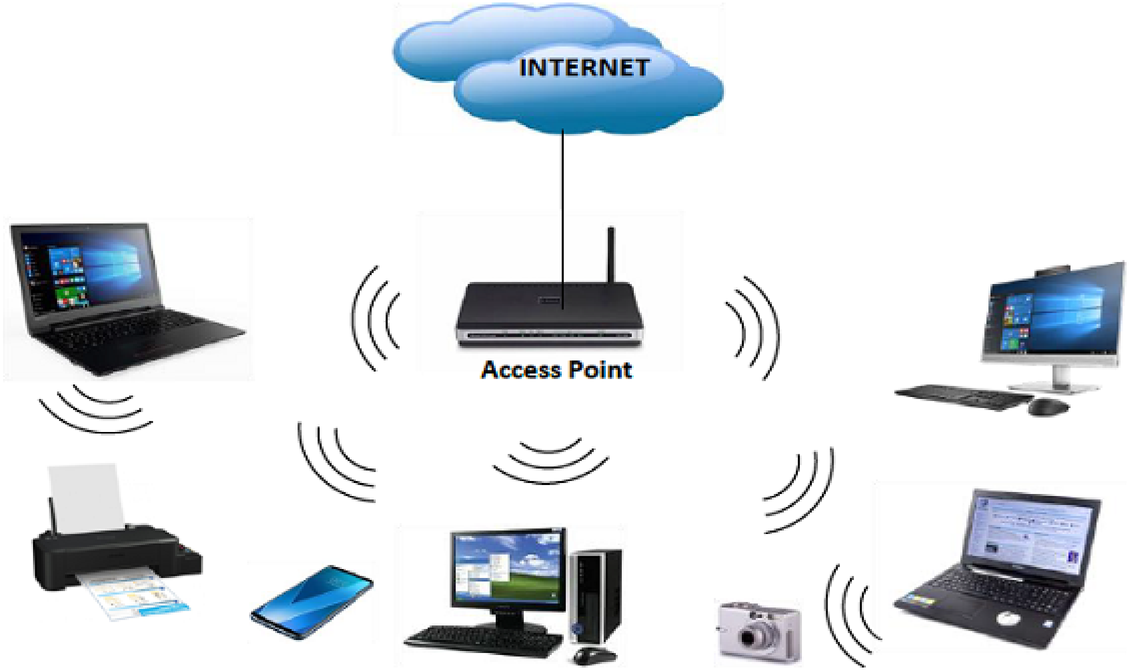
Wireless Networks: Computer networks that are not connected by cables are called wireless networks. They generally use radio waves for communication between the network nodes. They allow devices to be connected to the network while roaming around within the network coverage.



Examples of wireless networks

- Mobile phone networks
- Wireless sensor networks
- Satellite communication networks
- Terrestrial microwave networks

Security issues in wireless networks

Wireless local area networks (WLANs) transmit and receive data using radio waves rather than wires. This lack of a physical barrier makes WLANs vulnerable to unlawful interception, eavesdropping, hacking and a range of other cyber security issues.

Wireless network security issues and threats

The three most common WLAN security threats include:

- **Denial of service attacks** - where the intruder floods the network with messages affecting the availability of the network resources
- **Spoofing and session hijacking** - where the attacker gains access to network data and resources by assuming the identity of a valid user
- **Eavesdropping** - where unauthorised third parties intercept the data being transmitted over the secure network

Wireless LAN Architecture:

Wireless LANs are those Local Area Networks that use high frequency radio waves instead of cables for connecting the devices in LAN. Users connected by WLANs can move around within the area of network coverage. Most WLANs are based upon the standard IEEE 802.11 or WiFi.

IEEE 802.11 Architecture

The components of IEEE 802.11 architecture are as follows

1) Stations (STA) − Stations comprise all devices and equipments that are connected to the wireless LAN. A station can be of two types:

- **Wireless Access Points (WAP)** − WAPs or simply access points (AP) are generally wireless routers that form the base stations or access.
- **Client.** − Clients are workstations, computers, laptops, printers, smartphones, etc.

