QUESTION : WHAT IS BSS AND ESS AND WIFI TOPOLOGIES

In general, Wifi network is divided in terms of Service sets which defines how devices interact with each other. They are,

1. Independent Basic Service Set
2. Infrastructure Service Set (BSS and ESS via DS)
3. Mesh Service Set
4. Quality of Service Basic Service Set

All Service sets work with same SSID only to provide efficient connection to clients or stations even in the case of roaming.

INDEPENDENT BASIC SERVICE SET :

1. Network formed solely with Client stations and not using Access Points.
2. Every nodes participating in IBSS is peer. No need to route between peers for data transfer since they can directly communicate with destination node supporting ad-hoc network architecture.
3. Every node should understand the half duplex nature therefore one node can transmit data at a time as like in wifi.
4. A node starting communication should generate virtual BSSID for identification purposes inside IBSS.
5. Use case : To form short time wifi based networks (Eg: the post disaster scenario where conventional infrastructure would have been destroyed) between rescue devices or to temporarily connect devices for file transfer etc.

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. Types of AP – Standalone AP , cloud managed AP , Mesh AP, Controller based AP.
3. 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)
4. It manages the association of clients to it by 4 way handshaking.
5. 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.
6. It dynamically chooses the channel and wifi frequency in modern systems. (DFS).
7. 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.
8. It works with 802.11e QoS standard in prioritizing the clients request based on the data it wants to transmit.
9. 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).
10. It works in different modes like root , bridge , repeater, mesh, client modes.
11. For a client to get associated with AP, following are required
12. 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.
13. 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)
14. 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.
15. 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.
16. Association – final phase where client will get associated with particular AP and obtains Association ID.

BASIC SERVICE SET :

1. This is the basic and smallest wifi network with atmost one Access Point (AP) or none in case of ad-hoc network with only peers.
2. The single AP will have its own BSSID (Basic Service Set Identifier) and this connects all wireless clients. Communication between wireless clients is handled by AP which uses single radio channel (this is the core of Infrastructure Mode). However, if client nodes support Wifi Direct, they can bypass AP and communicate directly. (Wifi P2P is the simple scheme which also uses underlying wifi technology but forms a small network with one device as AP and remaining as clients with easy setup and uses WPA2 for security.)
3. AP used here will have its own Boundary called Cell (physical area coverage in BSS) (Basic Service Area). (Generally BSA need not be equidistant due to directional antenna gain in AP and transmit power and effect of surroundings) within which it advertises BSSID (Generally SSID) for clients to associated with the single point of contact (AP) in BSS.
4. More similar to Hub based Ethernet LAN where all the traffic from clients should pass through AP.
5. It is also possible to segment the single wireless network into multiple segments with the help of VLAN where managed switch will take of multiple VLAN tagging and router on stick concept can be applied to have Inter VLAN routing.
6. Access points in modern systems can broadcast multiple SSIDs for different segments.
7. Use case : a small office network comprising of single AP with 10 or more computers connected to it and getting internet access. AP will be connected to main network infrastructure like router or switch in wired backhaul.

DISTRIBUTION SYSTEM :

1. It is basically the integration of many BSS Aps via Ethernet LAN (wired backhaul) or wireless backhaul both commonly referred to DSM (Distribution System Medium) to have inter AP communication called ESS.
2. DSS (Distribution System Software) which is running on each AP to manage the associations and disassociations with Clients and also managing Distribution System Communication.
3. WDS (Wireless Distribution System) is the implementation of wireless backhaul between Aps but however at the end, it needs wired backhaul. Disadvantage in this approach is the reduction of overall throughput due to half duplex nature of medium and become even worse in case single radio AP since it cannot simultaneously communicate with client stations and other APs in distribution system.
4. Improvement can be made using Dual Radio APs (two different frequencies – one for STAs and other for WDS communication to avoid co channel interference )

EXTENDED SERVICE SET

1. An Extended Service Set (ESS) is a collection of multiple BSSs that work together to provide a larger wireless network.
2. Each BSS has its own AP.
3. The APs are connected via a wired network (Distribution System - DS).
4. STAs can roam between APs without losing connectivity.
5. Identified by an SSID (Service Set Identifier), which remains the same across all APs.
6. Covers a larger area than a single BSS.
7. Supports seamless roaming (handover between APs).
8. Found in enterprises, airports, universities, hotels.
9. 802.11k – Helps devices find the best AP quickly.
10. 802.11r (Fast Roaming) – Reduces delay when switching APs.
11. 802.11v – Optimizes AP selection for better performance.
12. Use Case : university WiFi where roaming is prioritized.

MBSS :

1. Mesh Basic Service Set provides wireless distribution of network traffic with set of APs that form mesh distribution.
2. APs in MBSS that directly connect to wired infrastructure is called MPP (Mesh Point Portal)
3. Rest of the APs are called as MP (Mesh Points)
4. Use case : Public wifi deployments where APs will be connected to each other in mesh fashion with self healing and with roaming optimization.

QBSS:

1. It stands for Quality of Service Basic Service Set.
2. It primarily uses 802.11e WMM for traffic prioritization.
3. It enhances the quality of service that is guaranteed by conventional BSS if and only if STAs and APs are supporting QoS enhancements.
4. Use case : Hospital network where VoIP should be given more priority than conventional web traffic.