.
Only APs with matching capabilities respond to client’s probes.

Simple Client Connection



Beacons: The access point periodically sends a beacon frame to announce its presence and relay many information that is required by the stations to connect to the wireless network
Probe Request: A station sends probe requests to discover 802.11 networks within its proximity. Probe requests advertise the stations supported data rates and 802.11 capabilities such as 802.11n.
Probe Response: Access point receiving the probe request check to see if the station has at least one common supported data rate. If they share a common data rate, a probe response is sent advertising the SSID, supported data rates, encryption types if required, and other 802.11 capabilities of the access point.
Authentication Request: The station chooses a SSID/network from the probe responses it receives. It also checks the compatibility on encryption type. Once compatible networks are discovered the station will attempt low-level 802.11 authentication with compatible access points. The station sends a low-level 802.11 authentication frame to an AP setting the authentication to open and the sequence to 0x0001.
Authentication Response: The access point receives the authentication frame and responds to the station with authentication frame set to open indicating a sequence, If an access point receives any frame other than an authentication or probe request from a station that is not authenticated it will respond with a Deauthentication frame placing the mobile into an unauthenticated an unassociated state. The station will have to begin the association process from the low level authentication step. At this point the station is authenticated but not yet associated.
Association Request : Once the station determines which access point it would like to associate to, it will send an association request to that access point. The association request contains chosen encryption types and other compatible 802.11 capabilities.
Association Response: If the elements of association request match the capabilities of the access point, it will create an Association ID for the mobile station and respond with an association response with a success message granting network access to the mobile station.
Data: At this stage the connection is established and the station is successfully associated to the access point and is ready for data transfer

Source: https://wifibond.com/2017/04/08/802-11-association-process/

Simple Client Connection and Data Transfer

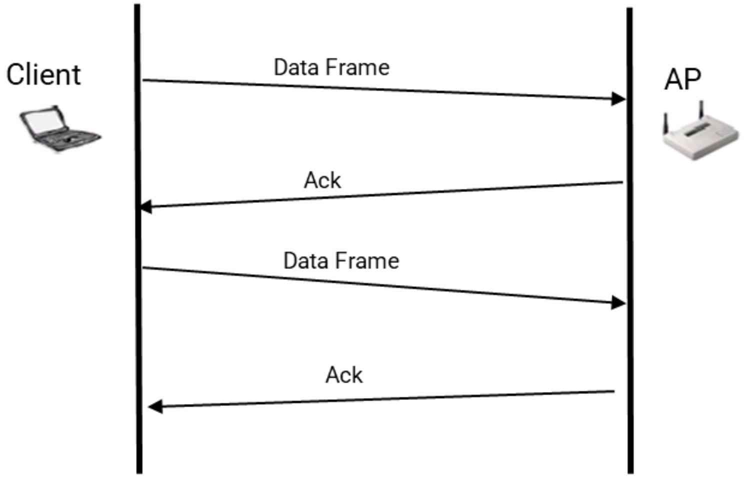
2.600267	FromusTe_02:00:00	TrapezeN_9…	IEEE 802	Probe Request, SN=0, FN=0, Flags=
2.600372		FromusTe_0…	IEEE 802	Acknowledgement, Flags=........
2.600730	TrapezeN_91:dd:c1	FromusTe_0…	IEEE 802	Probe Response, SN=3036, FN=0, F
2.601102		TrapezeN_9…	IEEE 802	Acknowledgement, Flags=........
2.611334	FromusTe_02:00:00	TrapezeN_9…	IEEE 802	Authentication, SN=1, FN=0, Flags
2.611422		FromusTe_0…	IEEE 802	Acknowledgement, Flags=.......
2.611545	TrapezeN_91:dd:c1	FromusTe_0…	IEEE 802	Authentication, SN=3037, FN=0,
2.611633		TrapezeN_9…	IEEE 802	Acknowledgement, Flags=.......
2.622368	FromusTe_02:00:00	TrapezeN_9…	IEEE 802	Association Request, SN=2, FN=
2.622492		FromusTe_0…	IEEE 802	Acknowledgement, Flags=.......
2.625950	TrapezeN_91:dd:c1	FromusTe_0…	IEEE 802	Association Response, SN=3038,
2.626549		TrapezeN_9…	IEEE 802	Acknowledgement, Flags=.......
2.637426	0.0.0.0	255.255.25…	DHCP	DHCP Discover - Transaction ID
2.637962		FromusTe_0…	IEEE 802	Acknowledgement, Flags=........
7.653973	0.0.0.0	255.255.25…	DHCP	DHCP Discover - Transaction ID 0x
7.654509		FromusTe_0…	IEEE 802	Acknowledgement, Flags=.......
7.657036	192.168.1.10	192.168.1.…	DHCP	DHCP Offer - Transaction ID
7.660564		TrapezeN_9…	IEEE 802	Acknowledgement, Flags=.......
7.660642	0.0.0.0	255.255.25…	DHCP	DHCP Request - Transaction ID 0x
7.661194		FromusTe_0…	IEEE 802	Acknowledgement, Flags=........
7.663934	192.168.1.10	192.168.1.…	DHCP	DHCP ACK - Transaction ID 0x
7.664454		TrapezeN_9…	IEEE 802	Acknowledgement, Flags=........
7.664532	FromusTe_02:00:00	Broadcast	ARP	Gratuitous ARP for 192.168.1.139
7.664660		FromusTe_0…	IEEE 802	Acknowledgement, Flags=........
7.675024	FromusTe_02:00:00	Broadcast	ARP	Gratuitous ARP for 192.168.1.139
7.675152		FromusTe_0…	IEEE 802	Acknowledgement, Flags=.......
7.686057	FromusTe_02:00:00	Broadcast	ARP	Gratuitous ARP for 192.168.1.
7.686185		FromusTe_0…	IEEE 802	Acknowledgement, Flags=.......
7.697090	FromusTe_02:00:00	Broadcast	ARP	Gratuitous ARP for 192.168.1.139
7.697218		FromusTe_0…	IEEE 802	Acknowledgement, Flags=........
7.719176	192.168.1.139	192.168.1.…	BROWSER	Host Announcement VW-Learning
7.719580		FromusTe_0…	IEEE 802	Acknowledgement, Flags=........
7.770322	192.168.1.139	192.168.1.…	BROWSER	Host Announcement VW-Learning
7.770727		FromusTe_0…	IEEE 802	Acknowledgement, Flags=........
7.821484	192.168.1.139	192.168.1.…	BROWSER	Host Announcement VW-Learning

