

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

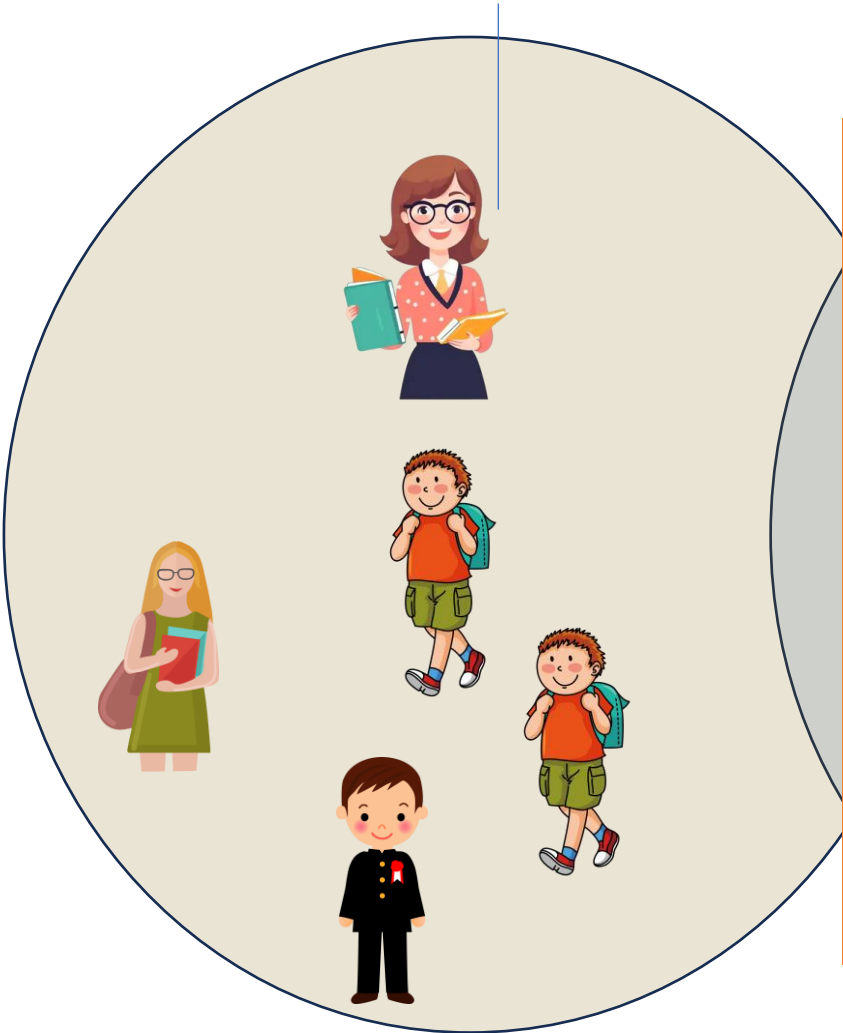
The Multiple Access Problem



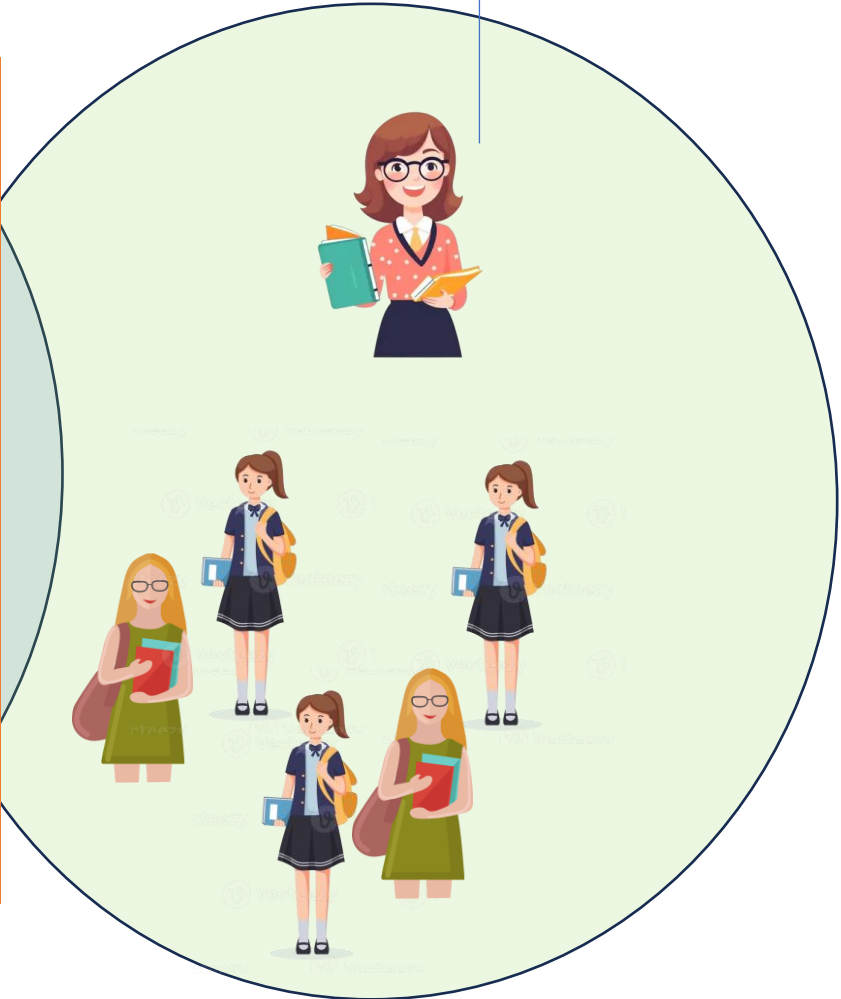
The Principal



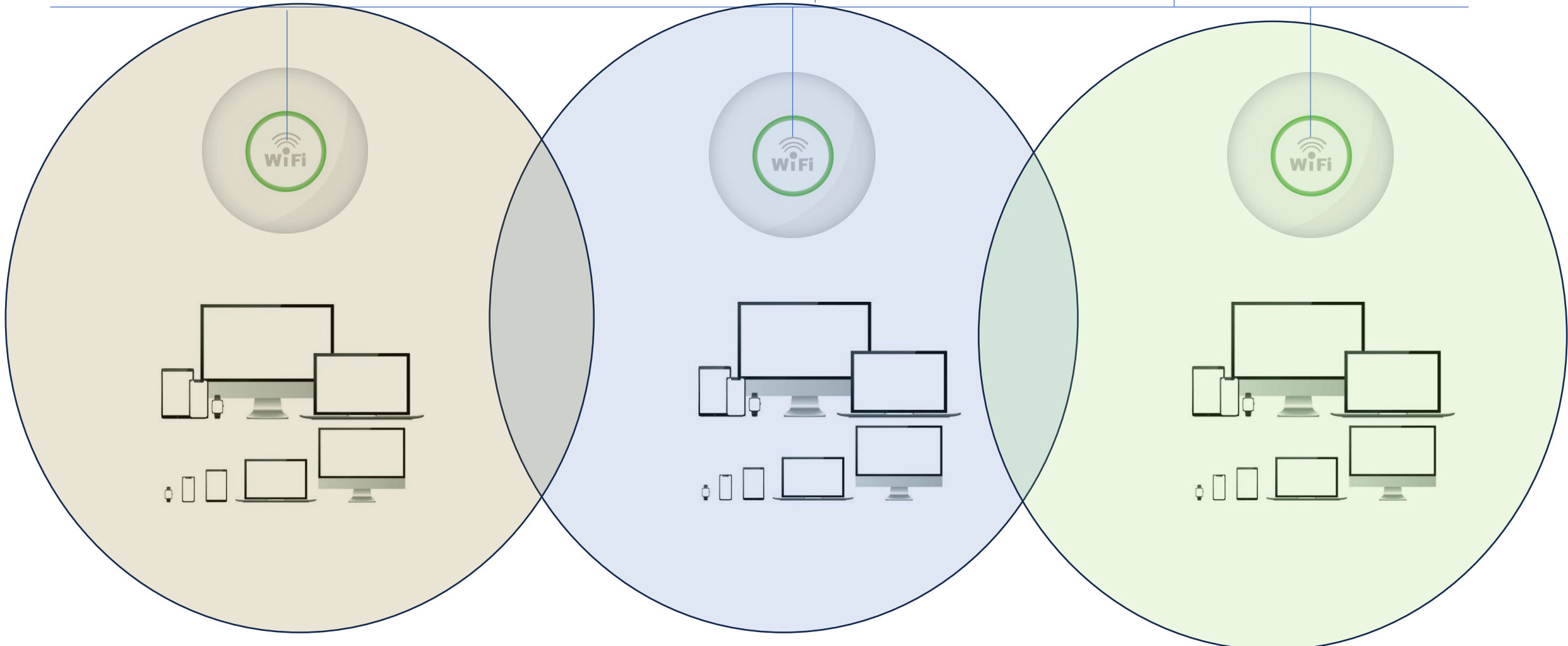
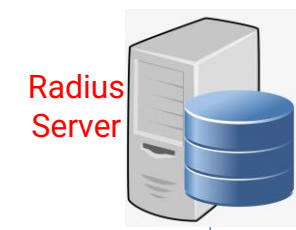
School Admins



Multiple Access
Range
Interference
Security
Roaming
Scheduling
Management
Controls



The Multiple Access Problem



The Food Court Experience

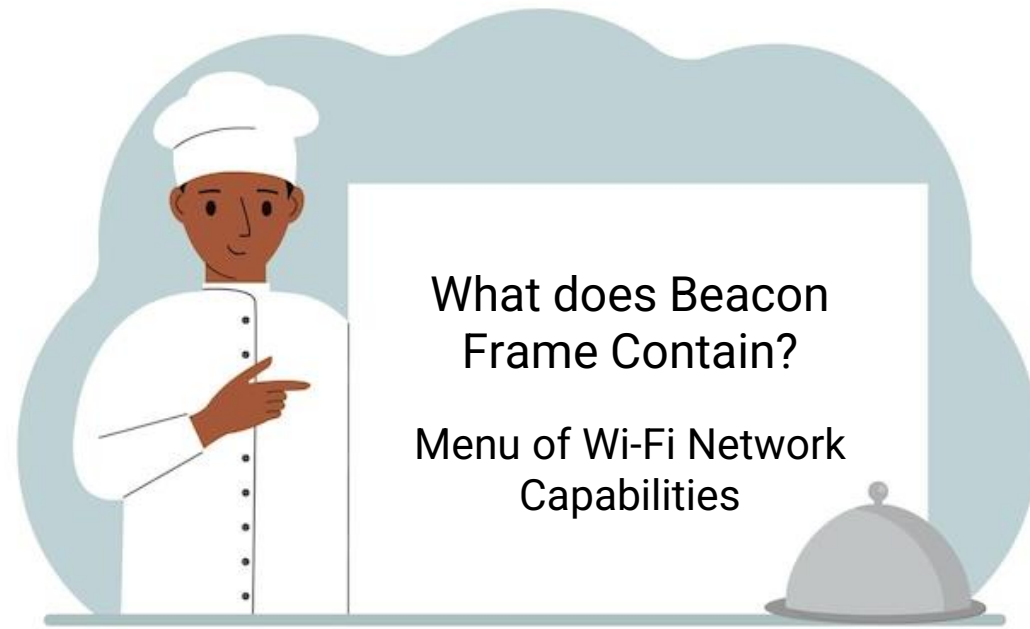


1. Rough scan all the restaurants in the food court
2. More detailed scan, check the menus.
3. Check how long it will take food to arrive and how busy the restaurant is.
4. Figure out which restaurant you like.
5. Place the order and pay the money
6. Enjoy the food and leave



What is a Beacon Frame?

