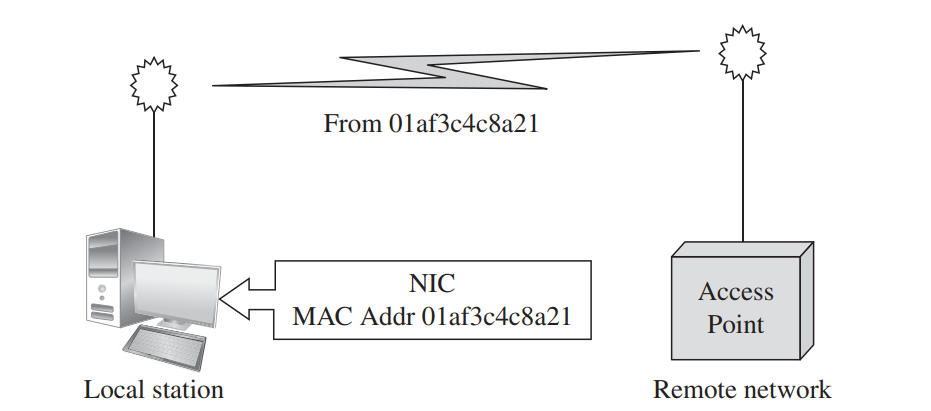
**WIRELESS NETWORK SECURITY**

**WiFi Background**

The wireless traffic occurs in a section of the radio spectrum and thus since most of these frequencies are predefined, the signals become exposed and are available to anyone with an effective antenna within range and therefore measures need to be taken in order to combat these security challenges.

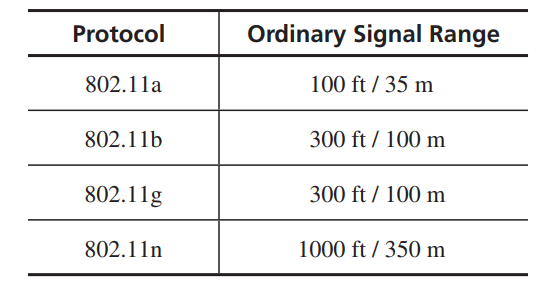
**Wireless Communication**

Wireless communications follow the 802.11 protocols suite. The protocols describe how devices communicate in the 2.4 GHz radio signal band (essentially 2.4 GHz–2.5 GHz) allotted to WiFi.

wireless network consists of an access point or router that receives, forwards and transmits data, and one or more devices, sometimes called stations, such as computers or printers, that communicate with the access point.

**Local Station Communicating with Remote Network**

**WiFi Access Range**

****

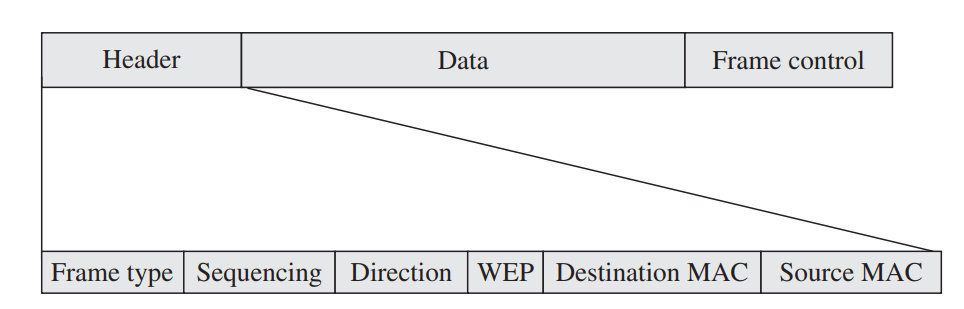
-Most WiFi-enabled computers now communicate on the 802.11n protocol

**WiFi Frames**

-A frame is a wifi data unit, the frame consists of:

1. MAC header
2. Payload
3. FCS (frame check sequence)

-The payload represents the actual data being transmitted and frame check sequence is an integrity check (a cyclic redundancy check).

-The format of a WIFI frame is as shown below:

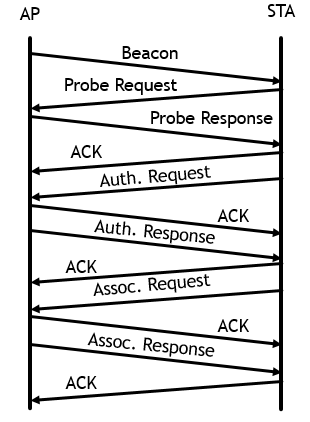
**Management Frames**

-These control the establishment and handling of a series of data flows, and the most important ones include:

* **Beacon:** A beacon signal advertises a network accepting connections.

These signals represent the location of a device or its readiness to perform a task.

* **Authentication:** A NIC requests a connection by sending an authentication frame.
* **Association request and response.**

****

**Association process diagram**

**SSID (Service Set Identifier):** An SSID is a string to identify a wireless access point.

**Vulnerabilities in Wireless Networks**

-The major vulnerabilities include threats to confidentiality, integrity, and availability.

