Q1. What are the different modes of access point operation?

Ans - Access points (APs) are networking devices that enable wireless devices to connect to a wired network using Wi-Fi technology. Access points can operate in different modes to meet different networking requirements. Some of the common modes of access point operation are:

Standalone mode: In this mode, an access point functions as a standalone device and manages its own configuration and security settings. This mode is suitable for small networks with only a few access points.

Mesh mode: In mesh mode, access points form a mesh network where each access point communicates with other access points to create a wireless network. This mode is useful in areas where running Ethernet cables to connect access points is difficult or impossible.

Controller-based mode: In this mode, access points are managed by a centralized controller that coordinates their operations, configurations, and security settings. This mode is suitable for large networks with many access points.

Repeater mode: In this mode, an access point receives a wireless signal from another access point and rebroadcasts it to extend the coverage area of the wireless network. This mode is useful in large areas where a single access point cannot provide adequate coverage.

Monitor mode: In this mode, an access point can be configured to operate as a passive listening device to capture network traffic for monitoring and analysis purposes. This mode is useful for troubleshooting network issues and optimizing network performance.

Q2. What are the different types of wireless network? Explain them briefly with example.

Ans - Wireless networks are computer networks that use wireless data connections to transmit data between devices. There are different types of wireless networks, some of the common ones are:

WLAN (Wireless Local Area Network): This type of wireless network is commonly used in homes, offices, and public places such as airports and coffee shops. WLANs use Wi-Fi technology to connect devices within a limited area such as a building, floor, or room. For

example, a Wi-Fi router in a home is used to connect laptops, smartphones, and other wireless devices to the internet.

WWAN (Wireless Wide Area Network): WWAN is a type of wireless network that covers a larger area such as a city, country, or even a continent. Mobile networks such as 3G, 4G, and 5G are examples of WWAN. These networks are used to provide internet access to mobile devices such as smartphones and tablets.

WPAN (Wireless Personal Area Network): WPAN is a type of wireless network that connects devices within a personal space such as a room or a person's body. Bluetooth is an example of WPAN technology. Bluetooth is used to connect wireless headphones, speakers, and other devices to smartphones, laptops, and other devices.

WMAN (Wireless Metropolitan Area Network): WMAN is a type of wireless network that covers a larger area than a WLAN but smaller than a WWAN. A typical example of WMAN is WiMAX (Worldwide Interoperability for Microwave Access). WiMAX is used to provide wireless broadband internet access to a large area such as a city or a rural area.

Q3. Briefly explain different modes of wireless bridges.

Ans - A wireless bridge is a networking device that connects two or more networks together using wireless technology. There are different modes of wireless bridges that are commonly used, including:

Point-to-Point Bridge: This mode of wireless bridge connects two separate networks in different locations to create a single network. Point-to-Point bridges are commonly used to connect two buildings or two campuses that are located within a few miles of each other.

Point-to-Multipoint Bridge: In this mode of wireless bridge, a single bridge connects multiple networks together. This type of bridge is commonly used to connect multiple buildings or remote locations to a single central network.

Wireless Mesh Bridge: A wireless mesh bridge is a type of bridge that connects multiple networks together to create a large network. Mesh bridges use multiple access points that are interconnected wirelessly to provide coverage over a wide area. This type of bridge is useful in areas where running cables is difficult or impossible.

WDS Bridge: WDS (Wireless Distribution System) bridge is a type of bridge that connects multiple access points wirelessly. WDS bridges are commonly used to extend the coverage area of an existing wireless network.

Repeater Bridge: In this mode of wireless bridge, a bridge acts as a wireless repeater to extend the range of an existing wireless network. Repeater bridges are commonly used to extend the coverage area of a wireless network.

Q4. What is modulation? What are the modulation schemes of spared spectrum system?

Ans - Modulation is the process of modifying a signal to transmit information. It involves adding information to an electromagnetic wave, which can then be transmitted wirelessly through the air or other media. Modulation is used in various communication systems to improve the transmission and reception of information.

In a spread spectrum system, the information signal is spread over a wide frequency band, making the signal resistant to interference and difficult to detect by unauthorized receivers. There are various modulation schemes that can be used in a spread spectrum system, including:

Direct Sequence Spread Spectrum (DSSS): In DSSS, a high-speed bit stream is used to modulate a higher-frequency carrier signal. The modulated signal is then spread over a wide frequency band using a spreading code. DSSS is used in wireless LANs, Bluetooth, and GPS systems.

Frequency Hopping Spread Spectrum (FHSS): In FHSS, the carrier signal frequency is changed rapidly and randomly over a wide frequency band. The data signal is transmitted over the carrier signal using a hopping pattern. FHSS is used in wireless LANs, Bluetooth, and military communications.

Orthogonal Frequency Division Multiplexing (OFDM): In OFDM, the data signal is divided into multiple sub-carriers that are transmitted simultaneously over different frequencies. OFDM is used in digital television, digital audio broadcasting, and Wi-Fi.

