# UNIT 5

***1.Explain about the following wireless terminology:***

a) **Access Point**
b) **Hotspot**
c) **GSM**
d) **SSID**

**Access point (AP) or Wireless Access Point (WAP):**An AP is used to connect wireless devices to connect to a wireless/wired network. It is a hardware device that allows wireless connectivity to the end devices. The access point can either be integrated with a router or a separate device connected to the router.

**Hotspot:**These are places where wireless networks are available for public use. Hotspots refer to ares with Wi-Fi availability, where users can enable Wi-Fi on their devices and connect to the internet

**Global System for Mobile Communication (GSM):**It is a standard by European Telecommunication Standards Institute. It is a second generation (2G) protocol for digital cellular networks. 2G was developed to replace 1G (analog) technology. This technology has been replaced by 3G UMTS standard, followed by 4G LTE standard. Mostly GSM networks operate in 900MHz or 1800MHz frequency bands.

**Service Set Identifier (SSID):**It is a unique identifier od a WLAN that is 32 alphanumeric characters in length. SSID is a token used to identify and locate 802.11(Wi-Fi) networks.

***2.Explain the different types of wireless network.***

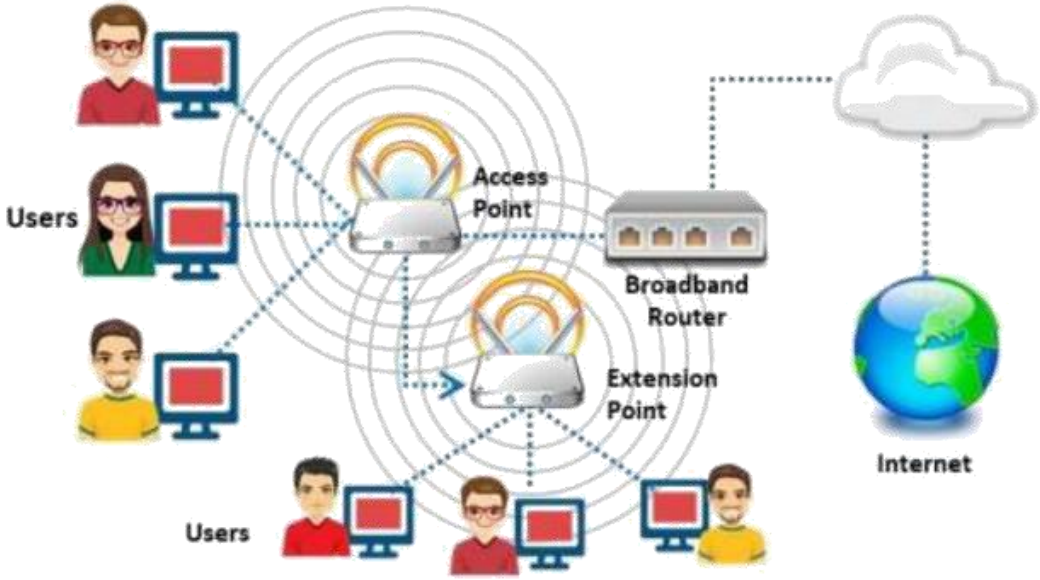
There are different types of wireless networks:

**a) Extension to a Wired Network:**

A user can extend a wired network by placing Aps between a wired network and wireless devices. A wireless network can also be created using AP. In this type of network, the AP acts as a switch, providing connectivity for computers that use a wireless NIC. The AP can connect wireless clients to a wired LAN, which allows wireless access to LAN resources such as file servers and internet connections.

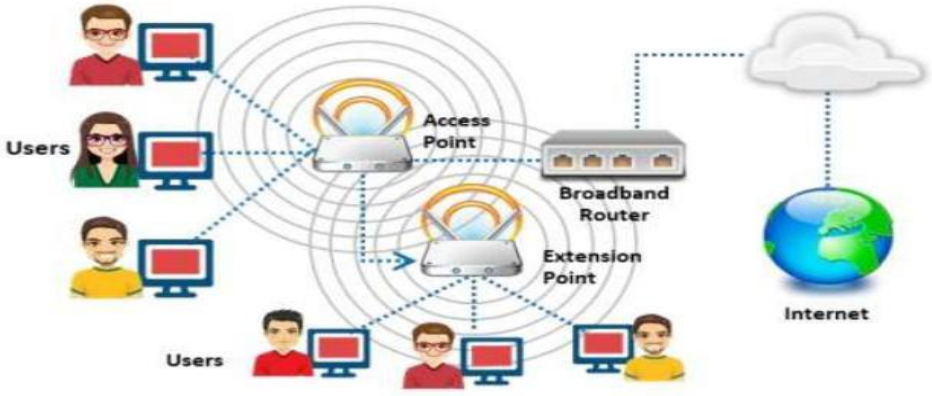
The types of APs Include:

**(1) <u>Software APs (SAPs):</u>**SAPs can be connected to a wired network, and they run on a computer equipped with a wireless network interface card (NIC).




