ACCESS POINT:

1. An access point is the switch like intelligent device which basically bridges wireless network with the wired network and it is the central device in a wireless network that creates and manages the Wi‑Fi network, providing a gateway between wireless clients and the wired network (or the internet).
2. AP can have either single or dual radio with each having unique BSSID working in different frequencies for enhanced throughput in case of wireless backhaul.
3. It involves in switch like operations such as associating the devices to it with unique MAC address for its radio and encodes the packets from clients in RF modulated form to 802.3 form compatible for backhaul communication and vice versa. It also involves in CSMA-CA access control technique since wireless clients are involved.
4. It is different from wireless router and / or wireless extender in the way that it creates the wireless LAN and doesn’t involve in routing the packets to internet directly or doesn’t extend the coverage by rebroadcasting. It predominantly works on Ethernet backhaul whereas extender works on existing Wi-Fi network.
5. Types of AP – Standalone AP, cloud managed AP, Mesh AP, Controller based AP.
6. Standalone AP is self-sufficient device that itself provides wireless connectivity and involves in secured association process without any external controller that is initial configuration can be done from GUI or SNMP. It itself implements all security protocols like WPA and ACL etc.
7. AP (mostly Standalone AP) can help in wireless network segmentation (Wireless - VLAN) by mapping unique SSID to unique VLAN. Mostly an AP will allow 16 different VLAN. AP itself can handle VLAN communication if source client does not require to talk to destination client in wired network. In that case, it requires managed switch. However, it requires Router to facilitate inter-VLAN communication.
8. Standalone AP can work in infrastructure, bridge, repeater, mesh mode.
9. AP will broadcast SSID (Logical Human friendly network name with maximum of 32 characters and case sensitive) and also BSSID (MAC address of AP for machines to get associated to)
10. It manages the association of clients to it by 4 way handshaking.
11. It involves in Encapsulating / Decapsulating the frames. That is, whenever wireless clients wants to have communication with wired infrastructure, AP will decapsulate the ethernet frame in it and sends to main network and does the reverse for reply to clients from main network. This is called Integration Service where it decapsulates MSDU (MAC Service Data Unit) from 802.11 frame and places that payload in 802.3 Ethernet frame and vice-versa.
12. It dynamically chooses the channel and wifi frequency in modern systems. (DFS).
13. It works with Encryption ,Security (WPA) protocols, Hidden SSID, MAC based filtering to ensure secured data transfer and safety in associating the clients during four way handshake.
14. It works with 802.11e QoS standard in prioritizing the clients request based on the data it wants to transmit.
15. It works with roaming optimization standards to provide seamless switching experience for clients in case of roaming inside the extended service set using Distribution System (with appropriate backhaul).
16. It works in different modes like root , bridge , repeater, mesh, client modes.
17. For a client to get associated with AP, following are required
18. Scanning – it is the process by which client device will discover the available Access points. There are two scanning methods. They are Passive and Active scanning.
19. Passive scanning is the most efficient and popular scanning methods in which AP will periodically broadcast BEACON frame which consists of SSID , BSSID , encryption standards, supported data rates , frequency in use and channel number etc. Station will choose an AP based on RSSI (Received Signal Strength Indicator)
20. Active Scanning – here, stations will broadcast the PROBE request to all AP in the needed channel and expects Probe reply from AP’s. now station chooses AP based on RSSI.
21. Authentication – Phase where client sends Authentication request to AP and expects Authentication reply from AP. Involves four way handshaking if WPA based security protocols involved. It is the phase where based on authentication done before with the help of 802.1X EAP , A Nonce, S Nonce, PSK , PMK, PTK, GTK, Passphrase, PBKDF.
22. Association – final phase where client will get associated with particular AP and obtains Association ID.
23. Modern AP supports MIMO , OFDMA (by allocating Resource Units – continguous subcarriers (tradeoff between channel width , interference and maximum data rate , reduced range on wider channel), to each other based on data size and priority and ), Dynamic Band selection, Beamforming, BSS Coloring, more wider channels include 160 MHz, target wake time (TWT) etc.
24. Generally AP will get its IP from main network’s DHCP server for management purposes however while bridging it just extends the wireless clients in getting IP from main network only. It doesn’t perform even NAT like router in extender or default mode.
25. AP in Bridged Mode :
    1. In this mode, AP acts as L-2 Device.
    2. It simply bridges wireless clients to wired main infrastructure and creates single broadcast domain.
    3. It gets its IP from main network’s DHCP and provides transparency to its associated clients in the way that it lets wireless clients receive all network information from main network itself (both wired and wireless stations remain in the same subnet only as of main network).
    4. It connects two wired network segments over wifi Link with two radios. One for communicating with its own clients and other to communicate with main network wirelessly (wireless backhaul).
    5. AP in bridged mode should either support wired or wireless backhaul to get internet access.
    6. Channel throughput or bandwidth will not get affected in this mode.
    7. Predominantly used when Ethernet devices want wifi access or wifi clients want to participate in wired network infrastructure.
    8. It joins as a client to the actual wifi network.
26. AP in Repeater Mode :
    1. Here, AP (in the name of extender or repeater) just extends the existing wifi (wireless part) network by repeating the signal.
    2. That is, it receives original wifi signals from actual AP (AP in bridged mode) and re-broadcasts it to the clients which are physically far away from main AP or present in the dead zone.
    3. Repeater device will get connected to main AP as one of the clients and boosts the existing signal to increase the range of the wifi network from main AP.
    4. In this mode, effective throughput will be atleast reduced by half since it works on the same channel as AP works.
    5. AP in repeater mode may create its own network with new subnet and does routing individually if needed.
    6. It may create its own broadcast SSID.
27. Recent Advancements in AP :