Chirp Spread Spectrum (CSS): In CSS, a chirp signal is used to spread the information signal over a wide frequency band. The frequency of the chirp signal changes linearly over time. CSS is used in radar systems and wireless LANs.

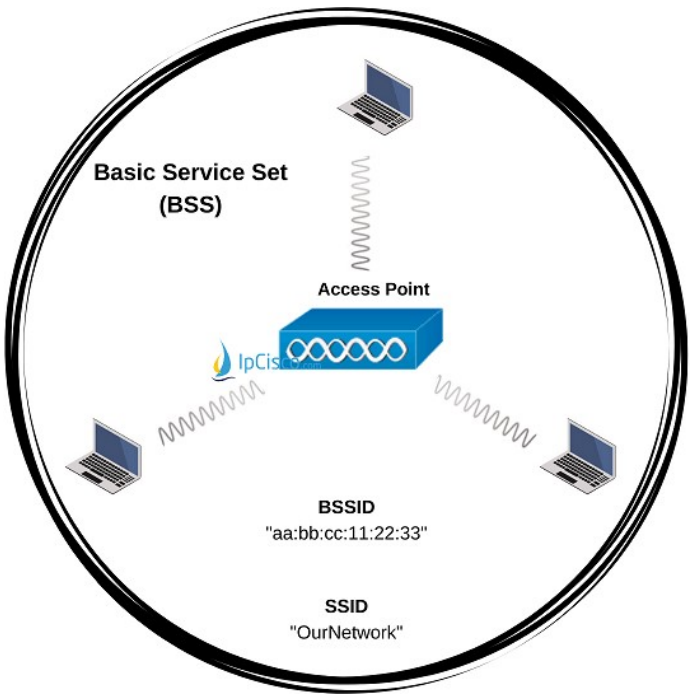
Q5. Briefly explain about service sets in 802.11 architecture.

Ans - In the 802.11 wireless network architecture, service sets are used to define different types of wireless network deployments. A service set refers to a group of wireless devices that communicate with each other over the same wireless network infrastructure.

There are two types of service sets in the 802.11 architecture:

Basic Service Set (BSS):

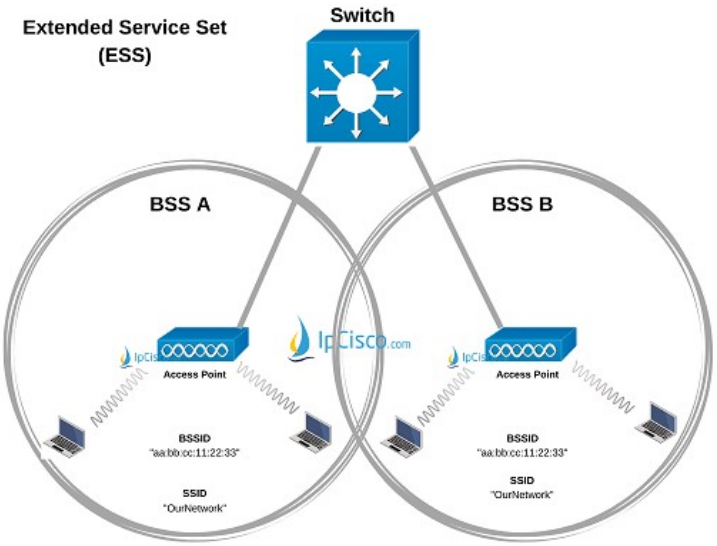
A Basic Service Set (BSS) consists of a single access point (AP) and one or more wireless devices, such as laptops or smartphones, that connect to the access point. The access point is responsible for managing the wireless network, and the devices communicate with the access point to access the network resources.



Extended Service Set (ESS):

An Extended Service Set (ESS) is a group of two or more Basic Service Sets that are connected together to form a larger network. ESS is typically used in larger deployments, such as in an office building or a campus, where multiple access points are used to provide wireless

coverage in a larger area. In an ESS, wireless devices can move between BSSs and still maintain connectivity to the network.



Q6. What is all the authentication mechanism currently supported by access point. Which one is better and why?

Ans - There are several authentication mechanisms that are currently supported by access points in wireless networks. Here are some of the most common authentication mechanisms:

Open System Authentication:

This is the default authentication mechanism in which the access point does not authenticate the wireless client. As a result, any wireless client can connect to the access point without providing any credentials. This is considered the least secure authentication method.

Wired Equivalent Privacy (WEP):

WEP is an older security protocol that uses a shared key authentication mechanism to encrypt wireless traffic. However, it is vulnerable to security attacks and is no longer recommended as a secure authentication mechanism.

Wi-Fi Protected Access (WPA and WPA2):

WPA and WPA2 are more secure authentication mechanisms that use a combination of pre-shared keys (PSKs) and/or 802.1X authentication to secure wireless traffic. WPA2 is currently the most commonly used authentication mechanism and provides strong security for wireless networks.