A periodic Message Broadcast
once every 100ms

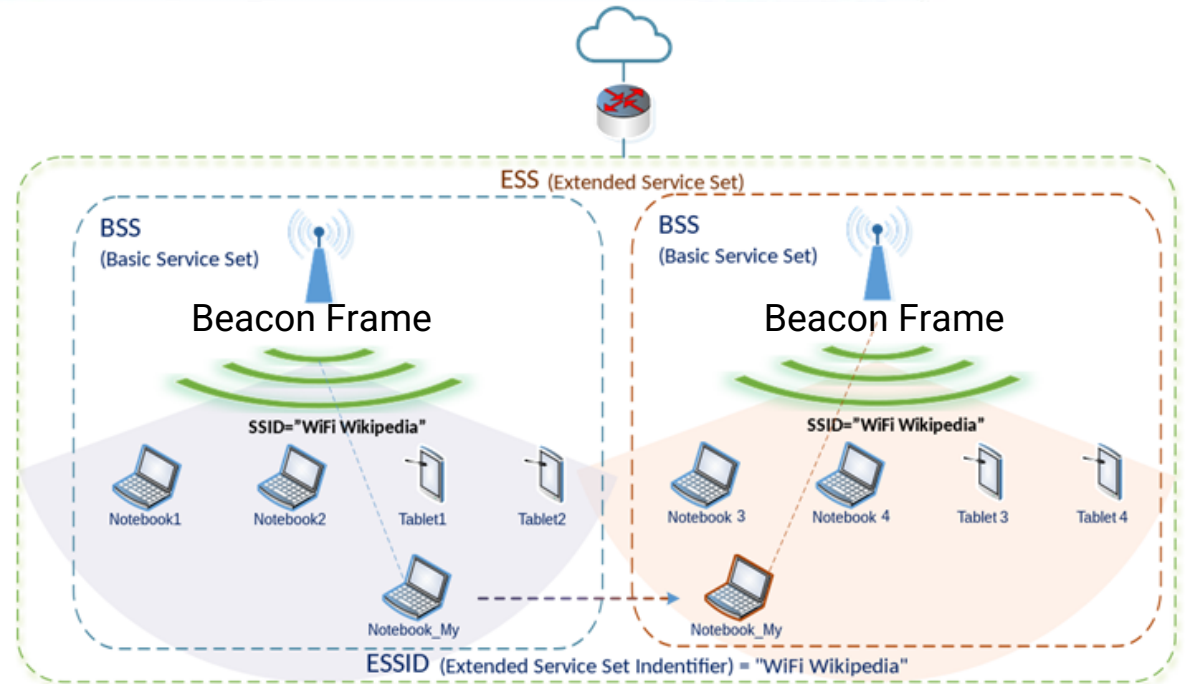
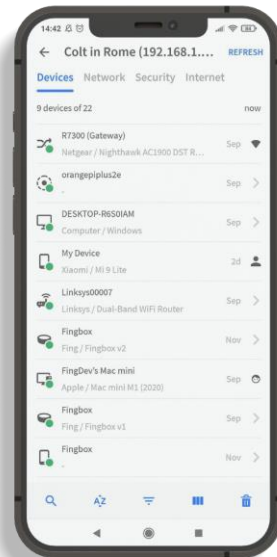


WNIC
(No WiFi)

WNIC
(No WiFi)



WNIC
(No WiFi)



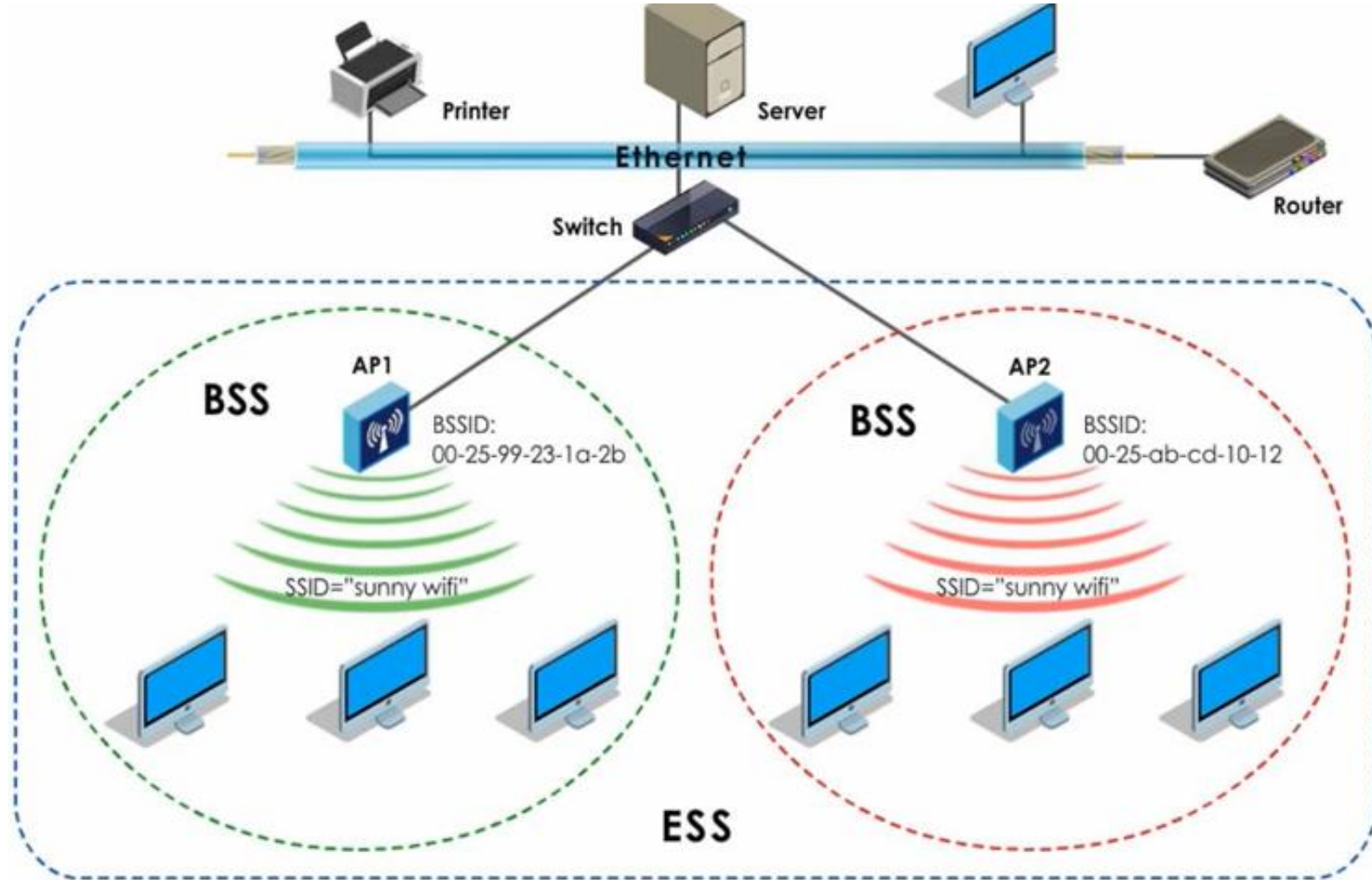
SSID and BSSID

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

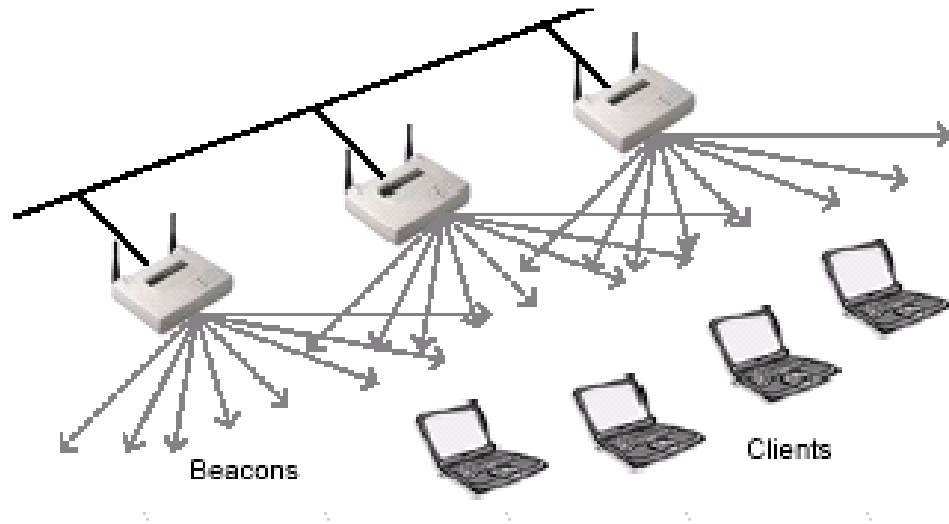
- Flow Control
- Power Save Control
- Medium Access Control

Data Plane

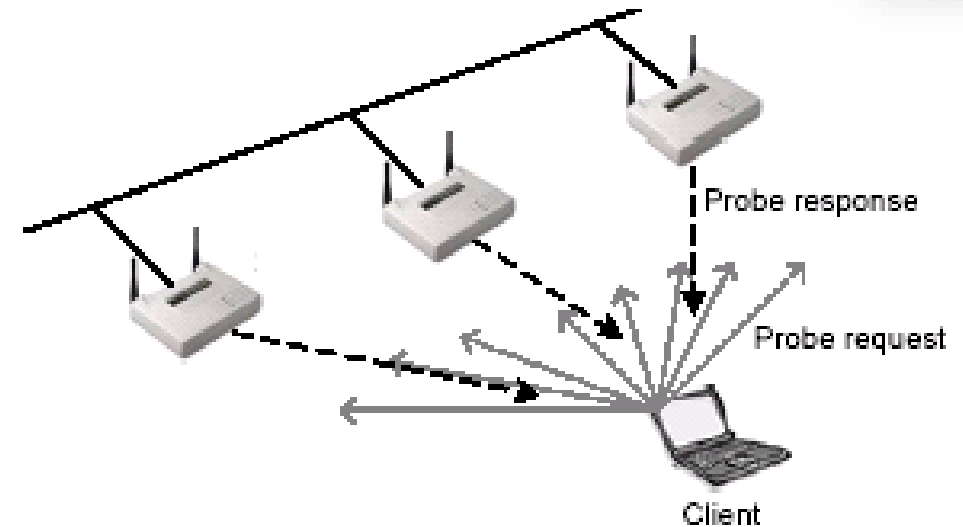
- Data Transmission

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.



Passive Scan



Active 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.