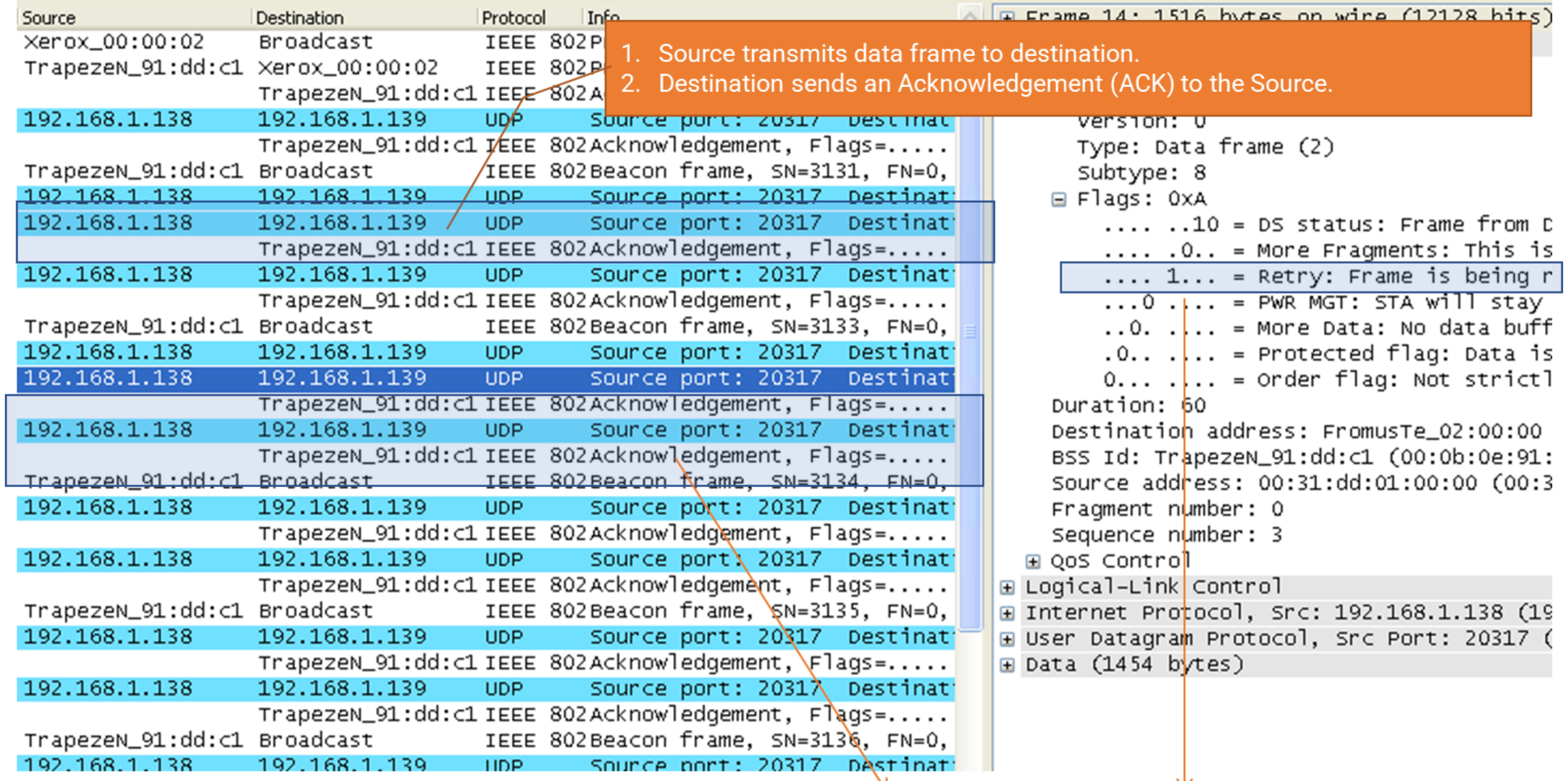
1. Clients sends a directed probe request .
2. AP checks client capabilities and sends probe response.
3. Clients send Auth Request
4. AP sends Auth response
5. Client sends Association Request
6. AP Sends Association Response.

After successful 802.11 connection, the client gets an IP address from the DHCP Server

Clients transmits Gratuitous ARP message if its usins a static IP address.

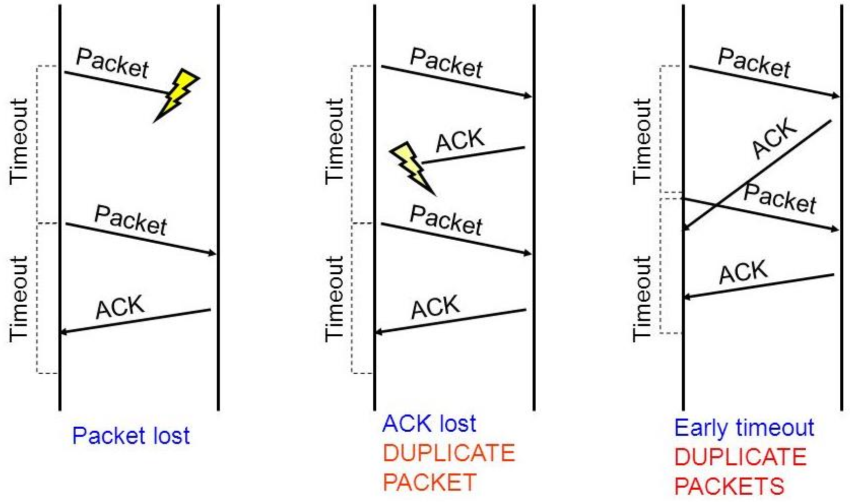
Data Transfer and Retries





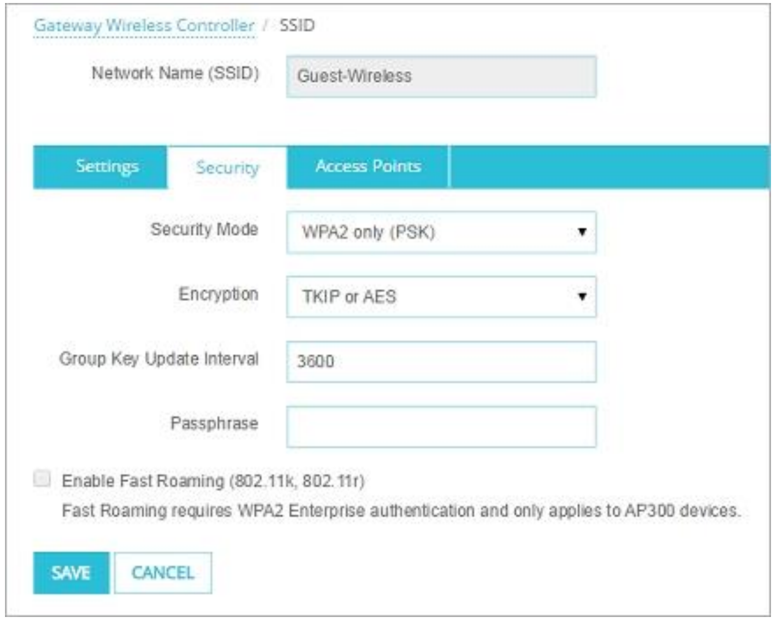
1. Source transmits data frame to destination.
2. Destination sends an Acknowledgement (ACK) to the Source.

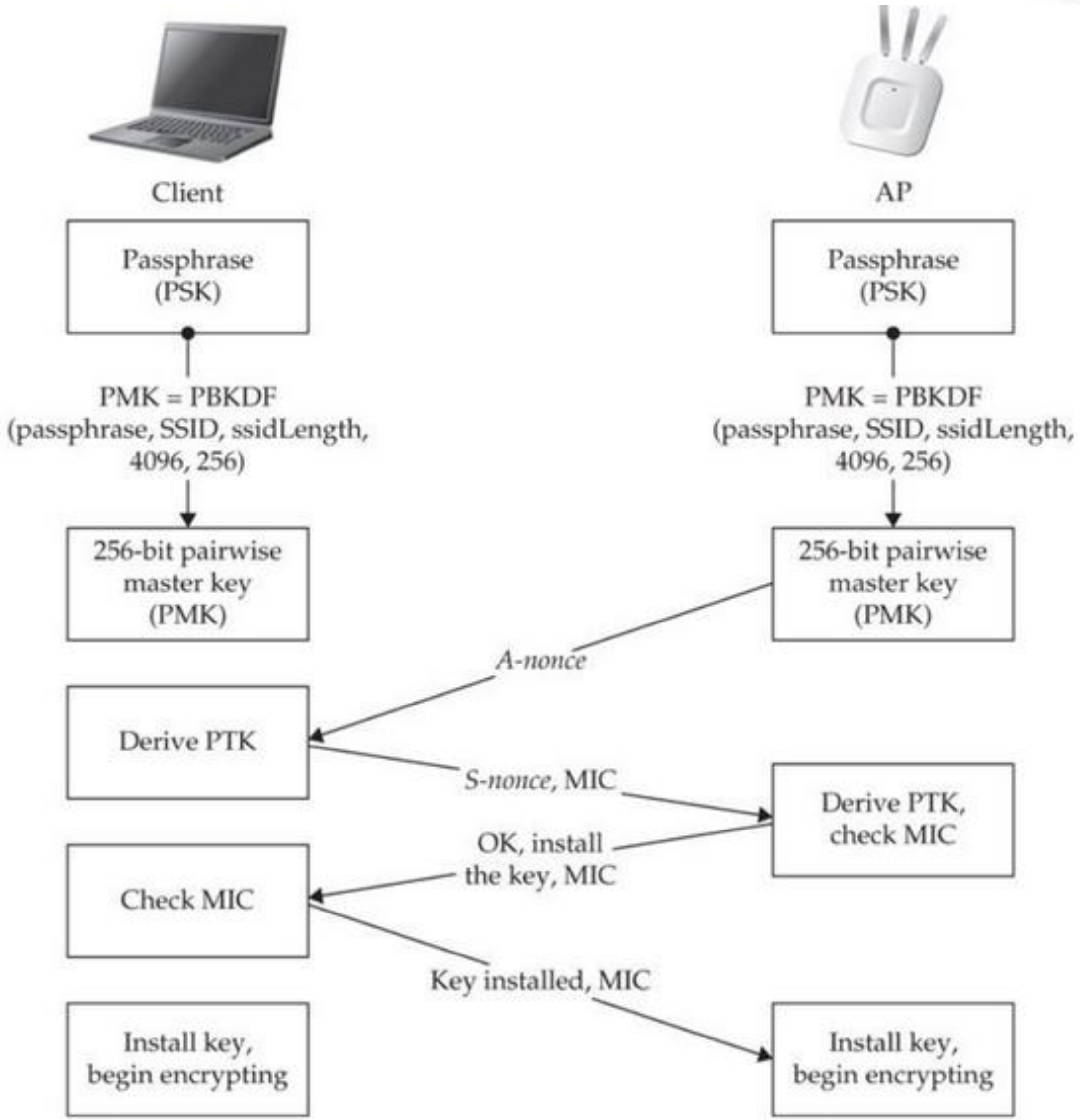
Why Retries?