**(2) <u>Hardware APs (HAPs):</u>** HAPs supports most wireless features

In this type of network, the AP acts as a switch, providing connectivity for computers that use a wireless NIC. The AP can connect wireless clients to a wired LAN, which allows wireless access to LAN resources such as file servers and internet connections.




**b)<u>Multiple Access Point:</u>**

This type of network connects computers wirelessly using multiple APs. If a single AP cannot cover an area, multiple APs or extension points can be established.

The wireless area of each AP must overlap its neighbour's area. This provides users the ability to move around seamlessly using a feature called roaming. Some

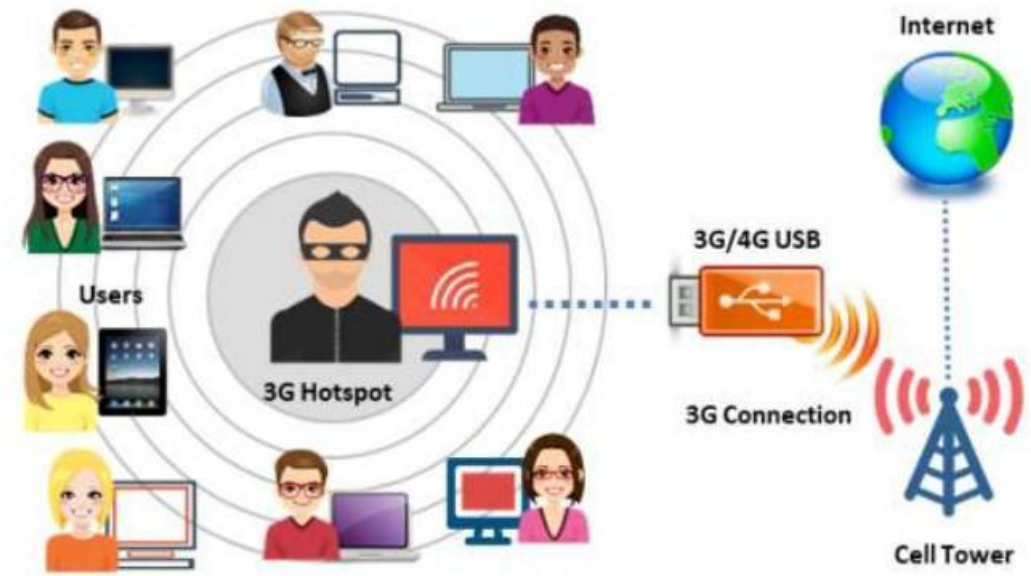
manufactures develop extensionpoints that act as wireless relays, extending the range of a single AP. Multiple extension.

**c)LAN-to-LAN Wireless Network:**

Aps provide wireless connectivity to local computers, and local computers on different networks can be interconnected. All hardware Aps have the capability to interconnect with other hardware Aps.
However, interconnecting LANs over wireless connections is a complex task


**d) 3G/4G Hotspot:**

A 3G/4G hotspot is type of wireless network that provides Wi-Fi access to Wi-fi enabled devices, including MP3 players, notebooks, tablets, cameras, PDAs, netbooks, and more

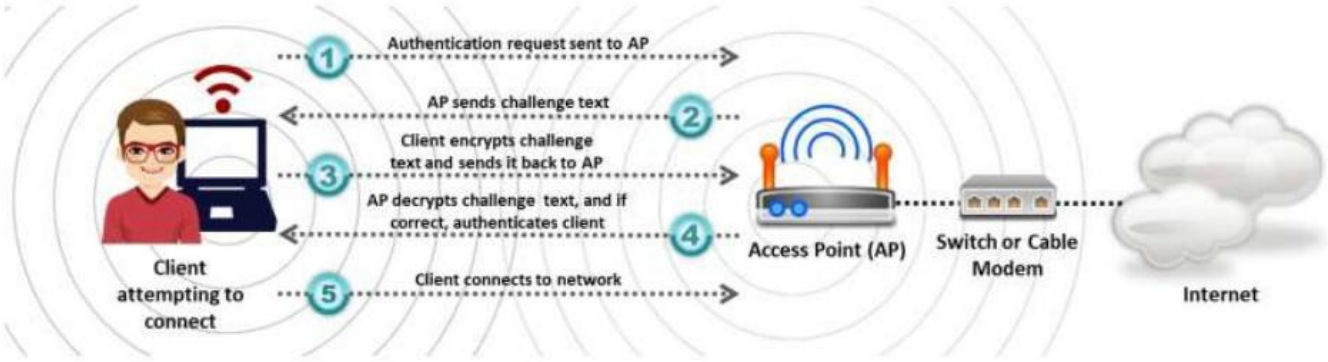


***3.Explain the concept of Shared Key authentication process.***

**Shared Key authentication Process:**

Shared Key authentication mode requires four frames to complete the process of authentication.