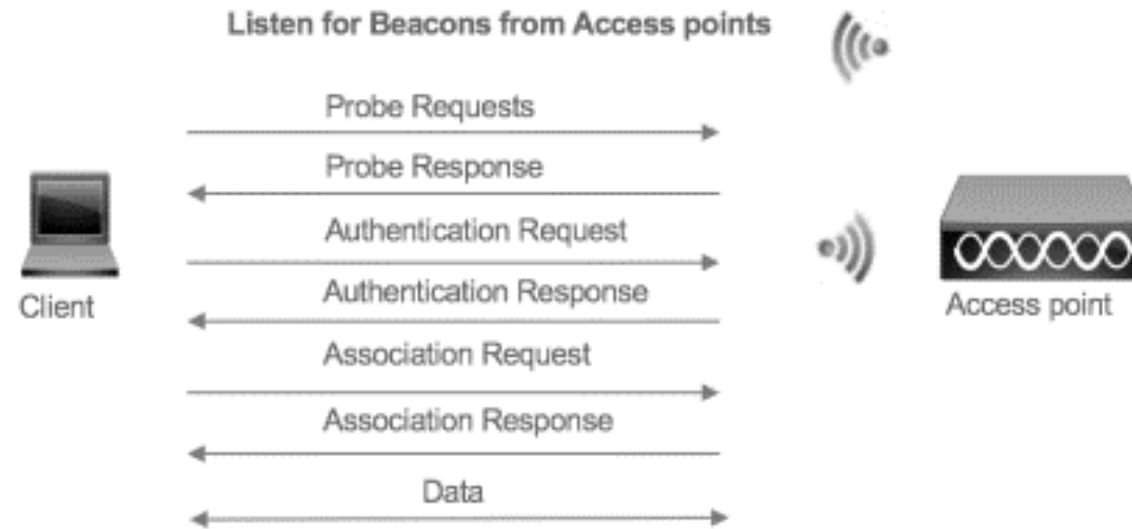
| Source | Destination | Protocol | Info |
|-------------------|-------------------|----------|--------------------------------|
| Trapezen_91:dd:c1 | Broadcast | IEEE 802 | Beacon frame, SN=2201, FN=0 |
| Trapezen_91:dd:c1 | Broadcast | IEEE 802 | Beacon frame, SN=2202, FN=0 |
| Trapezen_91:dd:c1 | Broadcast | IEEE 802 | Beacon frame, SN=2203, FN=0 |
| Trapezen_91:dd:c1 | Broadcast | IEEE 802 | Beacon frame, SN=2204, FN=0 |
| Trapezen_91:dd:c1 | Broadcast | IEEE 802 | Beacon frame, SN=2205, FN=0 |
| Trapezen_91:dd:c1 | Broadcast | IEEE 802 | Beacon frame, SN=2206, FN=0 |
| Trapezen_91:dd:c1 | Broadcast | IEEE 802 | Beacon frame, SN=2207, FN=0 |
| Trapezen_91:dd:c1 | Broadcast | IEEE 802 | Beacon frame, SN=2208, FN=0 |
| Trapezen_91:dd:c1 | Broadcast | IEEE 802 | Beacon frame, SN=2209, FN=0 |
| Trapezen_91:dd:c1 | Broadcast | IEEE 802 | Beacon frame, SN=2210, FN=0 |
| Trapezen_91:dd:c1 | Broadcast | IEEE 802 | Beacon frame, SN=2211, FN=0 |
| Trapezen_91:dd:c1 | Broadcast | IEEE 802 | Beacon frame, SN=2212, FN=0 |
| Trapezen_91:dd:c1 | Broadcast | IEEE 802 | Beacon frame, SN=2213, FN=0 |
| Trapezen_91:dd:c1 | Broadcast | IEEE 802 | Beacon frame, SN=2214, FN=0 |
| Trapezen_91:dd:c1 | Broadcast | IEEE 802 | Beacon frame, SN=2215, FN=0 |
| Xerox_00:00:02 | Broadcast | IEEE 802 | Probe Request, SN=0, FN=0, |
| Trapezen_91:dd:c1 | Xerox_00:00:02 | IEEE 802 | Probe Response, SN=2216, FN=0, |
| Trapezen_91:dd:c1 | Trapezen_91:dd:c1 | IEEE 802 | Acknowledgement, Flags=.... |
| Trapezen_91:dd:c1 | Broadcast | IEEE 802 | Beacon frame, SN=2217, FN=0 |
| Xerox_00:00:02 | Broadcast | IEEE 802 | Probe Request, SN=1, FN=0, |
| Trapezen_91:dd:c1 | Xerox_00:00:02 | IEEE 802 | Probe Response, SN=2218, FN=0, |
| Trapezen_91:dd:c1 | Trapezen_91:dd:c1 | IEEE 802 | Acknowledgement, Flags=.... |
| Trapezen_91:dd:c1 | Broadcast | IEEE 802 | Beacon frame, SN=2219, FN=0 |
| Xerox_00:00:02 | Broadcast | IEEE 802 | Probe Request, SN=2, FN=0, |
| Trapezen_91:dd:c1 | Xerox_00:00:02 | IEEE 802 | Probe Response, SN=2220, FN=0, |

Frame 16: 70 bytes on wire (560 bits), 70 bytes captured (560 b)

- ⊕ IEEE 802.11 Probe Request, Flags:
- ⊖ IEEE 802.11 wireless LAN management frame
 - ⊖ Tagged parameters (46 bytes)
 - ⊕ SSID parameter set
 - ⊕ Supported Rates: 1.0(B) 2.0(B) 5.5(B) 11.0(B) 6.0(B) 9.0(B)
 - ⊕ Extended Supported Rates: 18.0(B) 36.0(B) 48.0(B) 54.0(B)
 - ⊕ HT Capabilities (802.11n D1.10)

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

Simple Client Connection and Data Transfer

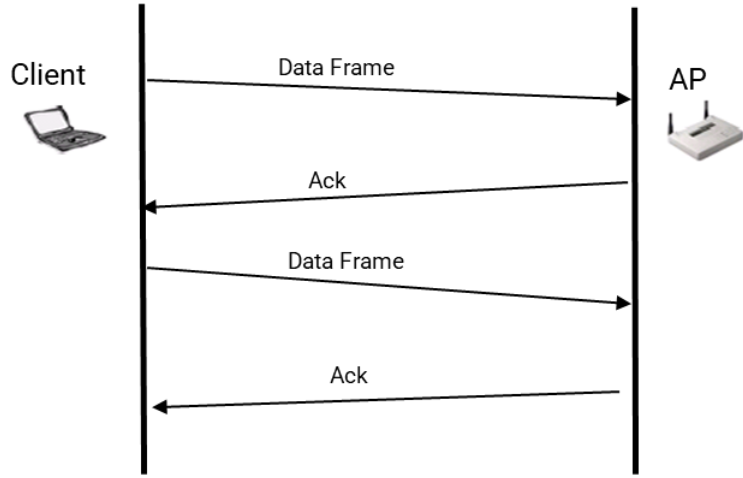
| | | | |
|----------|-------------------|---------------------|--------------------------------------|
| 2.600267 | Fromuste_02:00:00 | Trapezen_9:IEEE | 802Probe Request, SN=0, FN=0, Flags= |
| 2.600372 | | Fromuste_0:IEEE | 802Acknowledgement, Flags=..... |
| 2.600730 | Trapezen_91:dd:c1 | Fromuste_0:IEEE | 802Probe Response, SN=3036, FN=0, F |
| 2.601102 | | Trapezen_9:IEEE | 802Acknowledgement, Flags=..... |
| 2.611334 | Fromuste_02:00:00 | Trapezen_9:IEEE | 802Authentication, SN=1, FN=0, Flags |
| 2.611422 | | Fromuste_0:IEEE | 802Acknowledgement, Flags=..... |
| 2.611545 | Trapezen_91:dd:c1 | Fromuste_0:IEEE | 802Authentication, SN=3037, FN=0 |
| 2.611633 | | Trapezen_9:IEEE | 802Acknowledgement, Flags=..... |
| 2.622368 | Fromuste_02:00:00 | Trapezen_9:IEEE | 802Association Request, SN=2, FN= |
| 2.622492 | | Fromuste_0:IEEE | 802Acknowledgement, Flags=..... |
| 2.625950 | Trapezen_91:dd:c1 | Fromuste_0:IEEE | 802Association Response, SN=3038 |
| 2.626549 | | Trapezen_9:IEEE | 802Acknowledgement, Flags=..... |
| 2.637426 | 0.0.0.0 | 255.255.255:DHCP | DHCP Discover - Transaction ID 0x |
| 2.637962 | | Fromuste_0:IEEE | 802Acknowledgement, Flags=..... |
| 7.653973 | 0.0.0.0 | 255.255.255:DHCP | DHCP Discover - Transaction ID 0x |
| 7.654509 | | Fromuste_0:IEEE | 802Acknowledgement, Flags=..... |
| 7.657036 | 192.168.1.10 | 192.168.1.1:DHCP | DHCP offer - Transaction ID 0x |
| 7.660564 | | Trapezen_9:IEEE | 802Acknowledgement, Flags=..... |
| 7.660642 | 0.0.0.0 | 255.255.255:DHCP | DHCP Request - Transaction ID 0x |
| 7.661194 | | Fromuste_0:IEEE | 802Acknowledgement, Flags=..... |
| 7.663934 | 192.168.1.10 | 192.168.1.1:DHCP | DHCP ACK - Transaction ID 0x |
| 7.664454 | | Trapezen_9:IEEE | 802Acknowledgement, Flags=..... |
| 7.664532 | Fromuste_02:00:00 | Broadcast | ARP Gratuitous ARP for 192.168.1.139 |
| 7.664660 | | Fromuste_0:IEEE | 802Acknowledgement, Flags=..... |
| 7.675024 | Fromuste_02:00:00 | Broadcast | ARP Gratuitous ARP for 192.168.1.139 |
| 7.675152 | | Fromuste_0:IEEE | 802Acknowledgement, Flags=..... |
| 7.686057 | Fromuste_02:00:00 | Broadcast | ARP Gratuitous ARP for 192.168.1.139 |
| 7.686185 | | Fromuste_0:IEEE | 802Acknowledgement, Flags=..... |
| 7.697090 | Fromuste_02:00:00 | Broadcast | ARP Gratuitous ARP for 192.168.1.139 |
| 7.697218 | | Fromuste_0:IEEE | 802Acknowledgement, Flags=..... |
| 7.719176 | 192.168.1.139 | 192.168.1.1:BROWSER | Host Announcement vw-Learning |
| 7.719580 | | Fromuste_0:IEEE | 802Acknowledgement, Flags=..... |
| 7.770322 | 192.168.1.139 | 192.168.1.1:BROWSER | Host Announcement vw-Learning |
| 7.770727 | | Fromuste_0:IEEE | 802Acknowledgement, Flags=..... |
| 7.821484 | 192.168.1.139 | 192.168.1.1:BROWSER | Host Announcement vw-Learning |
| 7.821880 | | Fromuste_0:IEEE | 802Acknowledgement, Flags=..... |

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 uses a static IP address.