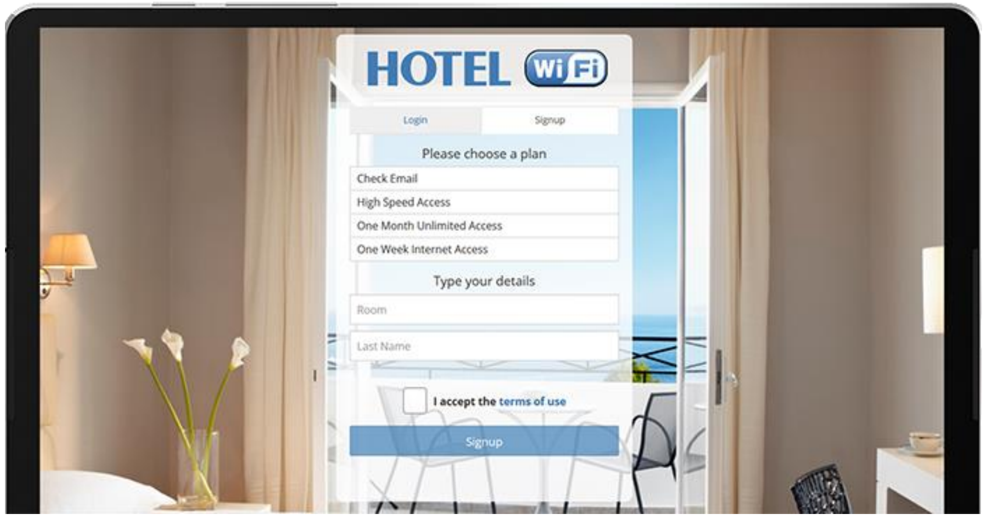
If the destination does not ACK the Source, the Source would continue re-transmitting (with the retry bit set in the frame control field) the frame till either the destination ACKs the source or the retry limit expires.

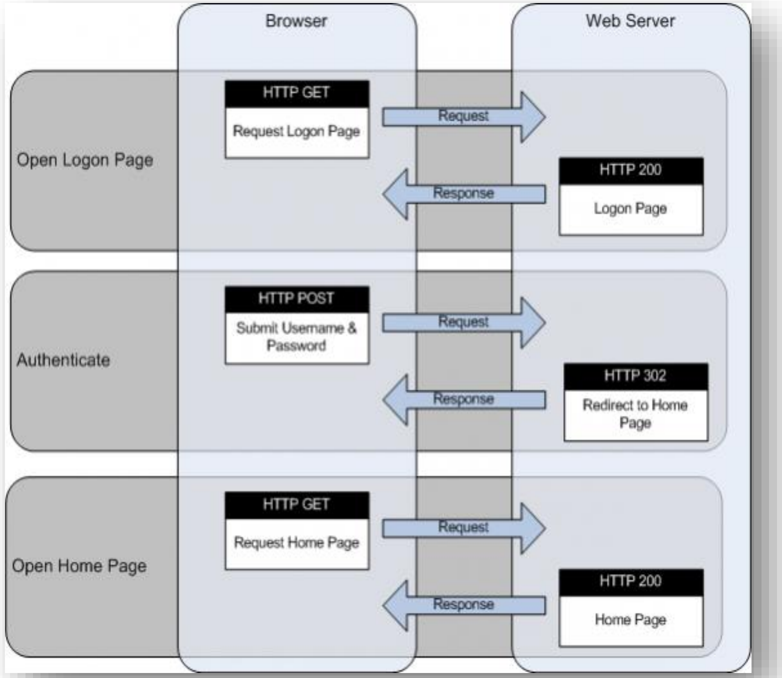
Connection with Basic Personal Security

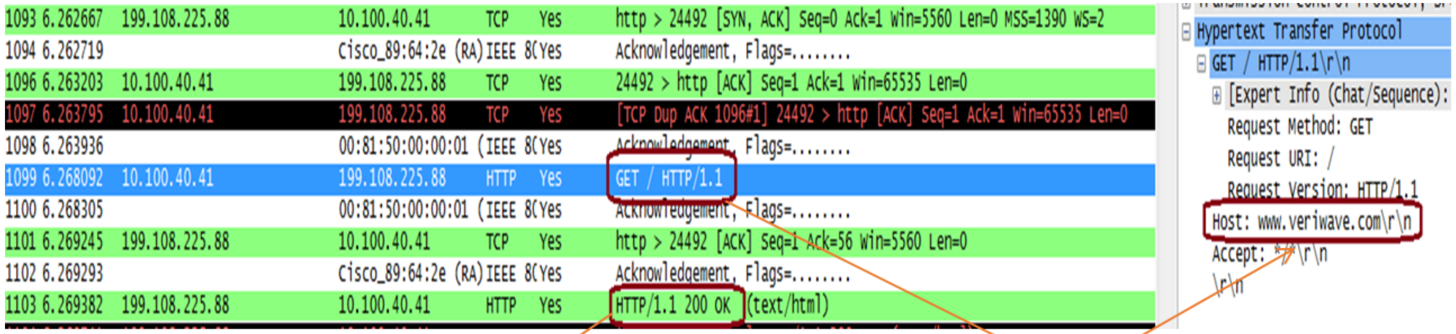




Connection using Browser

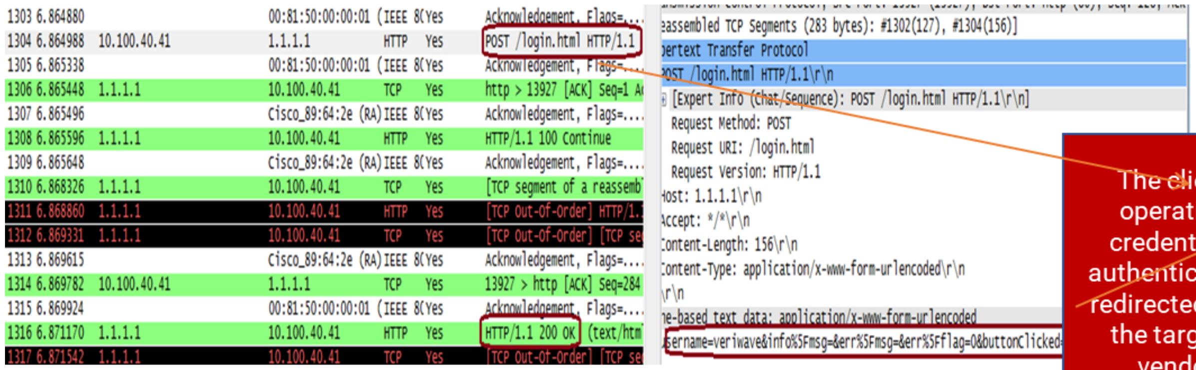






Step2: The client receives a 200 OK message from the web server providing the redirect information to the login page.