* **Confidentiality:** Since wifi transmissions occur in the open, unintended recipients may be able to get the transmitted data.
* **Integrity:**  integrity violations involve direct, malicious attacks to change the content of a communication.
* **Availability:**  Some of the availability problems in wifi networks can occur when a wireless network device stops working due to various reasons, loss of some but not all access, typically manifested as slow or degraded service and the possibility of rogue network connection.

1. **Unauthorized WiFi Access:**

An unauthorized device can attempt to establish an association with an access point.

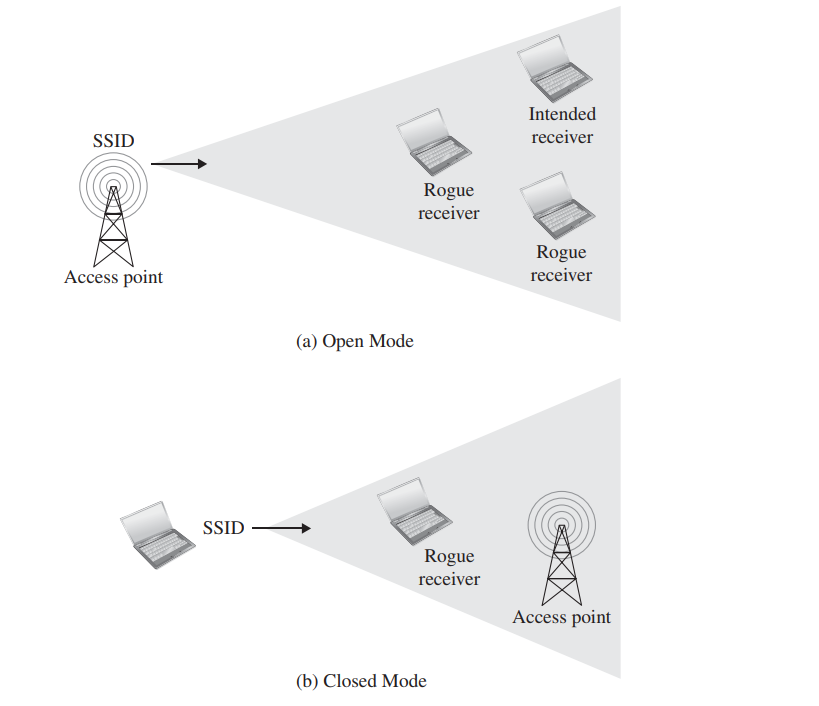
1. **WiFi Protocol Weaknesses:**

Wireless communication is more exposed than wired communication because of the lack of physical protection.

1. **Picking Up the Beacon:**

In open mode an access point continually broadcasts its SSID; in closed mode a client continually broadcasts a request to connect to a given SSID from a given MAC address.

**SSID in All Frames**

****

**Authentication in Wireless Networks**

Access points can manage lists of MAC addresses of devices with which they will accept connections.

**Changeable MAC Addresses**

An operating system can send any address as if it were the MAC address of a NIC. Changing the NIC’s MAC address not only undermines MAC-based authentication on an access point, it can lead to a larger attack called MAC spoofing.

**Stealing the Association**

Even though frames all contain the SSID of the intended recipient access point, nothing prevents any access point from accepting and replying to any frame.

**Preferred Associations**

A user can typically connect to several wifi networks at different times, to simplify connectivity in the future, the wireless interface software builds a list of favourite connection to which it will try to connect automatically.

-Some of those may be public vulnerable wifi networks and thus your device might connect to a vulnerable network unexpectedly and therefore, securing wifi networks becomes a even bigger challenge.

**Failed Countermeasure: WEP (Wired Equivalent Privacy)**

* WEP-was intended as a way for wireless communication to provide privacy equivalent to conventional wire communications.
* WEP uses an encryption key shared between the client and the access point.

**WEP Security Weaknesses**

* Weak Encryption Key
* Static Key
* Weak Encryption Process
* Weak Encryption Algorithm
* Initialization Vector Collisions
* Faulty Integrity Check
* No Authentication

-WEP uses short, infrequently changed encryption keys, it requires no authentication, and its integrity is easily compromised, therefore, WEP security is not acceptable.

**Stronger Protocol Suite: WPA (WiFi Protected Access)**

* The alternative to WEP is **WiFi Protected Access** or **WPA** which was designed in 2003.
* IEEE standard 802.11i is known as WPA2 and is an extension of WPA.

**Strengths of WPA over WEP**

* Non-Static Encryption Key: WPA has a key change approach, called **Temporal Key Integrity Program (TKIP),** by which the encryption key is changed automatically on each packet.
* Authentication: WPA employs the extensible authentication protocol (EAP) by which authentication can be done by password, token, certificate, or other mechanism.
* Strong Encryption
* Integrity Protection
* Session Initiation

In conclusion, WPA fixes many shortcomings of WEP by using stronger encryption; longer, changing keys; and secure integrity checks.

**Attacks on WPA**

-Some attacks against WPA include: Man-in-the-Middle attack, incomplete authentication and exhaustive key search (a cryptography limitation)