Data Transfer and Retries

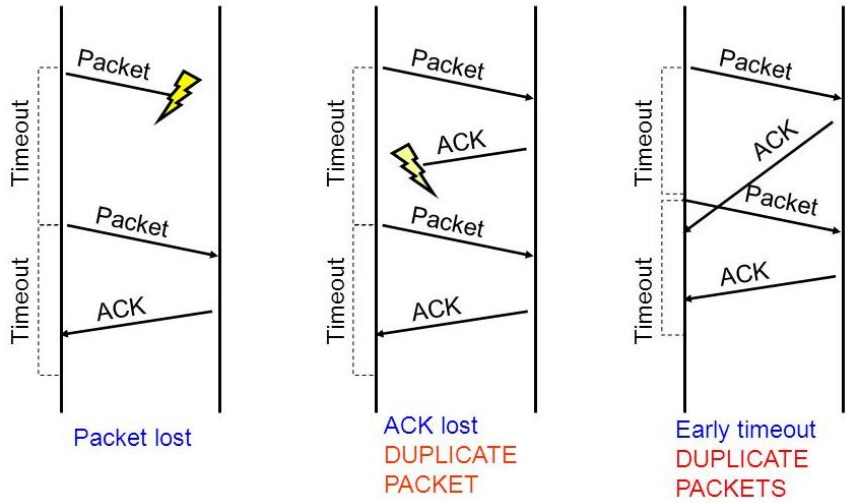


| Source | Destination | Protocol | Info |
|-------------------|-------------------|------------|------------------------------|
| Xerox_00:00:02 | Broadcast | IEEE 802 P | |
| Trapezen_91:dd:c1 | Xerox_00:00:02 | IEEE 802 P | |
| Trapezen_91:dd:c1 | Trapezen_91:dd:c1 | IEEE 802A | |
| 192.168.1.138 | 192.168.1.139 | UDP | Source port: 20317 Destinat |
| Trapezen_91:dd:c1 | Trapezen_91:dd:c1 | IEEE 802 | Acknowledgement, Flags=..... |
| Trapezen_91:dd:c1 | Broadcast | IEEE 802 | Beacon frame, SN=3131, FN=0, |
| 192.168.1.138 | 192.168.1.139 | UDP | Source port: 20317 Destinat |
| 192.168.1.138 | 192.168.1.139 | UDP | Source port: 20317 Destinat |
| Trapezen_91:dd:c1 | Trapezen_91:dd:c1 | IEEE 802 | Acknowledgement, Flags=..... |
| 192.168.1.138 | 192.168.1.139 | UDP | Source port: 20317 Destinat |
| Trapezen_91:dd:c1 | Trapezen_91:dd:c1 | IEEE 802 | Acknowledgement, Flags=..... |
| Trapezen_91:dd:c1 | Broadcast | IEEE 802 | Beacon frame, SN=3133, FN=0, |
| 192.168.1.138 | 192.168.1.139 | UDP | Source port: 20317 Destinat |
| 192.168.1.138 | 192.168.1.139 | UDP | Source port: 20317 Destinat |
| Trapezen_91:dd:c1 | Trapezen_91:dd:c1 | IEEE 802 | Acknowledgement, Flags=..... |
| 192.168.1.138 | 192.168.1.139 | UDP | Source port: 20317 Destinat |
| Trapezen_91:dd:c1 | Trapezen_91:dd:c1 | IEEE 802 | Acknowledgement, Flags=..... |
| Trapezen_91:dd:c1 | Broadcast | IEEE 802 | Beacon frame, SN=3134, FN=0, |
| 192.168.1.138 | 192.168.1.139 | UDP | Source port: 20317 Destinat |
| 192.168.1.138 | 192.168.1.139 | UDP | Source port: 20317 Destinat |
| Trapezen_91:dd:c1 | Trapezen_91:dd:c1 | IEEE 802 | Acknowledgement, Flags=..... |
| Trapezen_91:dd:c1 | Broadcast | IEEE 802 | Beacon frame, SN=3135, FN=0, |
| 192.168.1.138 | 192.168.1.139 | UDP | Source port: 20317 Destinat |
| 192.168.1.138 | 192.168.1.139 | UDP | Source port: 20317 Destinat |
| Trapezen_91:dd:c1 | Trapezen_91:dd:c1 | IEEE 802 | Acknowledgement, Flags=..... |
| Trapezen_91:dd:c1 | Broadcast | IEEE 802 | Beacon frame, SN=3136, FN=0, |
| 192.168.1.138 | 192.168.1.139 | UDP | Source port: 20317 Destinat |

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

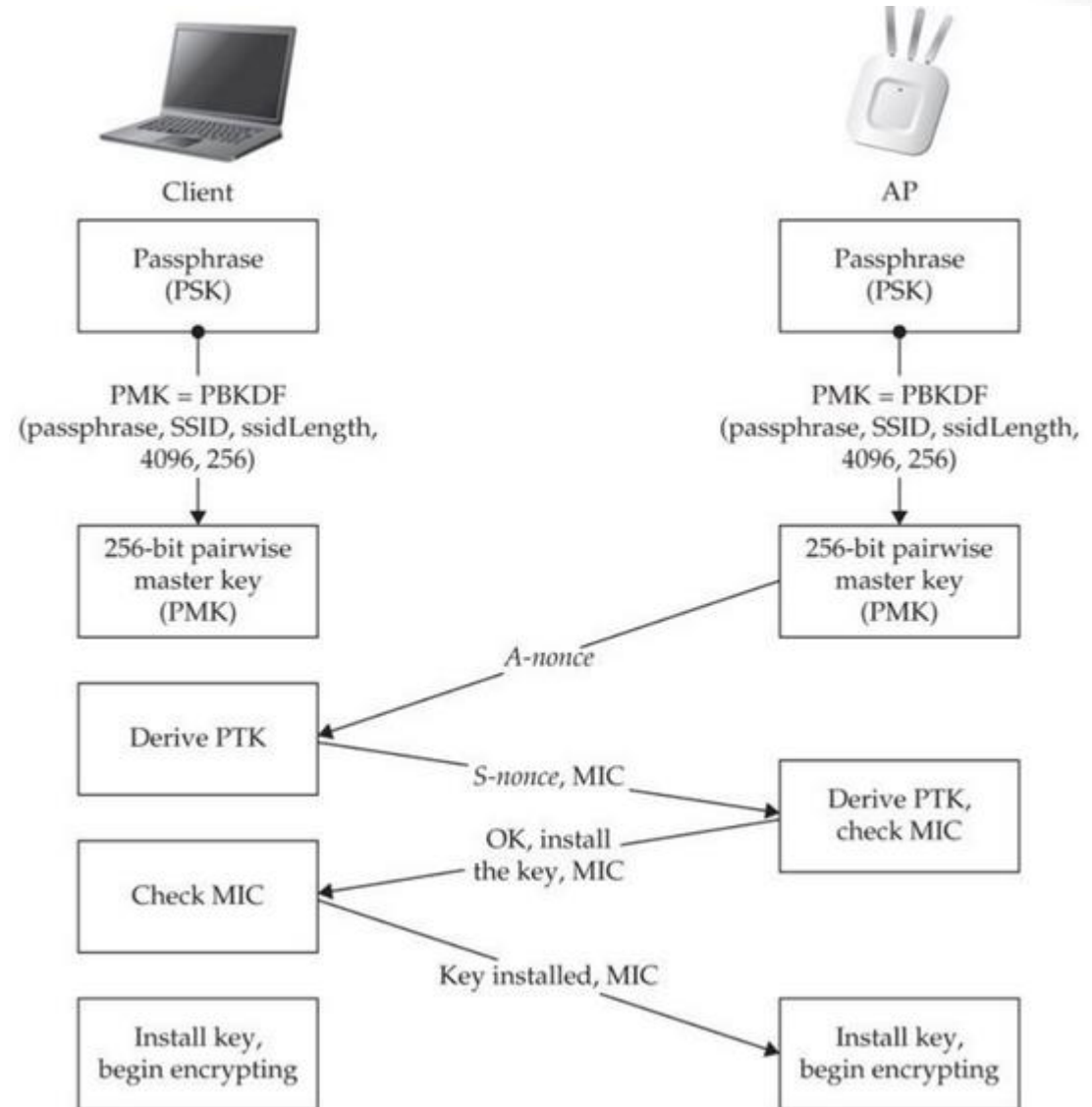
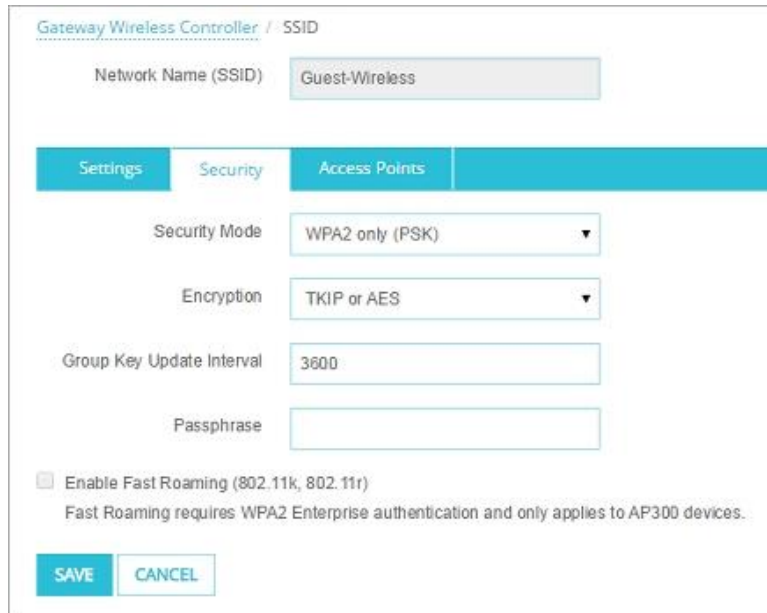
Frame 14: 1516 bytes on wire (12128 bits)
Version: 0
Type: Data frame (2)
Subtype: 8
Flags: 0xA
... ..10 = DS status: Frame from C
... ..0.. = More Fragments: This is
... ..1... = Retry: Frame is being r
... ..0 ... = PWR MGT: STA will stay
... ..0 ... = More Data: No data buff
... ..0 ... = Protected 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)