* MLO (Multi-Link Operation): it is one of the features of Wifi-7 which lets AP uses more than one radio thereby enabling simultaneous transmission and reception.
  1. It reduces congestion and traffic latency of single channel wifi.
  2. It also involves in channel aggregation that is combining bandwidth of channels for higher speed.
  3. Has two types – simultaneous (multiple bands at same time) and alternating (switches between links dynamically)
  4. Does load balancing by dynamically selecting the link for lower latency.
  5. Does packet scheduling by sending packets of even same user in different available channel for efficient data delivery.
* BSS COLORING : it is one of the features in Wifi-6 that reduces interference in dense environments and improves spatial reuse of frequencies.
* In general, if AP’s work with same frequency , they may interfere with each other.
* In accordance to this, every client will wait before transmitting even if the transaction is going on in different network (managed by different AP) just because they are in same frequency.
* BSS coloring solves this issue by assigning ID so that devices identify overlapping BSS and ignore non-relevant signals.
* However, analyzing BSS should not consume power and time. So , AP will broadcast BSS color while beaconing and each frame what client receives will get processed by client to identify its BSS in PHY header (High Efficiency Signal Field) itself not in MAC header and drops the packet if color is different and RSSI is relatively lower. However, If color is same, then device follows CSMA-CA rules only.

1. ASSOCIATION PROCESS IN AP:

* Passive Scanning is the process by which AP periodically broadcasts beacon frames on each channel.
* Beacon signals will have information like SSID , BSSID , Color, duration, supported data rates, encryption techniques and security protocol info.
* Client listens to that and selects AP based on parameters and RSSI.
* In Active scanning, STA will broadcast or selectively give some SSID in the form of probe request and will get probe responses and select AP based on RSSI.
* The scanning process will be followed by Authentication. It is done based on WPA2 (Wifi Protected Access - 2) or 3 security protocol from Wifi Alliance.
* Uses Encryption Standard like AES with CCMP – block chaining.
* Uses authentication mechanisms like Pre-Shared Key which is derived from wifi password with forward secrecy.
* Should use Enhanced Open authentication in public places.
* Uses PSK based on wifi password and SSID and derives PMK based on PSK , SSID, Hash MAC. Thus, PMK will be used in 4 way handshake.
* In 4-way handshake, AP sends ANonce to client first. Based on this and S Nonce from station end, it calculates PTK and sends MIC along with Encryption key to AP. AP sends GTK encrypted with Encryption key. Followed by, client acknowledges the GTK reception.
* This authentication may have KRACK (Key Reinstallation Attack) – may force client to reuse old keys by replaying attack. Offline dictionary attack – may capture handshaking packets and in brute force attack. If no forward secrecy, then after decryption, attacker can go through past traffic.
* Uses 802.1X authentication with RADIUS server for authentication. In 802.1X authentication, supplicant requests for authentication to AP which forwards the request to RADIUS (Remote Authentication Dial-In User Service) server that use EAP (Extensible Authentication Protocol)