Extensible Authentication Protocol (EAP):

EAP is an authentication framework that supports multiple authentication methods, including certificate-based authentication, smart card authentication, and biometric authentication. It is commonly used in enterprise-level wireless networks to provide strong security.

Out of these options, WPA2 with 802.1X authentication is considered the most secure, as it uses strong encryption protocols and mutual authentication between the access point and the wireless client. However, the best authentication mechanism to use will depend on the specific security needs of the network.

Q7. Explain shared key authentication?

Ans - Shared Key Authentication is a wireless security protocol where the access point and the wireless client share a secret key, or passphrase. When the client tries to connect to the wireless network, the access point sends a message to the client, and the client encrypts this message using the shared secret key and sends it back to the access point. If the access point can successfully decrypt the message using the shared key, the client is considered authenticated and is granted access to the network.

However, Shared Key Authentication is no longer considered secure as the shared key can be easily intercepted and compromised by attackers, which can lead to unauthorized access to the wireless network. Therefore, more secure authentication mechanisms, such as WPA2 with 802.1X authentication, are now recommended for wireless network security.

Q8. Explain wireless LAN or WLAN. What is difference between adhoc and infrastructure mode in IEEE 802.11?

Ans -A Wireless Local Area Network (WLAN) is a type of computer network that uses wireless communication technology to connect devices within a limited area. WLANs are based on the IEEE 802.11 standard, also known as Wi-Fi.

Ad-hoc mode and Infrastructure mode are two modes of operation for WLANs.

In Ad-hoc mode, wireless devices communicate directly with each other without the need for an access point. This mode is typically used for temporary wireless connections, such as between two laptops in a meeting or in a coffee shop.

In Infrastructure mode, wireless devices communicate with each other through an access point. The access point acts as a central hub for the wireless network, managing the wireless traffic and providing connectivity to the wired network infrastructure. Infrastructure mode is commonly used in permanent wireless network deployments, such as in offices, schools, and public spaces.

The main difference between Ad-hoc mode and Infrastructure mode is that Ad-hoc mode does not require an access point, while Infrastructure mode does. Infrastructure mode provides more reliable and secure wireless connectivity, as it allows for centralized management of the wireless network, while Ad-hoc mode is more suited for temporary, peer-to-peer wireless connections.

Q9. Differentiate Bluetooth and Infrared transmission.

Ans - Bluetooth and Infrared (IR) are two different wireless communication technologies that can be used to transmit data between devices. Here are the main differences between them:

Range: Bluetooth has a much longer range than Infrared. Bluetooth can typically transmit data over a range of up to 10 meters, while Infrared can only transmit data over short distances of up to 1 meter.

Line of sight: Infrared requires a direct line of sight between the transmitter and the receiver, whereas Bluetooth does not. Infrared signals can be blocked by physical obstacles, while Bluetooth signals can penetrate walls and other obstacles.

Data rate: Bluetooth can transmit data at a much higher rate than Infrared. Bluetooth 5.0 can transfer data at up to 2 Mbps, while Infrared typically has a maximum data rate of around 115 Kbps.

Compatibility: Bluetooth is a widely adopted standard that is supported by a wide range of devices, including smartphones, tablets, laptops, and other consumer electronics. Infrared is less commonly used and is mainly found in remote controls and some older mobile phones.

Security: Bluetooth supports advanced security features, such as pairing and encryption, to protect against unauthorized access and eavesdropping. Infrared does not offer the same level of security and is more vulnerable to interception.

Q10. States the different IEEE standards of wireless LAN.

Ans - The Institute of Electrical and Electronics Engineers (IEEE) has defined several standards for wireless LAN (WLAN) technologies, each with its own unique features and specifications. Here are some of the most common IEEE standards for WLAN:

IEEE 802.11b: This standard, also known as Wi-Fi 1, was the first widely adopted WLAN standard. It operates in the 2.4 GHz frequency band and supports data transfer rates of up to 11 Mbps.

IEEE 802.11a: This standard operates in the 5 GHz frequency band and supports data transfer rates of up to 54 Mbps. It is less widely used than 802.11b/g/n due to its higher cost and shorter range.

IEEE 802.11g: This standard operates in the 2.4 GHz frequency band and supports data transfer rates of up to 54 Mbps. It is backward compatible with 802.11b devices and is still in use in many applications.

IEEE 802.11n: This standard, also known as Wi-Fi 4, operates in both the 2.4 GHz and 5 GHz frequency bands and supports data transfer rates of up to 600 Mbps. It uses multiple antennas to increase range and reduce interference.

IEEE 802.11ac: This standard, also known as Wi-Fi 5, operates in the 5 GHz frequency band and supports data transfer rates of up to 6.9 Gbps. It uses multiple antennas and advanced modulation techniques to achieve higher speeds and improved performance.

IEEE 802.11ax: This standard, also known as Wi-Fi 6, operates in both the 2.4 GHz and 5 GHz frequency bands and supports data transfer rates of up to 9.6 Gbps. It uses advanced modulation and scheduling techniques to improve performance and efficiency.