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



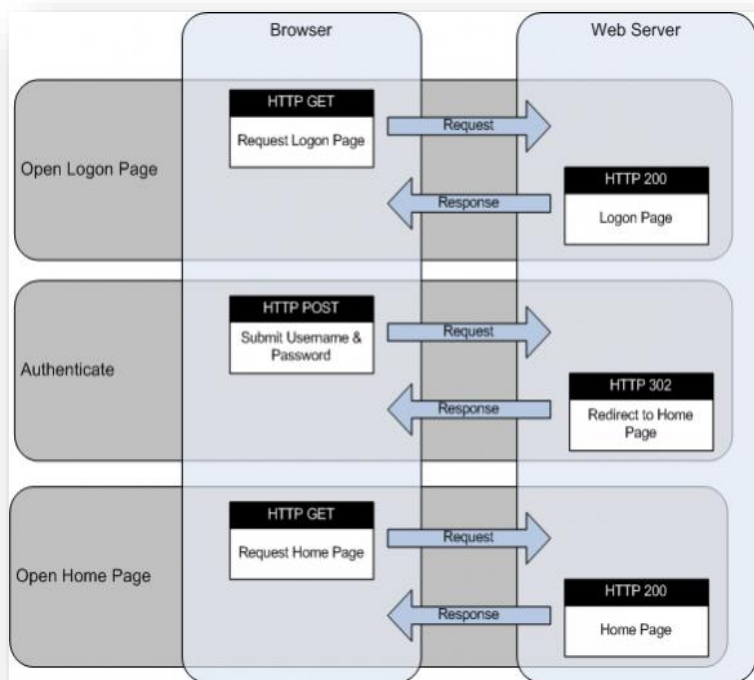
Connection using Browser



| | | | | | | |
|------|----------|----------------|--------------------------------|------|-----|---|
| 1093 | 6.262667 | 199.108.225.88 | 10.100.40.41 | TCP | Yes | http > 24492 [SYN, ACK] Seq=0 Ack=1 Win=5560 Len=0 MSS=1390 WS=2 |
| 1094 | 6.262719 | | Cisco_89:64:2e (RA) IEEE 8(Yes | | | Acknowledgement, Flags=..... |
| 1096 | 6.263203 | 10.100.40.41 | 199.108.225.88 | TCP | Yes | 24492 > http [ACK] Seq=1 Ack=1 win=65535 Len=0 |
| 1097 | 6.263795 | 10.100.40.41 | 199.108.225.88 | TCP | Yes | [TCP Dup ACK 1096#1] 24492 > http [ACK] Seq=1 Ack=1 win=65535 Len=0 |
| 1098 | 6.263936 | | 00:81:50:00:00:01 (IEEE 8(Yes | | | Acknowledgement, Flags=..... |
| 1099 | 6.268092 | 10.100.40.41 | 199.108.225.88 | HTTP | Yes | GET / HTTP/1.1 |
| 1100 | 6.268305 | | 00:81:50:00:00:01 (IEEE 8(Yes | | | Acknowledgement, Flags=..... |
| 1101 | 6.269245 | 199.108.225.88 | 10.100.40.41 | TCP | Yes | http > 24492 [ACK] Seq=1 Ack=56 win=5560 Len=0 |
| 1102 | 6.269293 | | Cisco_89:64:2e (RA) IEEE 8(Yes | | | Acknowledgement, Flags=..... |
| 1103 | 6.269382 | 199.108.225.88 | 10.100.40.41 | HTTP | Yes | HTTP/1.1 200 OK (text/html) |

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

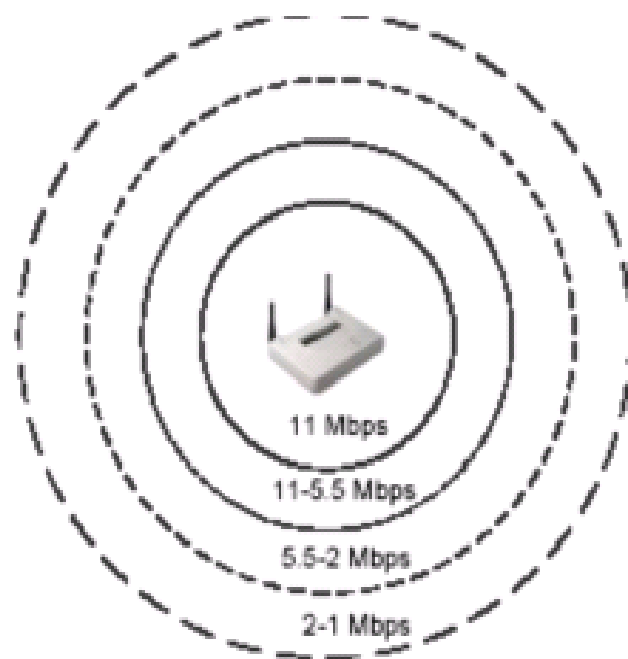


| | | | | | | |
|------|----------|--------------|--------------------------------|------|-----|-------------------------------|
| 1303 | 6.864880 | | 00:81:50:00:00:01 (IEEE 8(Yes | | | Acknowledgement, Flags=... |
| 1304 | 6.864988 | 10.100.40.41 | 1.1.1.1 | HTTP | Yes | POST /login.html HTTP/1.1 |
| 1305 | 6.865238 | | 00:81:50:00:00:01 (IEEE 8(Yes | | | Acknowledgement, Flags=... |
| 1306 | 6.865448 | 1.1.1.1 | 10.100.40.41 | TCP | Yes | http > 13927 [ACK] Seq=1 A... |
| 1307 | 6.865496 | | Cisco_89:64:2e (RA) IEEE 8(Yes | | | Acknowledgement, Flags=... |
| 1308 | 6.865596 | 1.1.1.1 | 10.100.40.41 | HTTP | Yes | HTTP/1.1 100 Continue |
| 1309 | 6.865648 | | Cisco_89:64:2e (RA) IEEE 8(Yes | | | Acknowledgement, Flags=... |
| 1310 | 6.868326 | 1.1.1.1 | 10.100.40.41 | TCP | Yes | [TCP segment of a reasemb... |
| 1311 | 6.868860 | 1.1.1.1 | 10.100.40.41 | HTTP | Yes | [TCP out-of-order] HTTP/1... |
| 1312 | 6.869331 | 1.1.1.1 | 10.100.40.41 | TCP | Yes | [TCP out-of-order] [TCP se... |
| 1313 | 6.869615 | | Cisco_89:64:2e (RA) IEEE 8(Yes | | | Acknowledgement, Flags=... |
| 1314 | 6.869782 | 10.100.40.41 | 1.1.1.1 | TCP | Yes | 13927 > http [ACK] Seq=284 |
| 1315 | 6.869924 | | 00:81:50:00:00:01 (IEEE 8(Yes | | | Acknowledgement, Flags=... |
| 1316 | 6.871170 | 1.1.1.1 | 10.100.40.41 | HTTP | Yes | HTTP/1.1 200 OK (text/html) |
| 1317 | 6.871542 | 1.1.1.1 | 10.100.40.41 | TCP | Yes | [TCP out-of-order] [TCP se... |

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



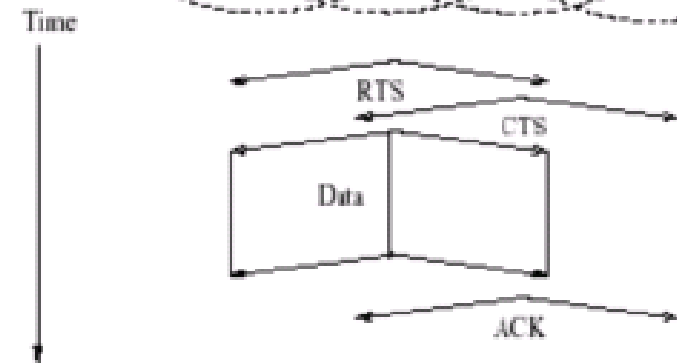
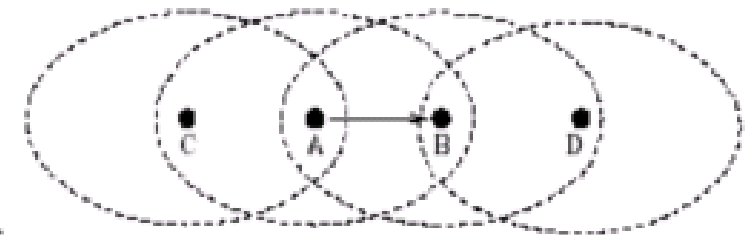
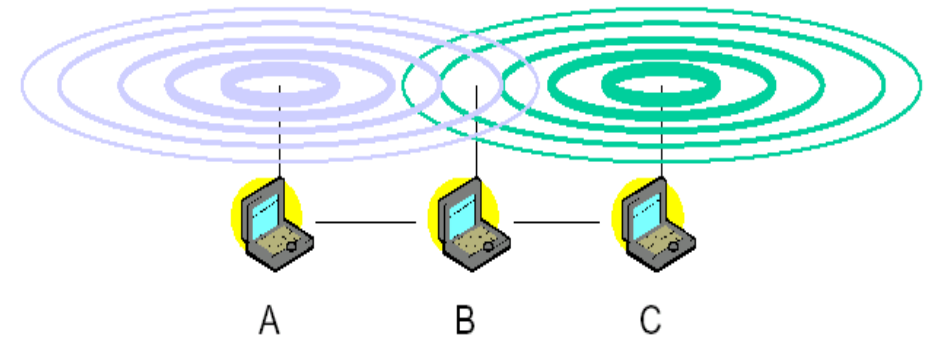
| Time | PHY Rate | Source | Destination | Protocol | Info |
|----------|----------|---------------|-------------|----------|---------------------|
| 3.379609 | 54.0 | 172.16.63.215 | 172.16.50.1 | ICMP | Echo (ping) request |
| 3.379777 | 54.0 | 172.16.63.215 | 172.16.50.1 | ICMP | Echo (ping) request |
| 3.380249 | 54.0 | 172.16.63.215 | 172.16.50.1 | ICMP | Echo (ping) request |
| 3.381145 | 54.0 | 172.16.63.215 | 172.16.50.1 | ICMP | Echo (ping) request |
| 3.381735 | 48.0 | 172.16.63.215 | 172.16.50.1 | ICMP | Echo (ping) request |
| 3.385290 | 48.0 | 172.16.63.215 | 172.16.50.1 | ICMP | Echo (ping) request |
| 3.421509 | 48.0 | 172.16.63.215 | 172.16.50.1 | ICMP | Echo (ping) request |
| 3.423516 | 36.0 | 172.16.63.215 | 172.16.50.1 | ICMP | Echo (ping) request |
| 3.440587 | 36.0 | 172.16.63.215 | 172.16.50.1 | ICMP | Echo (ping) request |
| 3.449311 | 36.0 | 172.16.63.215 | 172.16.50.1 | ICMP | Echo (ping) request |
| 3.465505 | 36.0 | 172.16.63.215 | 172.16.50.1 | ICMP | Echo (ping) request |
| 3.467551 | 24.0 | 172.16.63.215 | 172.16.50.1 | ICMP | Echo (ping) request |
| 3.473262 | 24.0 | 172.16.63.215 | 172.16.50.1 | ICMP | Echo (ping) request |
| 3.477246 | 24.0 | 172.16.63.215 | 172.16.50.1 | ICMP | Echo (ping) request |
| 3.415667 | 24.0 | 172.16.63.215 | 172.16.50.1 | ICMP | Echo (ping) request |
| 3.420031 | 24.0 | 172.16.63.215 | 172.16.50.1 | ICMP | Echo (ping) request |
| 3.420602 | 18.0 | 172.16.63.215 | 172.16.50.1 | ICMP | Echo (ping) request |
| 3.448302 | 18.0 | 172.16.63.215 | 172.16.50.1 | ICMP | Echo (ping) request |
| 3.470822 | 18.0 | 172.16.63.215 | 172.16.50.1 | ICMP | Echo (ping) request |
| 3.520808 | 18.0 | 172.16.63.215 | 172.16.50.1 | ICMP | Echo (ping) request |
| 3.532584 | 12.0 | 172.16.63.215 | 172.16.50.1 | ICMP | Echo (ping) request |
| 3.587616 | 12.0 | 172.16.63.215 | 172.16.50.1 | ICMP | Echo (ping) request |
| 3.286032 | 11.0 | 172.16.63.215 | 172.16.50.1 | ICMP | Echo (ping) request |
| 3.302502 | 11.0 | 172.16.63.215 | 172.16.50.1 | ICMP | Echo (ping) request |
| 3.326484 | 11.0 | 172.16.63.215 | 172.16.50.1 | ICMP | Echo (ping) request |
| 3.365331 | 11.0 | 172.16.63.215 | 172.16.50.1 | ICMP | Echo (ping) request |
| 3.368087 | 5.5 | 172.16.63.215 | 172.16.50.1 | ICMP | Echo (ping) request |
| 3.388501 | 5.5 | 172.16.63.215 | 172.16.50.1 | ICMP | Echo (ping) reply |
| 3.391612 | 5.5 | 172.16.63.215 | 172.16.50.1 | ICMP | Echo (ping) reply |
| 3.393055 | 2.0 | 172.16.63.215 | 172.16.50.1 | ICMP | Echo (ping) reply |
| 3.397234 | 2.0 | 172.16.63.215 | 172.16.50.1 | ICMP | Echo (ping) reply |