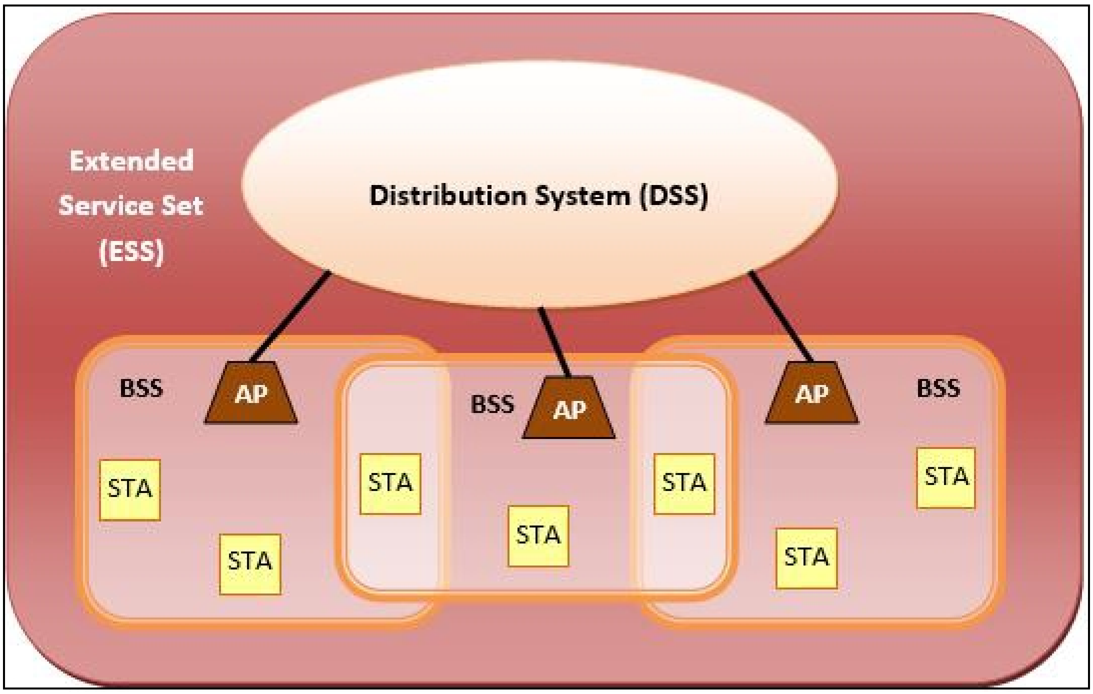
Each station has a wireless network interface controller.

2) Basic Service Set (BSS) −A basic service set is a group of stations communicating at physical layer level. BSS can be of two categories depending upon mode of operation:

- **Infrastructure BSS** − Here, the devices communicate with other devices through access points.
- **Independent BSS** − Here, the devices communicate in peer-to-peer basis in an ad hoc manner.

3) Extended Service Set (ESS) − It is a set of all connected BSS.

4) Distribution System (DS) − It connects access points in ESS.



Advantages of WLANs

- They provide clutter free homes, offices and other networked places.
- The LANs are scalable in nature, i.e. devices may be added or removed from the network at a greater ease than wired LANs.
- The system is portable within the network coverage and access to the network is not bounded by the length of the cables.
- Installation and setup is much easier than wired counterparts.
- The equipment and setup costs are reduced.