- The first frame is the initial authentication request frame that sent by the client to the responder or access point.
- Access point responds the authentication request frame with the authentication response frame with the challenge text.
- The client will encrypt the challenge with the shared secret key and send it back to the responder.
- Responder decrypts the challenge with the shared secret key. If the decrypted challenge matches with the challenge text, successful authentication response frame is sent to the client.




***4.What is War driving?***

War driving comes from an old term called war dialling, where people would dial random phone numbers in search of modems. War driving is basically people driving around looking for vulnerable APs to attack. People will even use drones to try and hack APs on higher floors of a building. A company that owns multiple floors around ten stories up might assume nobody is even in range to hack their wireless, but there is no end to the creativity of hackers!

***5. Explain bluejacking attack?***

**Bluejacking**is the use of Bluetooth to send messages to users without the recipient's consent, similar to email spamming. Prior to any Bluetooth communication, the device initiating the connection must provide a name that is displayed on the recipient's screen. As this name is user-defined, it can be set to be an annoying message or advertisement. Strictly speaking, Bluejacking does not cause any damage to the receiving device. However, it may be irritating and disruptive to the victims.

**Bluejacking attack**the attacker can sniff, jam, and take control of the data transmission between BLE devices by performing an MITM attack. Following a successful attempt, the attacker can also bypass security mechanisms and listen to the information being shared. To implement this attack, the attacker must use affordable firmware-embedded equipment and minor software coding.

***6. Explain about WEP Encryption and steps to break WEP Encryption.***

**WEP Encryption:**

Wired Equivalent Privacy (WEP) is an oldest and weakestencryption protocol. It was developed to ensure the security of wireless protocols however it is highly vulnerable. It uses 24-bit initialization vector (IV) to create a stream cipher RC4 with Cyclic Redundant Check (CRC) to ensure confidentiality and integrity. Standard 64-bit WEP uses the 40-bit key, 128- bit WEP uses 104-bit key and 256-bit WEP uses a 232-bit key. Authentications used with WEP are Open System authentication and Shared Key authentication.

**Working of WEP Encryption:**

Initialization Vector (IV) and Key together is called WEP Seed. This WEP Seed is used to from RC4 Key. RC4 generates a pseudorandom stream of bits. This pseudorandom stream is XORed with the Plain text to encrypt the data. CRC-32 Checksum is used to calculate the Integrity Check Value (ICV).

**Weak Initialization Vector (IV) :**

The one of the major issues with WEP is with Initialization Vector (IV) . IV value is too small to protect from reuse and replay. RC4 Algorithm uses IV and Key to create a stream using Key Scheduling algorithm. Weak IV reveal information. Collection of weak IV will be the base key. WEP has no built-in provision to update key.

**Breaking WEP Encryption:**

Breaking WEP encryption can be performed by following the steps mentioned below: -

1. Monitor the Access point channel.
2. Test Injection Capability to the Access point.
3. Use tool for Fake Authentication.
4. Sniff the packets using Wi-Fi Sniffing tools
5. Use Encryption tool to inject Encrypted packets
6. Use the Cracking tool to extract the encryption key from IV.

***7.Discuss some defence against Bluetooth hacking***

**Defence Against Bluetooth Hacking:**

- use non-regular pattern as PINs while pairing a device. Key combinations should not be sequential on the keypad.
- Keep Bluetooth in the non-discoverable (hidden) mode.
- Do not accept any unknown or unexpected request for pairing.
- Regularly check of all devices paired in the past and delete any suspicious paired device.
- Always enable encryption when establishing a Bluetooth connection.
- Set the network range of a Bluetooth-enabled device to the lowest and perform pairing only in a secure area.
- Install antivirus software that supports host-based security software on Bluetooth-enabled devices.

***8.Explain about two different types of Bluetooth modes***

Bluetooth modes:

A user can set Bluetooth in the following modes.

- Discoverable mode
- Limited discoverable mode

- When Bluetooth devices are in the **discoverable mode**, they are visible to other Bluetooth-enabled devices. If a device attempts to connect to another, the

device attempting to establish the connection must search for a device that is in the discoverable mode; otherwise, the device attempting to initiate the connection will not be able to detect the other device. The discoverable mode is necessary only while connecting to a device for the first time. Upon saving the connection, the devices remember each other; therefore, the discoverable mode is not necessary for lateral connection establishment.

- : In the **limited discoverable mode**, the Bluetooth devices are discoverable only for a limited period, for a specific event, or during temporary conditions. However, there is no Host Controller interface (HCI) command to set a device directly in the limited discoverable mode. A user has to do this indirectly When a device is set to the limited discoverable mode, it filters out non-matched IACs and reveals itself only to those that matched.