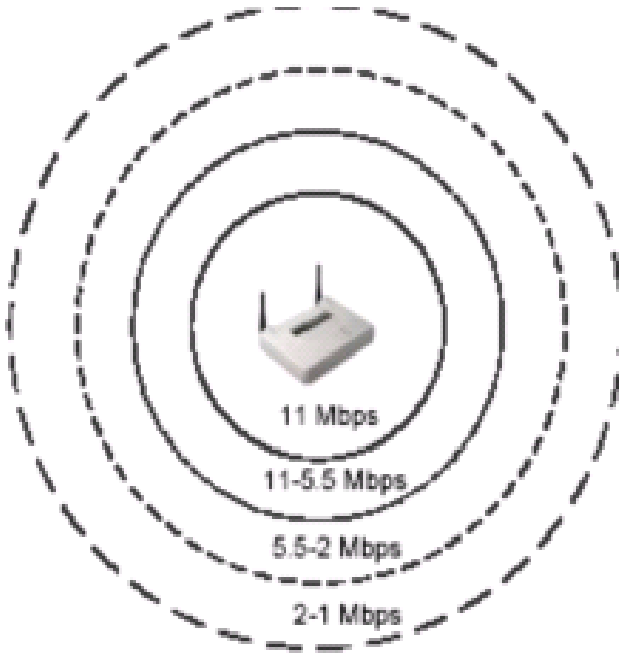
Step1 : Client performs an Initial Get on the target page

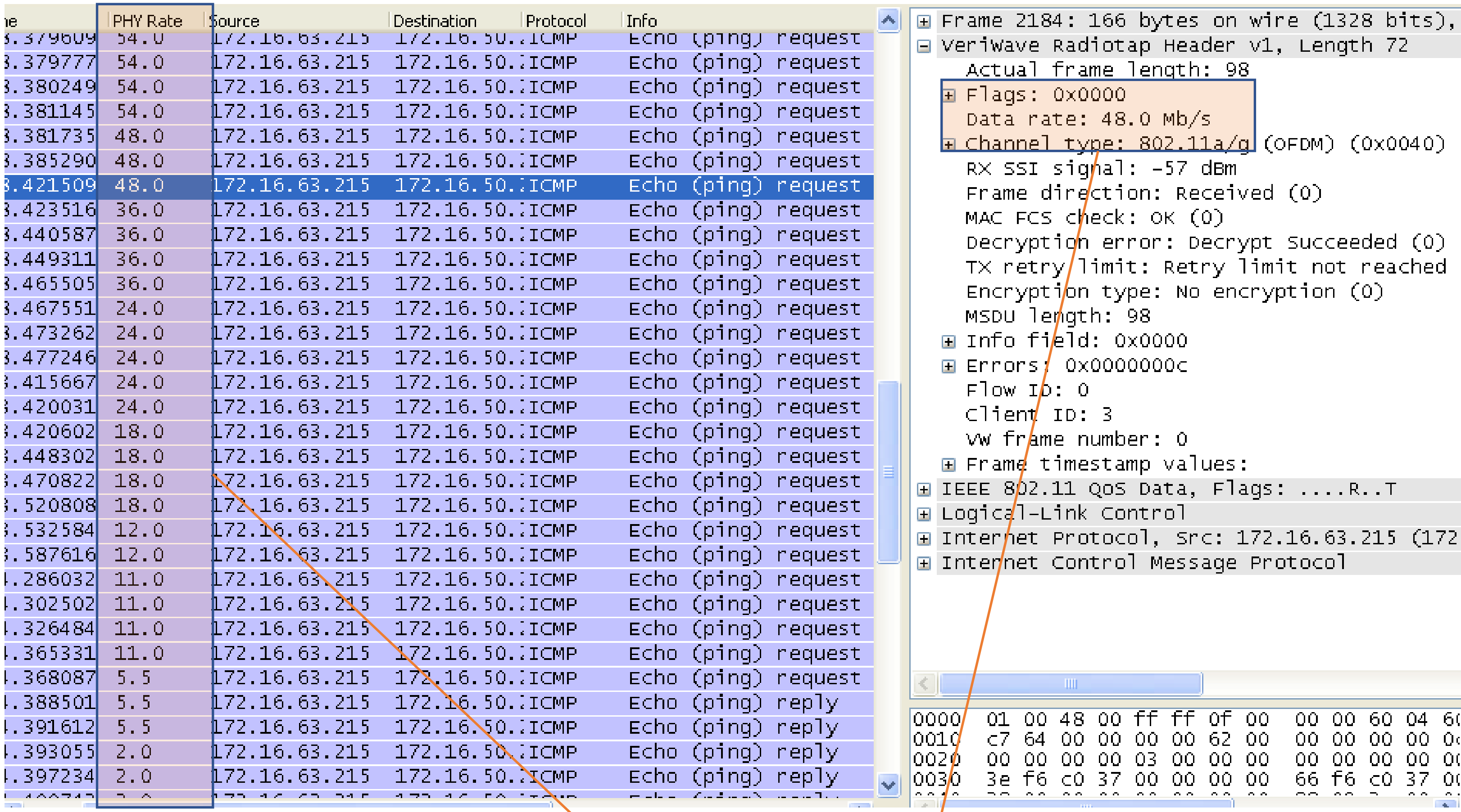


The client performs a POST operation passing the login credentials. Upon successful authentication the client is either redirected to a welcome page or the target page based on the vendor implementation.

Rate Adaptation

- Speed adjusted dynamically depending on the distance and the signal strength
- As the distance between the AP and the MS increases, the signal strength will decrease to a point where the current data rate cannot be maintained
- When the signal strength decreases the transmitting unit will drop its data rate to the next lower data rate in order to maintain a reasonable SNR



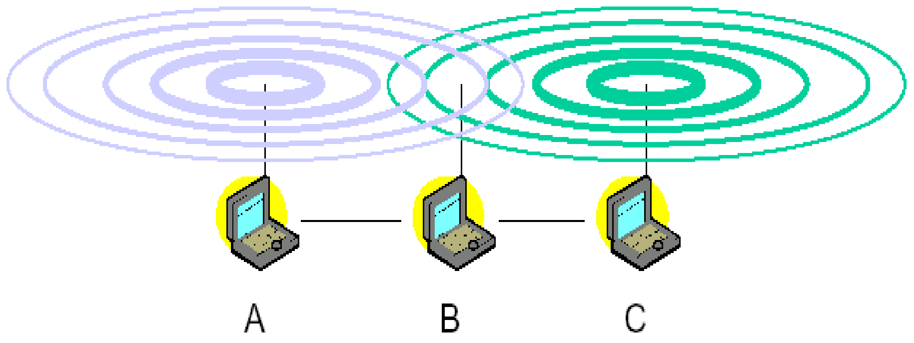


ne	PHY Rate	Source	Destination	Protocol	Info
3.379609	54.0	172.16.63.215	172.16.50.	ICMP	Echo (ping) request
3.379777	54.0	172.16.63.215	172.16.50.	ICMP	Echo (ping) request
3.380249	54.0	172.16.63.215	172.16.50.	ICMP	Echo (ping) request
3.381145	54.0	172.16.63.215	172.16.50.	ICMP	Echo (ping) request
3.381735	48.0	172.16.63.215	172.16.50.	ICMP	Echo (ping) request
3.385290	48.0	172.16.63.215	172.16.50.	ICMP	Echo (ping) request
3.421509	48.0	172.16.63.215	172.16.50.	ICMP	Echo (ping) request
3.423516	36.0	172.16.63.215	172.16.50.	ICMP	Echo (ping) request
3.440587	36.0	172.16.63.215	172.16.50.	ICMP	Echo (ping) request
3.449311	36.0	172.16.63.215	172.16.50.	ICMP	Echo (ping) request
3.465505	36.0	172.16.63.215	172.16.50.	ICMP	Echo (ping) request
3.467551	24.0	172.16.63.215	172.16.50.	ICMP	Echo (ping) request
3.473262	24.0	172.16.63.215	172.16.50.	ICMP	Echo (ping) request
3.477246	24.0	172.16.63.215	172.16.50.	ICMP	Echo (ping) request
3.415667	24.0	172.16.63.215	172.16.50.	ICMP	Echo (ping) request
3.420031	24.0	172.16.63.215	172.16.50.	ICMP	Echo (ping) request
3.420602	18.0	172.16.63.215	172.16.50.	ICMP	Echo (ping) request
3.448302	18.0	172.16.63.215	172.16.50.	ICMP	Echo (ping) request
3.470822	18.0	172.16.63.215	172.16.50.	ICMP	Echo (ping) request
3.520808	18.0	172.16.63.215	172.16.50.	ICMP	Echo (ping) request
3.532584	12.0	172.16.63.215	172.16.50.	ICMP	Echo (ping) request
3.587616	12.0	172.16.63.215	172.16.50.	ICMP	Echo (ping) request
1.286032	11.0	172.16.63.215	172.16.50.	ICMP	Echo (ping) request
1.302502	11.0	172.16.63.215	172.16.50.	ICMP	Echo (ping) request
1.326484	11.0	172.16.63.215	172.16.50.	ICMP	Echo (ping) request
1.365331	11.0	172.16.63.215	172.16.50.	ICMP	Echo (ping) request
1.368087	5.5	172.16.63.215	172.16.50.	ICMP	Echo (ping) request
1.388501	5.5	172.16.63.215	172.16.50.	ICMP	Echo (ping) reply
1.391612	5.5	172.16.63.215	172.16.50.	ICMP	Echo (ping) reply
1.393055	2.0	172.16.63.215	172.16.50.	ICMP	Echo (ping) reply
1.397234	2.0	172.16.63.215	172.16.50.	ICMP	Echo (ping) reply