Disadvantages of WLANs

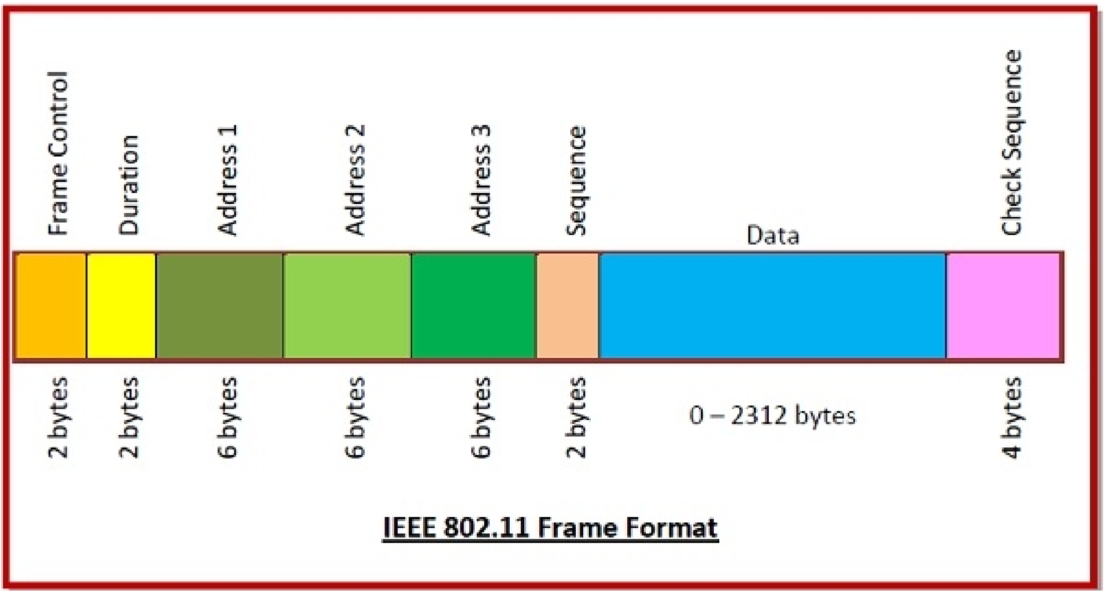
- Since radio waves are used for communications, the signals are noisier with more interference from nearby systems.
- Greater care is needed for encrypting information. Also, they are more prone to errors. So, they require greater bandwidth than the wired LANs.
- WLANs are slower than wired LANs.

Frame Format of IEEE 802.11

The main fields of a frame of wireless LANs as laid down by IEEE 802.11 are −

- **Frame Control** − It is a 2 bytes starting field composed of 11 subfields. It contains control information of the frame.
- **Duration** − It is a 2-byte field that specifies the time period for which the frame and its acknowledgment occupy the channel.

- **Address fields** − There are three 6-byte address fields containing addresses of source, immediate destination, and final endpoint respectively.
- **Sequence** − It a 2 bytes field that stores the frame numbers.
- **Data** − This is a variable-sized field that carries the data from the upper layers. The maximum size of the data field is 2312 bytes.
- **Check Sequence** − It is a 4-byte field containing error detection information.



WLAN security features: Early WLAN hardware used a number of basic security methods, including:

- **Service Set Identifiers (SSIDs)** - these prevent connection to access points unless a device uses a given identifier correctly
- **Media Access Control (MAC)** - this involves using addresses attached to each device to limit connection to access points
- **Wired Equivalent Privacy (WEP)** - WEP uses encryption keys so that only devices with the correct key can communicate with access points

WEP: Introduced in 1997, Wired Equivalent Privacy (WEP) was the first attempt at wireless protection. The aim was to add security to wireless networks by encrypting data. If wireless data were intercepted, it would be unrecognizable to the interceptors since it had been encrypted. However, systems that are authorized on the network would be able to recognize and decrypt the data. This is because devices on the network make use of the same encryption algorithm.

WEP encrypts traffic using a 64- or 128-bit key in hexadecimal. This is a static key, which means all traffic, regardless of device, is encrypted using a single key.

WEP still exists in many devices as users have found compatibility problems when introducing new equipment. However, WEP has been proven ineffective against hackers. You should consider upgrading any devices relying on this technology.