| | | | | | | | | | | |
|---|--|--|--|--|--|--|--|--|--|--|
| Frame 2184: 166 bytes on wire (1328 bits), Veriwave Radiotap Header v1, Length 72 | | | | | | | | | | |
| Actual frame length: 98 | | | | | | | | | | |
| Flags: 0x0000 | | | | | | | | | | |
| Data rate: 48.0 Mb/s | | | | | | | | | | |
| Channel type: 802.11a/g (OFDM) (0x0040) | | | | | | | | | | |
| RX SSI signal: -57 dBm | | | | | | | | | | |
| Frame direction: Received (0) | | | | | | | | | | |
| MAC FCS check: OK (0) | | | | | | | | | | |
| Decryption error: Decrypt succeeded (0) | | | | | | | | | | |
| TX retry limit: Retry limit not reached | | | | | | | | | | |
| Encryption type: No encryption (0) | | | | | | | | | | |
| MSDU length: 98 | | | | | | | | | | |
| Info field: 0x0000 | | | | | | | | | | |
| Errors: 0x0000000c | | | | | | | | | | |
| Flow ID: 0 | | | | | | | | | | |
| Client ID: 3 | | | | | | | | | | |
| Vw frame number: 0 | | | | | | | | | | |
| Frame timestamp values: | | | | | | | | | | |
| IEEE 802.11 QoS Data, Flags:R..T | | | | | | | | | | |
| Logical-Link Control | | | | | | | | | | |
| Internet Protocol, Src: 172.16.63.215 (172.16.63.215) | | | | | | | | | | |
| Internet Control Message Protocol | | | | | | | | | | |

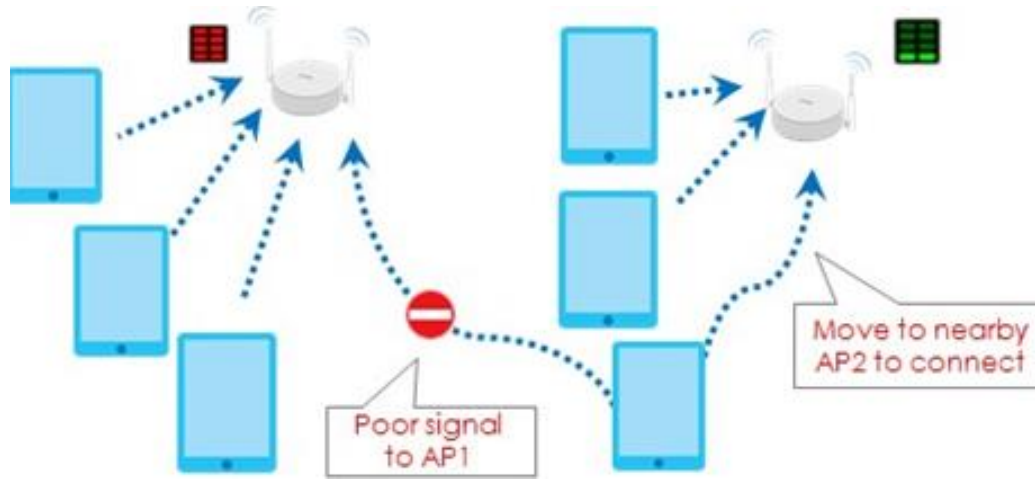
When the signal strength decreases the transmitting unit will drop its data rate to the next lower data rate in order to maintain a reasonable SNR

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

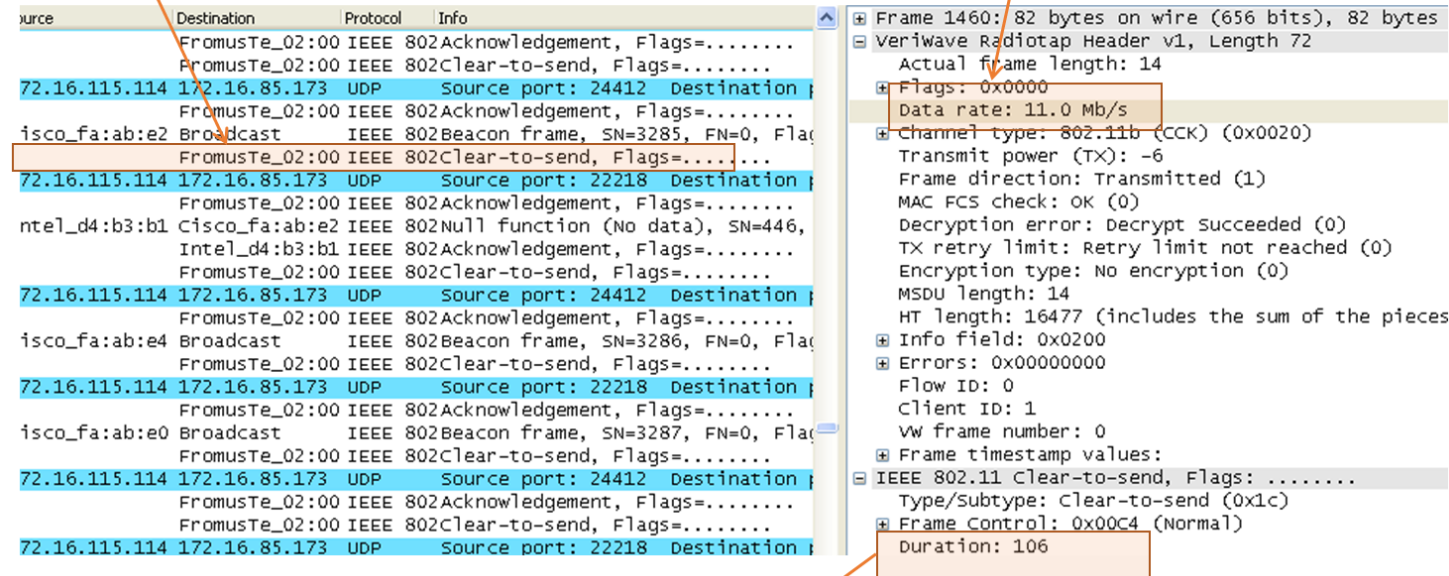
- 2.4GHz has lesser bandwidth and hence cannot support too many clients
- APs can choose to steer some clients from 2.4GHz to 5GHz band.

Legacy Protection and Greenfield Mode

- 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



The image shows a Wireshark packet capture analysis. The left pane displays a list of packets with columns for Source, Destination, Protocol, and Info. The right pane shows the details of the selected packet (Frame 1460), including the Veriwave Radiotap Header, Flags, Data rate (11.0 Mb/s), Channel type (802.11b (CCK) (0x0020)), and IEEE 802.11 Clear-to-send (CTS) frame details (Type/Subtype: Clear-to-send (0x1c), Frame Control: 0x00C4 (Normal), Duration: 106).

| Source | Destination | Protocol | Info |
|----------------|----------------|----------|----------------------------------|
| FromusTe_02:00 | FromusTe_02:00 | IEEE 802 | Acknowledgement, Flags=..... |
| FromusTe_02:00 | FromusTe_02:00 | IEEE 802 | Clear-to-send, Flags=..... |
| 72.16.115.114 | 172.16.85.173 | UDP | Source port: 24412 Destination |
| FromusTe_02:00 | FromusTe_02:00 | IEEE 802 | Acknowledgement, Flags=..... |
| isco_fa:ab:e2 | Broadcast | IEEE 802 | Beacon frame, SN=3285, FN=0, Fla |
| FromusTe_02:00 | FromusTe_02:00 | IEEE 802 | Clear-to-send, Flags=..... |
| 72.16.115.114 | 172.16.85.173 | UDP | Source port: 22218 Destination |
| FromusTe_02:00 | FromusTe_02:00 | IEEE 802 | Acknowledgement, Flags=..... |
| ntel_d4:b3:b1 | Cisco_fa:ab:e2 | IEEE 802 | Null function (No data), SN=446, |
| Intel_d4:b3:b1 | Intel_d4:b3:b1 | IEEE 802 | Acknowledgement, Flags=..... |
| FromusTe_02:00 | FromusTe_02:00 | IEEE 802 | Clear-to-send, Flags=..... |
| 72.16.115.114 | 172.16.85.173 | UDP | Source port: 24412 Destination |
| FromusTe_02:00 | FromusTe_02:00 | IEEE 802 | Acknowledgement, Flags=..... |
| isco_fa:ab:e4 | Broadcast | IEEE 802 | Beacon frame, SN=3286, FN=0, Fla |
| FromusTe_02:00 | FromusTe_02:00 | IEEE 802 | Clear-to-send, Flags=..... |
| 72.16.115.114 | 172.16.85.173 | UDP | Source port: 22218 Destination |
| FromusTe_02:00 | FromusTe_02:00 | IEEE 802 | Acknowledgement, Flags=..... |
| isco_fa:ab:e0 | Broadcast | IEEE 802 | Beacon frame, SN=3287, FN=0, Fla |
| FromusTe_02:00 | FromusTe_02:00 | IEEE 802 | Clear-to-send, Flags=..... |
| 72.16.115.114 | 172.16.85.173 | UDP | Source port: 24412 Destination |
| FromusTe_02:00 | FromusTe_02:00 | IEEE 802 | Acknowledgement, Flags=..... |
| FromusTe_02:00 | FromusTe_02:00 | IEEE 802 | Clear-to-send, Flags=..... |
| 72.16.115.114 | 172.16.85.173 | UDP | Source port: 22218 Destination |