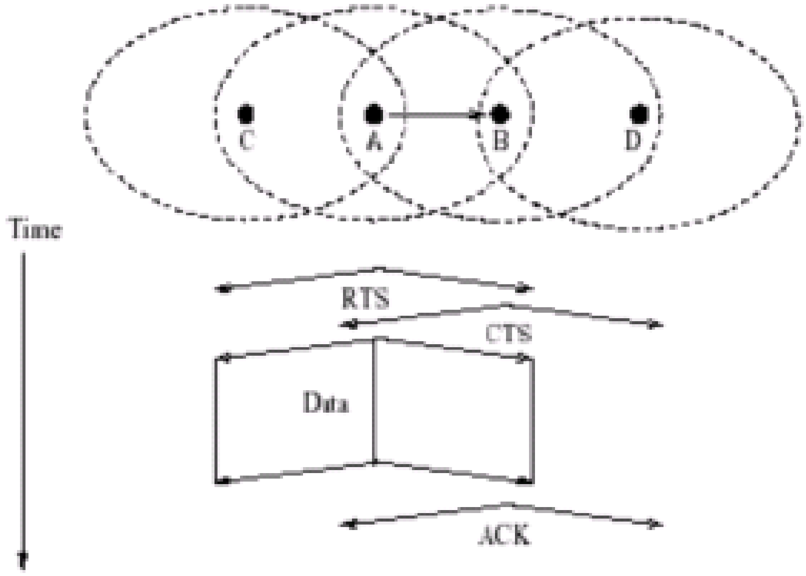
When the signal strength decreases the transmitting unit will drop its data rate to the next lower data rate in order to maintain a reasonable SNR

Carrier Sensing

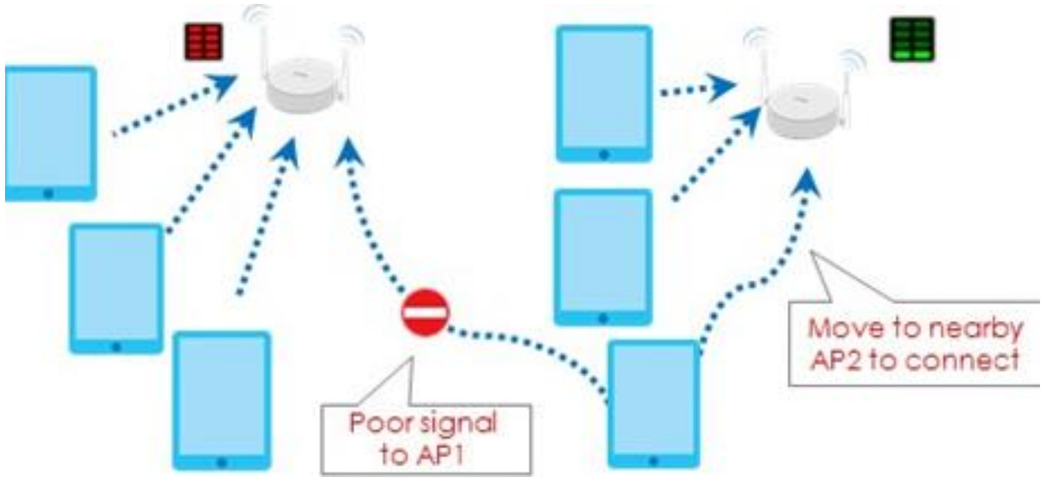
- Physical Carrier Sensing
  - Uses CSMA/CA scheme
  - Each station detects activity on the channel by analyzing the signal from other clients in the network
  - All the clients connected to the same AP are considered to be in a common contention zone
  - If a station is not able to detect any signal 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

- Important issue in areas of heavy traffic
- In multi-cell structure with heavy traffic, several co-located APs can cover the same region to increase the throughput
- The clients with load balancing functionality configured can automatically associate with the AP that is less loaded and provides the best quality of service

Band Steering

- 2.4GHz has lesser bandwidth and hence cannot support too many clients
- APs can choose to steer some clients from 2.4GHz to 5GHz band.

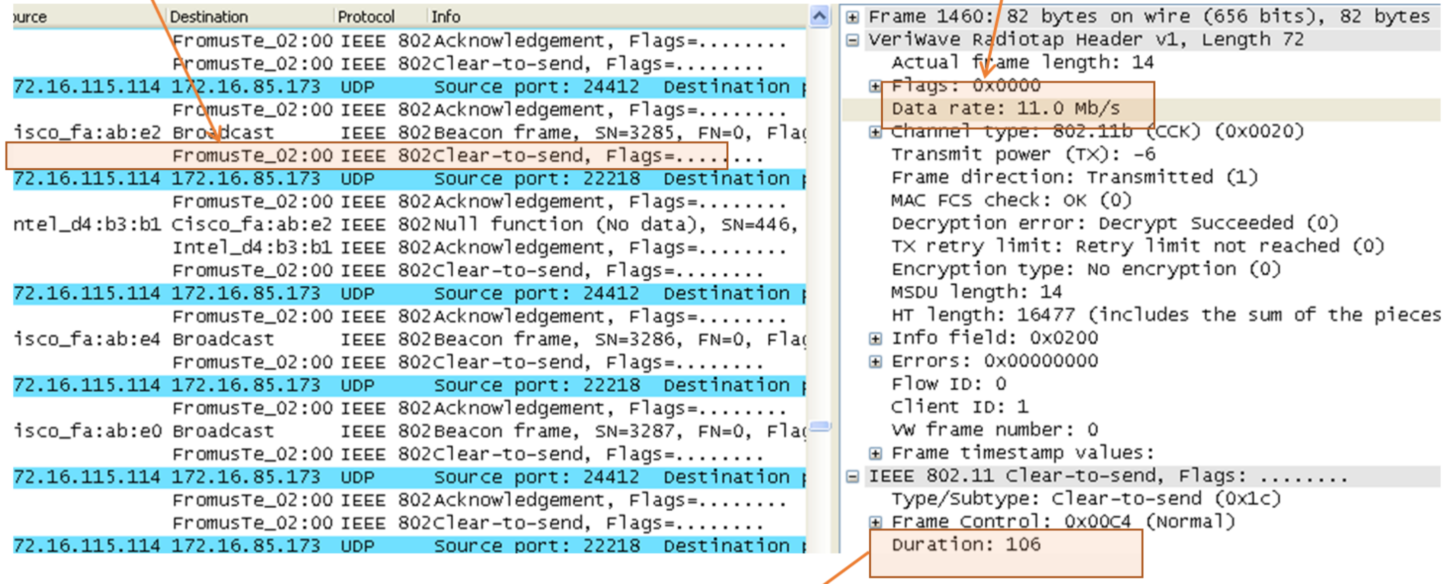
Legacy Protection and Greenfield Mode

WI-FI TECHNOLOGY
FUNDAMENTALS COURSE

- Legacy Protection Example:
  - In the case of 802.11g, protection mechanisms were created to allow 802.11b and 802.11g wireless devices to co-exist on the same frequencies.
  - Since older 802.11b-only clients cannot detect OFDM transmissions, 802.11g clients must “protect” their transmissions by first sending a bandwidth reservation request frame using DSSS modulation.
  - This frame, which is usually a CTS-to-self or RTS/CTS exchange alerts 802.11b clients to not attempt to transmit for a specified period of time.
  - 802.11n clients face the same problem as described above when operating a mixed mode environment with legacy a/b/g clients
  - Since the protection frames are send out at low PHY rates, this decreases overall system performance.
- Greenfield Mode:
  - Assumes that the network is not obligated to support legacy devices.
  - Devices operating in this mode can take full advantage of the improvements in the new standards.
  - Ideal for situations where a new network is created a from scratch with no possibility of using legacy devices.

CTS-to-Self frame is used to provide legacy protection. This frame is transmitted at the highest common PHY rate supported by all the legacy clients and this frame informs the legacy clients to get off the medium for a specified duration so that the 802.11n/a/g clients can transmit at high PHY rates.