Keys of WEP: WEP aims to protect and keep the integrity of the data. In order to do so, it uses two shared keys:

Unicast session key: Unicast session key is an **encryption key** that is used to protect the unicast traffic between a wireless AP and a wireless client, multicast and/or broadcast traffic between wireless AP and wireless client. It is called unicast to highlight the fact that the data transmission is done between two points in the network: there is a single sender and a single receiver.

Multicast key (also known as the global key): As the name suggests, multicast key aims to protect the broadcast and multicast traffic between a single wireless AP and all of its wireless clients. The term multicast is used to highlight the fact that the data transmission is done between one sender and many receivers or many senders and one receiver.

Several weaknesses have been discovered using WEP encryption that allows an attacker using readily available software to crack the key within minutes. WEP encryption uses a shared key authentication and sends the same key with data packets being transmitted across the wireless network

WPA: Next came WPA, or Wi-Fi Protected Access. Introduced in 2003, this protocol was the Wi-Fi Alliance's replacement for WEP. It shared similarities with WEP but offered improvements in how it handled security keys and the way users are authorized. While WEP provides each authorized system with the same key, WPA uses the temporal key integrity protocol (TKIP), which dynamically changes the key that systems use. This prevents intruders from creating their own encryption key to match the one used by the secure network. The TKIP encryption standard was later superseded by the Advanced Encryption Standard (AES).

In addition, WPA included message integrity checks to determine if an attacker had captured or altered data packets. The keys used by WPA were 256-bit, a significant increase over the 64 bit and 128-bit keys used in the WEP system. However, despite these improvements, elements of WPA came to be exploited – which led to WPA2.

WPA2: WPA2 was introduced in 2004 and was an upgraded version of WPA. WPA2 is based on the robust security network (RSN) mechanism and operates on two modes:

- **Personal mode or Pre-shared Key (WPA2-PSK)** – which relies on a shared passcode for access and is usually used in home environments.
- **Enterprise mode (WPA2-EAP)** – as the name suggests, this is more suited to organizational or business use.

Both modes use the CCMP – which stands for Counter Mode Cipher Block Chaining Message Authentication Code Protocol. The CCMP protocol is based on the Advanced Encryption Standard (AES) algorithm, which provides message authenticity and integrity verification. CCMP is stronger and more reliable than WPA's original Temporal Key Integrity Protocol (TKIP), making it more difficult for attackers to spot patterns.

However, WPA2 still has drawbacks. For example, it is vulnerable to key reinstallation attacks (KRACK). KRACK exploits a weakness in WPA2, which allows attackers to pose as a clone network and force the victim to connect to a malicious network instead. This enables the hacker to decrypt a small piece of data that may be aggregated to crack the encryption key. However, devices can be patched, and WPA2 is still considered more secure than WEP or WPA.

WPA3: WPA3 is the third iteration of the Wi-Fi Protected Access protocol. The Wi-Fi Alliance introduced WPA3 in 2018. WPA3 introduced new features for both personal and enterprise use, including:

- **Individualized data encryption**: When logging on to a public network, WPA3 signs up a new device through a process other than a shared password. WPA3 uses a Wi-Fi Device Provisioning Protocol (DPP) system that allows users to use Near Field Communication (NFC) tags or QR codes to allow devices on the network. In addition, WPA3 security uses GCMP-256 encryption rather than the previously used 128-bit encryption.

- **Simultaneous Authentication of Equals protocol**: This is used to create a secure handshake, where a network device will connect to a wireless access point, and both devices communicate to verify authentication and connection. Even if a user’s password is weak, WPA3 provides a more secure handshake using Wi-Fi DPP.

- **Stronger brute force attack protection**: WPA3 protects against offline password guesses by allowing a user only one guess, forcing the user to interact with the Wi-Fi device directly, meaning they would have to be physically present every time they want to guess the password. WPA2 lacks built-in encryption and privacy in public open networks, making brute force attacks a significant threat.

WPA3 devices became widely available in 2019 and are backwards compatible with devices that use the WPA2 protocol.