Frame 1460: 82 bytes on wire (656 bits), 82 bytes
Veriwave Radiotap Header v1, Length 72
Actual frame length: 14
Flags: 0x0000
Data rate: 11.0 Mb/s
Channel type: 802.11b (CCK) (0x0020)
Transmit power (TX): -6
Frame direction: Transmitted (1)
MAC FCS check: OK (0)
Decryption error: Decrypt succeeded (0)
TX retry limit: Retry limit not reached (0)
Encryption type: No encryption (0)
MSDU length: 14
HT length: 16477 (includes the sum of the pieces)
Info field: 0x0200
Errors: 0x00000000
Flow ID: 0
Client ID: 1
Vw frame number: 0
Frame timestamp values:
IEEE 802.11 Clear-to-send, Flags:
Type/Subtype: Clear-to-send (0x1c)
Frame Control: 0x00C4 (Normal)
Duration: 106

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.

| Destination | Protocol | Info |
|------------------|----------|-----------------------------------|
| 1 Broadcast | IEEE 802 | Beacon frame, SN=2435, FN=0, Flag |
| 1 Broadcast | IEEE 802 | Beacon frame, SN=2437, FN=0, Flag |
| 1 Broadcast | IEEE 802 | Beacon frame, SN=2439, FN=0, Flag |
| 1 Broadcast | IEEE 802 | Beacon frame, SN=2440, FN=0, Flag |
| 1 Broadcast | IEEE 802 | Beacon frame, SN=2441, FN=0, Flag |
| 1 Broadcast | IEEE 802 | Beacon frame, SN=2442, FN=0, Flag |
| 1 Broadcast | IEEE 802 | Beacon frame, SN=2443, FN=0, Flag |
| 1 Broadcast | IEEE 802 | Beacon frame, SN=2444, FN=0, Flag |
| 1 Broadcast | IEEE 802 | Beacon frame, SN=2444, FN=0, Flag |
| 1 Broadcast | IEEE 802 | Beacon frame, SN=2445, FN=0, Flag |
| 1 Broadcast | IEEE 802 | Beacon frame, SN=2446, FN=0, Flag |
| 1 Broadcast | IEEE 802 | Beacon frame, SN=2447, FN=0, Flag |
| 1 Broadcast | IEEE 802 | Beacon frame, SN=2448, FN=0, Flag |
| 1 Broadcast | IEEE 802 | Beacon frame, SN=2449, FN=0, Flag |
| 1 Broadcast | IEEE 802 | Beacon frame, SN=2450, FN=0, Flag |
| Northsta_02:00 | IEEE 802 | Acknowledgement, Flags=..... |
| TrapezeN_91:dd | IEEE 802 | Power-Save poll, Flags=...P... |
| 192.168.1.188 | UDP | source port: 23286 Destination |
| TrapezeN_91:dd | IEEE 802 | Acknowledgement, Flags=..... |
| Northsta_02:00 | IEEE 802 | Acknowledgement, Flags=..... |
| 0 TrapezeN_91:dd | IEEE 802 | Power-Save poll, Flags=...P... |
| Northsta_02:00 | IEEE 802 | Acknowledgement, Flags=..... |
| 0 TrapezeN_91:dd | IEEE 802 | Power-Save poll, Flags=...P... |
| 192.168.1.188 | UDP | source port: 23286 Destination |
| TrapezeN_91:dd | IEEE 802 | Acknowledgement, Flags=..... |
| 192.168.1.188 | UDP | source port: 23286 Destination |
| TrapezeN_91:dd | IEEE 802 | Acknowledgement, Flags=..... |
| Northsta_02:00 | IEEE 802 | Acknowledgement, Flags=..... |
| 0 TrapezeN_91:dd | IEEE 802 | Power-Save poll, Flags=...P... |
| Northsta_02:00 | IEEE 802 | Acknowledgement, Flags=..... |

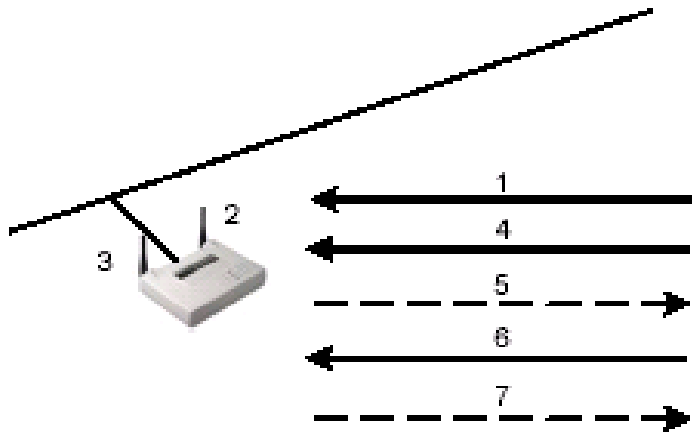
Frame 565: 339 bytes on wire (2712 bits), 339 bytes captured on interface 0

- VeriWave Radiotap Header v1, Length 72
- IEEE 802.11 Beacon frame, Flags:
- IEEE 802.11 wireless LAN management frame
 - Fixed parameters (12 bytes)
 - Tagged parameters (231 bytes)
 - SSID parameter set
 - Supported Rates: 6.0(B) 9.0 12.0(B) 18.0 24.0(B) 36.0
 - DS Parameter set: Current Channel: 100
 - Traffic Indication Map (TIM): DTIM 0 of 1 bitmap 1 2
 - Country Information: Country Code: US, Any Environment
 - Power Constraint: Tag 32 Len 1
 - TPC Report
 - QSS Load Element
 - Reserved tag number: Tag 67 Len 2
 - Vendor Specific: Trapezen
 - Vendor Specific: Trapezen
 - Vendor Specific: Microsoft: WME
 - Vendor Specific: Microsoft: WME
 - HT Capabilities (802.11n D1.10)
 - HT Information (802.11n D1.10)

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

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.

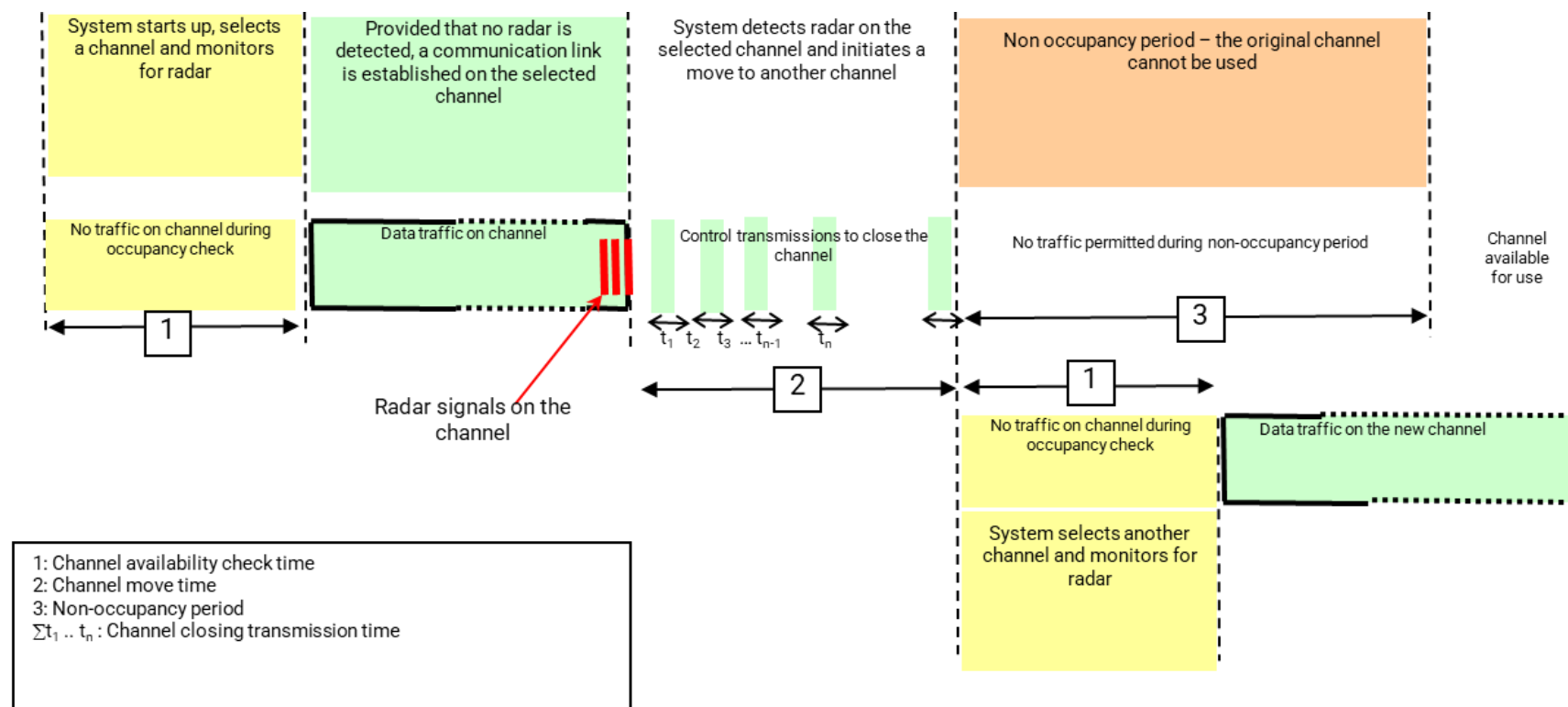
Step4: AP sends one buffered frame to the client with the "More Data" bit set if there is more buffered data.



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

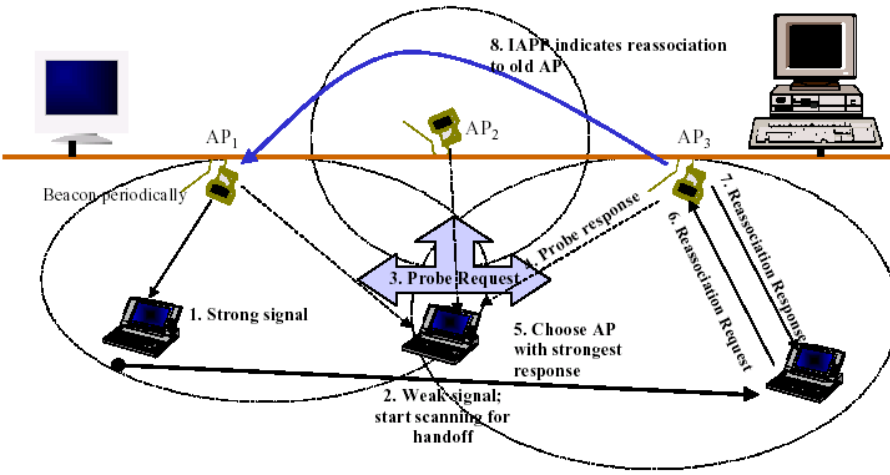
Dynamic Frequency Selection (DFS)