In this example, the CTS frame is Transmitted at 11 Mbps and the following data frame is send out at 54 Mbps



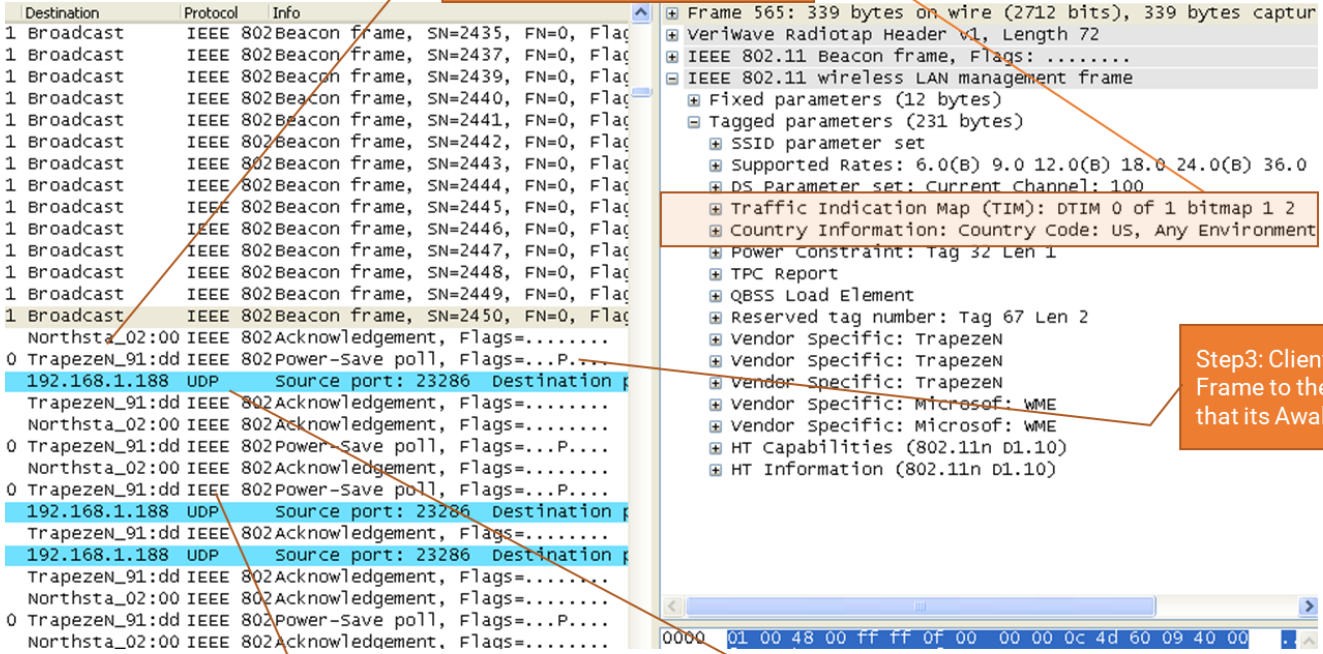
Duration for which the channel is requested.

Power Management

- Saving power is very important on battery operated 802.11 devices
- Power management schemes place a client in sleep mode when no activity occurs
- The MS can be configured to be in continuous aware mode (CAM) or Power Save Polling (PSP) mode
- In the PSP mode, the client can go to sleep by informing the AP when there is no activity
- The APs buffers any data directed to the client when the client is asleep

Step1: Client informs AP and goes to Sleep

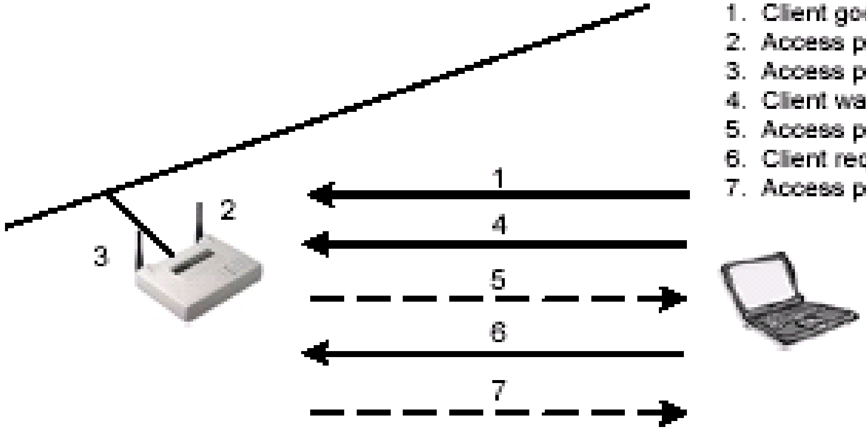
Step2: AP Sends out beacons with the TIM bits set for the Client IDs that have data buffered.



Step3: Client sends a PS-Poll Frame to the AP indicating that its Awake.

Step4: AP sends one buffered frame to the client with the "More Data" bit set if there is more buffered data.

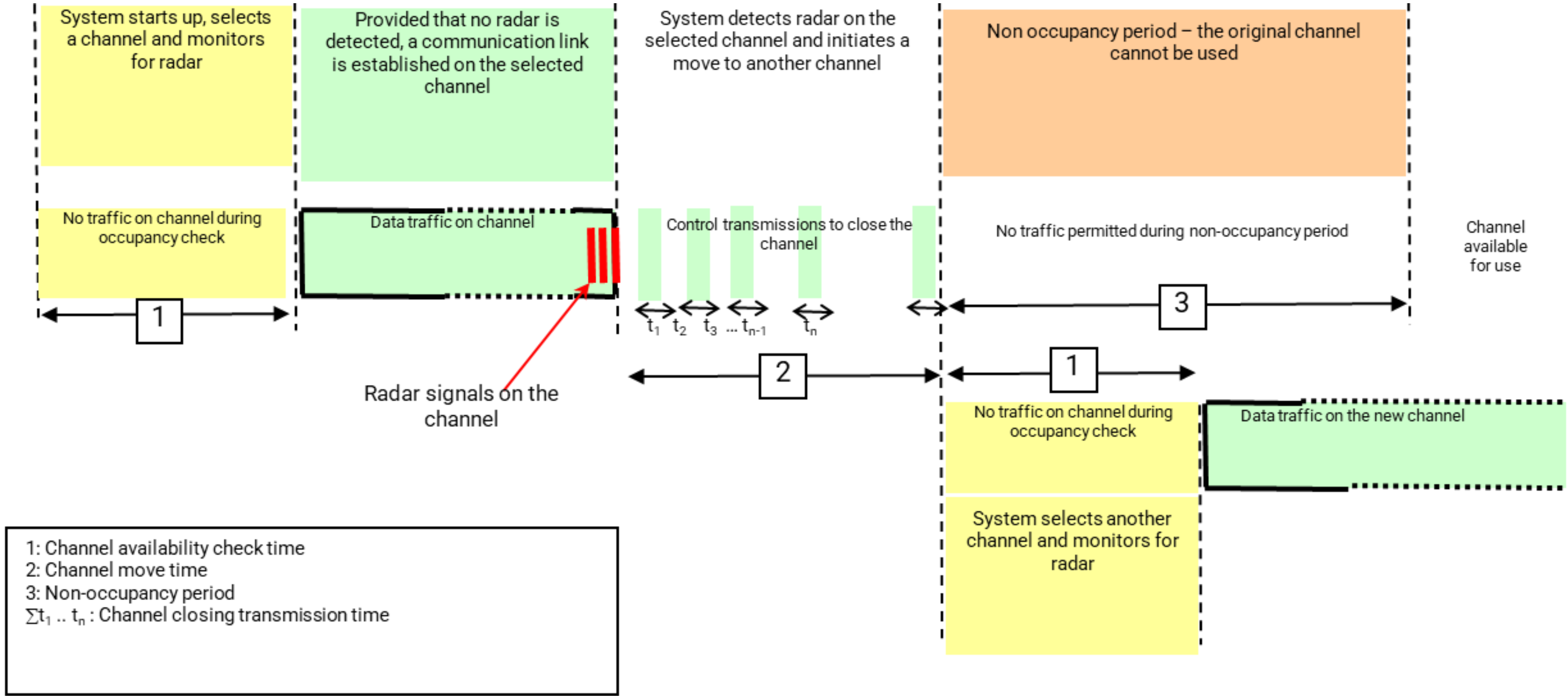
Step5: Client keeps sending PS-Poll frames to get one data frame at a time as long as AP says there is more buffered data.



1. Client goes to sleep
2. Access point marks client asleep
3. Access point buffers client packets
4. Client wakes up, notifies access point
5. Access point tells client data is waiting
6. Client requests data
7. Access point sends data

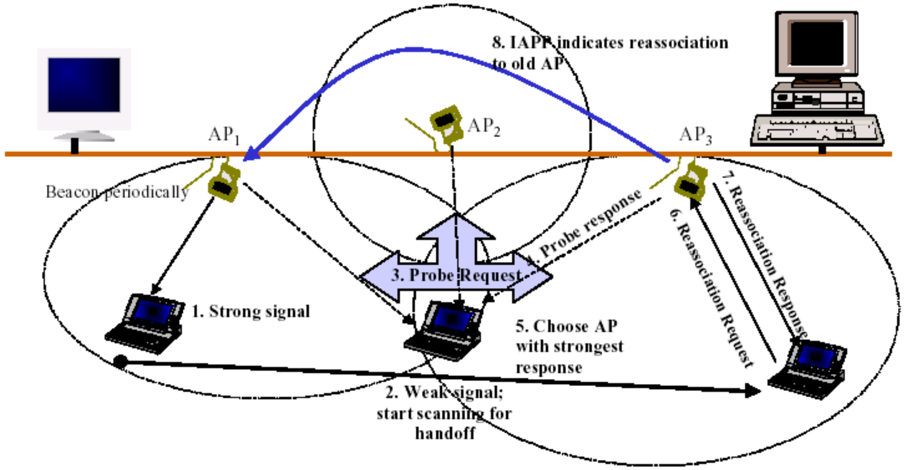
Dynamic Frequency Selection (DFS)

- DFS is a channel allocation scheme that dynamically selects and/or changes the operating frequency to avoid interfering with other systems.
- Unlicensed wireless networking systems (e.g. 802.11a/n) using the 5250-5350 MHz and/or 5470-5725 MHz bands cannot interfere with radar systems.
- A system implementing DFS needs to be capable of avoiding interfering with radar systems by
  - Verifying a channel is free of radar before using it .
  - Monitoring for radar once a channel is in use and vacating the channel if radar is detected.
  - Remaining off of a “radar” channel once radar has been detected .



WLAN Roaming

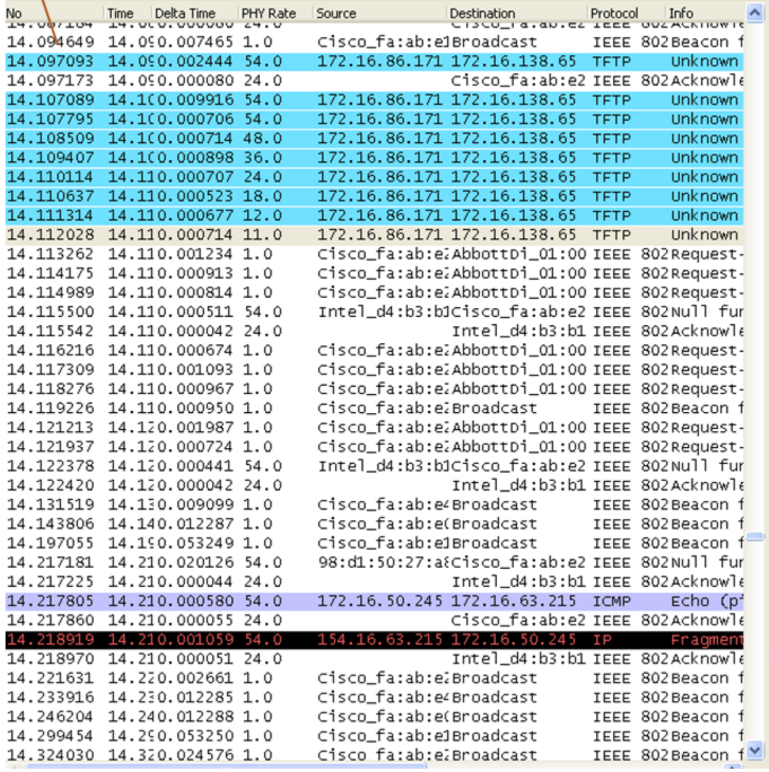
- Roaming can be defined as the client moving between APs advertising the same or similar wireless network
- Since the WLAN clients are mobile and coverage range of a single AP is limited, roaming happens whenever the client passes the boundaries of a WLAN cell
- The roaming protocol should be implemented effectively in order to cause very minimal delays during the handoff
- The clients usually make the roaming decisions by scanning the various available wireless networks at all times and trying to connect to the best available network
- Decision to roam can be made on various factors such as RSSI, number of missed beacons, SNR, frame errors, etc.
- When a decision is made to roam the client can authenticate and associate with the new AP and continue its data communication through the new AP
- Roaming when security is enabled would involve setting up a new security session with the new AP



Last Data packet on AP1 14.09 secs

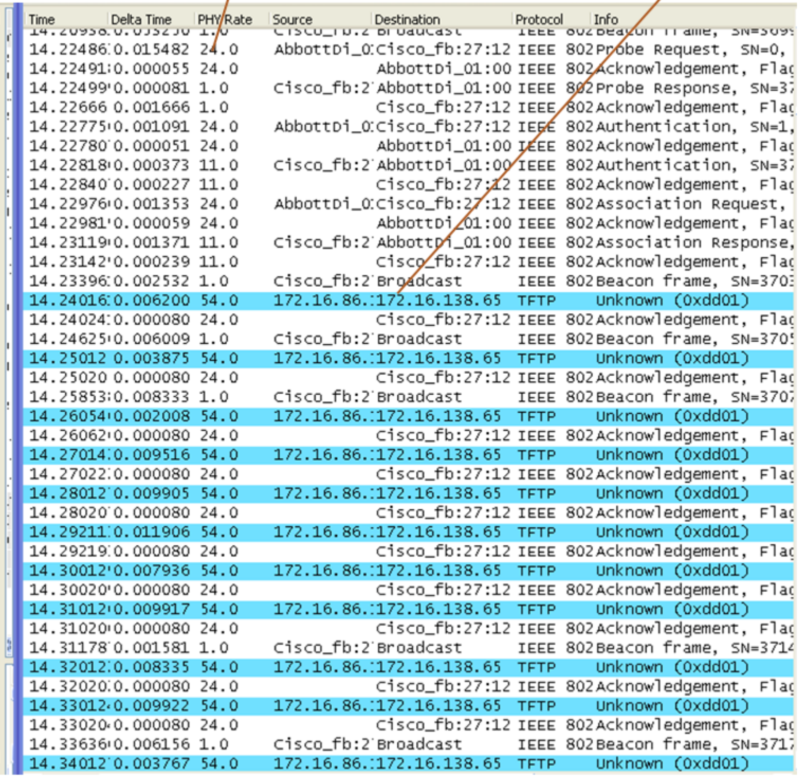
Perform 802.11 connection with AP2 starting at 14.22 secs

Start Data Transfer on AP2 at 14.24 seconds. Roaming delay is approximately 13 msecs