- 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. 802.11 a/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 msec

| No. | Time | Delta Time | PHY Rate | Source | Destination | Protocol | Info |
|-----------|-----------|------------|----------|----------------|------------------|------------------|----------|
| 14.097104 | 14.097104 | 0.000000 | 24.0 | | | IEEE 802Acknowle | |
| 14.094649 | 14.094649 | 0.007465 | 1.0 | Cisco_fa:ab:e | Broadcast | IEEE 802Beacon f | |
| 14.097093 | 14.097093 | 0.002444 | 54.0 | 172.16.86.171 | 172.16.138.65 | TFTP | Unknown |
| 14.097173 | 14.097173 | 0.000080 | 24.0 | | Cisco_fa:ab:e2 | IEEE 802Acknowle | |
| 14.107089 | 14.107089 | 0.009916 | 54.0 | 172.16.86.171 | 172.16.138.65 | TFTP | Unknown |
| 14.107795 | 14.107795 | 0.000706 | 54.0 | 172.16.86.171 | 172.16.138.65 | TFTP | Unknown |
| 14.108509 | 14.108509 | 0.000714 | 48.0 | 172.16.86.171 | 172.16.138.65 | TFTP | Unknown |
| 14.109407 | 14.109407 | 0.000898 | 36.0 | 172.16.86.171 | 172.16.138.65 | TFTP | Unknown |
| 14.110114 | 14.110114 | 0.000707 | 24.0 | 172.16.86.171 | 172.16.138.65 | TFTP | Unknown |
| 14.110637 | 14.110637 | 0.000523 | 18.0 | 172.16.86.171 | 172.16.138.65 | TFTP | Unknown |
| 14.111314 | 14.111314 | 0.000677 | 12.0 | 172.16.86.171 | 172.16.138.65 | TFTP | Unknown |
| 14.112028 | 14.112028 | 0.000714 | 11.0 | 172.16.86.171 | 172.16.138.65 | TFTP | Unknown |
| 14.113262 | 14.113262 | 0.001234 | 1.0 | Cisco_fa:ab:e | Abbottdi_01:00 | IEEE 802Request- | |
| 14.114175 | 14.114175 | 0.000913 | 1.0 | Cisco_fa:ab:e | Abbottdi_01:00 | IEEE 802Request- | |
| 14.114989 | 14.114989 | 0.000814 | 1.0 | Cisco_fa:ab:e | Abbottdi_01:00 | IEEE 802Request- | |
| 14.115500 | 14.115500 | 0.000511 | 54.0 | Intel_d4:b3:b | Cisco_fa:ab:e2 | IEEE 802Null fur | |
| 14.115542 | 14.115542 | 0.000042 | 24.0 | Intel_d4:b3:b | IEEE 802Acknowle | | |
| 14.116216 | 14.116216 | 0.000674 | 1.0 | Cisco_fa:ab:e | Abbottdi_01:00 | IEEE 802Request- | |
| 14.117309 | 14.117309 | 0.001093 | 1.0 | Cisco_fa:ab:e | Abbottdi_01:00 | IEEE 802Request- | |
| 14.118276 | 14.118276 | 0.000967 | 1.0 | Cisco_fa:ab:e | Abbottdi_01:00 | IEEE 802Request- | |
| 14.119226 | 14.119226 | 0.000950 | 1.0 | Cisco_fa:ab:e | Broadcast | IEEE 802Beacon f | |
| 14.121213 | 14.121213 | 0.001987 | 1.0 | Cisco_fa:ab:e | Abbottdi_01:00 | IEEE 802Request- | |
| 14.121937 | 14.121937 | 0.000724 | 1.0 | Cisco_fa:ab:e | Abbottdi_01:00 | IEEE 802Request- | |
| 14.122378 | 14.122378 | 0.000441 | 54.0 | Intel_d4:b3:b | Cisco_fa:ab:e2 | IEEE 802Null fur | |
| 14.122420 | 14.122420 | 0.000042 | 24.0 | Intel_d4:b3:b | IEEE 802Acknowle | | |
| 14.131519 | 14.131519 | 0.009099 | 1.0 | Cisco_fa:ab:e | Broadcast | IEEE 802Beacon f | |
| 14.143806 | 14.143806 | 0.012287 | 1.0 | Cisco_fa:ab:e | Broadcast | IEEE 802Beacon f | |
| 14.197055 | 14.197055 | 0.053249 | 1.0 | Cisco_fa:ab:e | Broadcast | IEEE 802Beacon f | |
| 14.217181 | 14.217181 | 0.020126 | 54.0 | 98:d1:50:27:a | Cisco_fa:ab:e2 | IEEE 802Null fur | |
| 14.217225 | 14.217225 | 0.000044 | 24.0 | Intel_d4:b3:b | IEEE 802Acknowle | | |
| 14.217805 | 14.217805 | 0.000580 | 54.0 | 172.16.50.245 | 172.16.63.215 | ICMP | Echo (p |
| 14.217860 | 14.217860 | 0.000055 | 24.0 | Cisco_fa:ab:e2 | IEEE 802Acknowle | | |
| 14.218919 | 14.218919 | 0.001059 | 54.0 | 154.16.63.215 | 172.16.50.245 | IP | Fragment |
| 14.218970 | 14.218970 | 0.000051 | 24.0 | | Intel_d4:b3:b | IEEE 802Acknowle | |
| 14.221631 | 14.221631 | 0.002661 | 1.0 | Cisco_fa:ab:e | Broadcast | IEEE 802Beacon f | |
| 14.233916 | 14.233916 | 0.012285 | 1.0 | Cisco_fa:ab:e | Broadcast | IEEE 802Beacon f | |
| 14.246204 | 14.246204 | 0.012288 | 1.0 | Cisco_fa:ab:e | Broadcast | IEEE 802Beacon f | |
| 14.299454 | 14.299454 | 0.053250 | 1.0 | Cisco_fa:ab:e | Broadcast | IEEE 802Beacon f | |
| 14.324030 | 14.324030 | 0.024576 | 1.0 | Cisco_fa:ab:e | Broadcast | IEEE 802Beacon f | |

| Time | Delta Time | PHY Rate | Source | Destination | Protocol | Info |
|----------|------------|----------|----------------|----------------------|------------------------------|------------------|
| 14.20958 | 0.03520 | 1.0 | Cisco_fa:ab:e2 | Broadcast | IEEE 802Beacon f | |
| 14.22486 | 0.015482 | 24.0 | Abbottdi_0:0 | Cisco_fb:27:12 | IEEE 802Probe Request | SN=0 |
| 14.22491 | 0.000055 | 24.0 | | Abbottdi_01:00 | IEEE 802Acknowledge | Flag |
| 14.22499 | 0.000081 | 1.0 | Cisco_fa:2 | Abbottdi_01:00 | IEEE 802Probe Response | SN=37 |
| 14.22666 | 0.001666 | 1.0 | | Cisco_fb:27:12 | IEEE 802Acknowledge | Flag |
| 14.22775 | 0.001091 | 24.0 | Abbottdi_0:0 | Cisco_fb:27:12 | IEEE 802Authentication | SN=1 |
| 14.22780 | 0.000051 | 24.0 | | Abbottdi_01:00 | IEEE 802Acknowledge | Flag |
| 14.22818 | 0.000373 | 11.0 | Cisco_fb:2 | Abbottdi_01:00 | IEEE 802Authentication | SN=37 |
| 14.22840 | 0.000227 | 11.0 | | Cisco_fb:27:12 | IEEE 802Acknowledge | Flag |
| 14.22976 | 0.001353 | 24.0 | Abbottdi_0:0 | Cisco_fb:27:12 | IEEE 802Association Request | |
| 14.22981 | 0.000059 | 24.0 | | Abbottdi_01:00 | IEEE 802Acknowledge | Flag |
| 14.23119 | 0.001371 | 11.0 | Cisco_fb:2 | Abbottdi_01:00 | IEEE 802Association Response | |
| 14.23142 | 0.000239 | 11.0 | | Cisco_fb:27:12 | IEEE 802Acknowledge | Flag |
| 14.23396 | 0.002532 | 1.0 | | Cisco_fb:2 Broadcast | IEEE 802Beacon frame | SN=3703 |
| 14.24016 | 0.006200 | 54.0 | 172.16.86.172 | 172.16.138.65 | TFTP | unknown (0xdd01) |
| 14.24024 | 0.000080 | 24.0 | | Cisco_fb:27:12 | IEEE 802Acknowledge | Flag |
| 14.24625 | 0.006009 | 1.0 | Cisco_fb:2 | Broadcast | IEEE 802Beacon frame | SN=3705 |
| 14.25012 | 0.003875 | 54.0 | 172.16.86.172 | 172.16.138.65 | TFTP | unknown (0xdd01) |
| 14.25020 | 0.000080 | 24.0 | | Cisco_fb:27:12 | IEEE 802Acknowledge | Flag |
| 14.25853 | 0.008333 | 1.0 | Cisco_fb:2 | Broadcast | IEEE 802Beacon frame | SN=3707 |
| 14.26054 | 0.002008 | 54.0 | 172.16.86.172 | 172.16.138.65 | TFTP | unknown (0xdd01) |
| 14.26062 | 0.000080 | 24.0 | | Cisco_fb:27:12 | IEEE 802Acknowledge | Flag |
| 14.27014 | 0.009516 | 54.0 | 172.16.86.172 | 172.16.138.65 | TFTP | unknown (0xdd01) |
| 14.27022 | 0.000080 | 24.0 | | Cisco_fb:27:12 | IEEE 802Acknowledge | Flag |
| 14.28012 | 0.009905 | 54.0 | 172.16.86.172 | 172.16.138.65 | TFTP | unknown (0xdd01) |
| 14.28020 | 0.000080 | 24.0 | | Cisco_fb:27:12 | IEEE 802Acknowledge | Flag |
| 14.29211 | 0.011906 | 54.0 | 172.16.86.172 | 172.16.138.65 | TFTP | unknown (0xdd01) |
| 14.29219 | 0.000080 | 24.0 | | Cisco_fb:27:12 | IEEE 802Acknowledge | Flag |
| 14.30012 | 0.007936 | 54.0 | 172.16.86.172 | 172.16.138.65 | TFTP | unknown (0xdd01) |
| 14.30020 | 0.000080 | 24.0 | | Cisco_fb:27:12 | IEEE 802Acknowledge | Flag |
| 14.31012 | 0.009917 | 54.0 | 172.16.86.172 | 172.16.138.65 | TFTP | unknown (0xdd01) |
| 14.31020 | 0.000080 | 24.0 | | Cisco_fb:27:12 | IEEE 802Acknowledge | Flag |
| 14.31178 | 0.001581 | 1.0 | Cisco_fb:2 | Broadcast | IEEE 802Beacon frame | SN=3714 |
| 14.32012 | 0.008335 | 54.0 | 172.16.86.172 | 172.16.138.65 | TFTP | unknown (0xdd01) |
| 14.32020 | 0.000080 | 24.0 | | Cisco_fb:27:12 | IEEE 802Acknowledge | Flag |
| 14.33012 | 0.009922 | 54.0 | 172.16.86.172 | 172.16.138.65 | TFTP | unknown (0xdd01) |
| 14.33020 | 0.000080 | 24.0 | | Cisco_fb:27:12 | IEEE 802Acknowledge | Flag |
| 14.33636 | 0.006156 | 1.0 | Cisco_fb:2 | Broadcast | IEEE 802Beacon frame | SN=3717 |
| 14.34012 | 0.003767 | 54.0 | 172.16.86.172 | 172.16.138.65 | TFTP | unknown (0xdd01) |

AP1 Capture

AP2 Capture

References



802.11 Network Service Set

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



QUIZ!

TIME

Quiz 2d Results

Number of participants - 124



Winner
Pradyumna

INDIA

Score distribution - quiz 2d