No	Time	Delta Time	PHY Rate	Source	Destination	Protocol	Info
14.094649	14.09	0.007465	1.0	Cisco_fa:ab:e1	Broadcast	IEEE 802	Beacon f
14.097093	14.09	0.002444	54.0	172.16.86.171	172.16.138.65	TFTP	Unknown
14.097173	14.09	0.000080	24.0		Cisco_fa:ab:e2	IEEE 802	Acknowle
14.107089	14.10	0.009916	54.0	172.16.86.171	172.16.138.65	TFTP	Unknown
14.107795	14.10	0.000706	54.0	172.16.86.171	172.16.138.65	TFTP	Unknown
14.108509	14.10	0.000714	48.0	172.16.86.171	172.16.138.65	TFTP	Unknown
14.109407	14.10	0.000898	36.0	172.16.86.171	172.16.138.65	TFTP	Unknown
14.110114	14.11	0.000707	24.0	172.16.86.171	172.16.138.65	TFTP	Unknown
14.110637	14.11	0.000523	18.0	172.16.86.171	172.16.138.65	TFTP	Unknown
14.111314	14.11	0.000677	12.0	172.16.86.171	172.16.138.65	TFTP	Unknown
14.112028	14.11	0.000714	11.0	172.16.86.171	172.16.138.65	TFTP	Unknown
14.113262	14.11	0.001234	1.0	Cisco_fa:ab:e2	AbbottDi_01:00	IEEE 802	Request-
14.114175	14.11	0.000913	1.0	Cisco_fa:ab:e2	AbbottDi_01:00	IEEE 802	Request-
14.114989	14.11	0.000814	1.0	Cisco_fa:ab:e2	AbbottDi_01:00	IEEE 802	Request-
14.115500	14.11	0.000511	54.0	Intel_d4:b3:b1	Cisco_fa:ab:e2	IEEE 802	Null fur
14.115542	14.11	0.000042	24.0		Intel_d4:b3:b1	IEEE 802	Acknowle
14.116216	14.11	0.000674	1.0	Cisco_fa:ab:e2	AbbottDi_01:00	IEEE 802	Request-
14.117309	14.11	0.001093	1.0	Cisco_fa:ab:e2	AbbottDi_01:00	IEEE 802	Request-
14.118276	14.11	0.000967	1.0	Cisco_fa:ab:e2	AbbottDi_01:00	IEEE 802	Request-
14.119226	14.11	0.000950	1.0	Cisco_fa:ab:e2	Broadcast	IEEE 802	Beacon f
14.121213	14.12	0.001987	1.0	Cisco_fa:ab:e2	AbbottDi_01:00	IEEE 802	Request-
14.121937	14.12	0.000724	1.0	Cisco_fa:ab:e2	AbbottDi_01:00	IEEE 802	Request-
14.122378	14.12	0.000441	54.0	Intel_d4:b3:b1	Cisco_fa:ab:e2	IEEE 802	Null fur
14.122420	14.12	0.000042	24.0		Intel_d4:b3:b1	IEEE 802	Acknowle
14.131519	14.13	0.009099	1.0	Cisco_fa:ab:e4	Broadcast	IEEE 802	Beacon f
14.143806	14.14	0.012287	1.0	Cisco_fa:ab:e(	Broadcast	IEEE 802	Beacon f
14.197055	14.19	0.053249	1.0	Cisco_fa:ab:e1	Broadcast	IEEE 802	Beacon f
14.217181	14.21	0.020126	54.0	98:d1:50:27:a8	Cisco_fa:ab:e2	IEEE 802	Null fur
14.217225	14.21	0.000044	24.0		Intel_d4:b3:b1	IEEE 802	Acknowle
14.217805	14.21	0.000580	54.0	172.16.50.245	172.16.63.215	ICMP	Echo (p
14.217860	14.21	0.000055	24.0		Cisco_fa:ab:e2	IEEE 802	Acknowle
14.218919	14.21	0.001059	54.0	154.16.63.215	172.16.50.245	IP	Fragment
14.218970	14.21	0.000051	24.0		Intel_d4:b3:b1	IEEE 802	Acknowle
14.221631	14.22	0.002661	1.0	Cisco_fa:ab:e2	Broadcast	IEEE 802	Beacon f
14.233916	14.23	0.012285	1.0	Cisco_fa:ab:e4	Broadcast	IEEE 802	Beacon f
14.246204	14.24	0.012288	1.0	Cisco_fa:ab:e(	Broadcast	IEEE 802	Beacon f
14.299454	14.29	0.053250	1.0	Cisco_fa:ab:e1	Broadcast	IEEE 802	Beacon f
14.324030	14.32	0.024576	1.0	Cisco_fa:ab:e2	Broadcast	IEEE 802	Beacon f

AP1 Capture



Time	Delta Time	PHY Rate	Source	Destination	Protocol	Info
14.22486	0.015482	24.0	AbbottDi_0	Cisco_fb:27:12	IEEE 802	Probe Request, SN=0,
14.22491	0.000055	24.0		AbbottDi_01:00	IEEE 802	Acknowledgement, Flag
14.22499	0.000081	1.0	Cisco_fb:2	AbbottDi_01:00	IEEE 802	Probe Response, SN=37
14.22666	0.001666	1.0		Cisco_fb:27:12	IEEE 802	Acknowledgement, Flag
14.22775	0.001091	24.0	AbbottDi_0	Cisco_fb:27:12	IEEE 802	Authentication, SN=1,
14.22780	0.000051	24.0		AbbottDi_01:00	IEEE 802	Acknowledgement, Flag
14.22818	0.000373	11.0	Cisco_fb:2	AbbottDi_01:00	IEEE 802	Authentication, SN=37
14.22840	0.000227	11.0		Cisco_fb:27:12	IEEE 802	Acknowledgement, Flag
14.22976	0.001353	24.0	AbbottDi_0	Cisco_fb:27:12	IEEE 802	Association Request,
14.22981	0.000059	24.0		AbbottDi_01:00	IEEE 802	Acknowledgement, Flag
14.23119	0.001371	11.0	Cisco_fb:2	AbbottDi_01:00	IEEE 802	Association Response,
14.23142	0.000239	11.0		Cisco_fb:27:12	IEEE 802	Acknowledgement, Flag
14.23396	0.002532	1.0	Cisco_fb:2	Broadcast	IEEE 802	Beacon frame, SN=370
14.24016	0.006200	54.0	172.16.86.	172.16.138.65	TFTP	Unknown (0xdd01)
14.24024	0.000080	24.0		Cisco_fb:27:12	IEEE 802	Acknowledgement, Flag
14.24625	0.006009	1.0	Cisco_fb:2	Broadcast	IEEE 802	Beacon frame, SN=370
14.25012	0.003875	54.0	172.16.86.	172.16.138.65	TFTP	Unknown (0xdd01)
14.25020	0.000080	24.0		Cisco_fb:27:12	IEEE 802	Acknowledgement, Flag
14.25853	0.008333	1.0	Cisco_fb:2	Broadcast	IEEE 802	Beacon frame, SN=370
14.26054	0.002008	54.0	172.16.86.	172.16.138.65	TFTP	Unknown (0xdd01)
14.26062	0.000080	24.0		Cisco_fb:27:12	IEEE 802	Acknowledgement, Flag
14.27014	0.009516	54.0	172.16.86.	172.16.138.65	TFTP	Unknown (0xdd01)
14.27022	0.000080	24.0		Cisco_fb:27:12	IEEE 802	Acknowledgement, Flag
14.28012	0.009905	54.0	172.16.86.	172.16.138.65	TFTP	Unknown (0xdd01)
14.28020	0.000080	24.0		Cisco_fb:27:12	IEEE 802	Acknowledgement, Flag
14.29211	0.011906	54.0	172.16.86.	172.16.138.65	TFTP	Unknown (0xdd01)
14.29219	0.000080	24.0		Cisco_fb:27:12	IEEE 802	Acknowledgement, Flag
14.30012	0.007936	54.0	172.16.86.	172.16.138.65	TFTP	Unknown (0xdd01)
14.30020	0.000080	24.0		Cisco_fb:27:12	IEEE 802	Acknowledgement, Flag
14.31012	0.009917	54.0	172.16.86.	172.16.138.65	TFTP	Unknown (0xdd01)
14.31020	0.000080	24.0		Cisco_fb:27:12	IEEE 802	Acknowledgement, Flag
14.31178	0.001581	1.0	Cisco_fb:2	Broadcast	IEEE 802	Beacon frame, SN=3714
14.32012	0.008335	54.0	172.16.86.	172.16.138.65	TFTP	Unknown (0xdd01)
14.32020	0.000080	24.0		Cisco_fb:27:12	IEEE 802	Acknowledgement, Flag
14.33012	0.009922	54.0	172.16.86.	172.16.138.65	TFTP	Unknown (0xdd01)
14.33020	0.000080	24.0		Cisco_fb:27:12	IEEE 802	Acknowledgement, Flag
14.33636	0.006156	1.0	Cisco_fb:2	Broadcast	IEEE 802	Beacon frame, SN=371
14.34012	0.003767	54.0	172.16.86.	172.16.138.65	TFTP	Unknown (0xdd01)

AP2 Capture

References

802.11 Network Service Set

https://en.wikipedia.org/wiki/Service_set_(802.11_network)

802.11 Client Active And Passive Scanning

http://www.my80211.com/home/2010/1/11/80211-client-active-and-passive-scanning.html

Captive Portal Basics

https://en.wikipedia.org/wiki/Captive_portal

Carrier Sensing Mechanisms

https://howiwifi.com/2020/06/30/wireless-contention-mechanisms/

Power Save Methods

https://howiwifi.com/2020/06/25/power-save-methods /


Q&A

WI-FI TECHNOLOGY
FUNDAMENTALS COURSE

Quiz 2d Results

Winner

Pradyumna

INDIA

Number of participants - 124