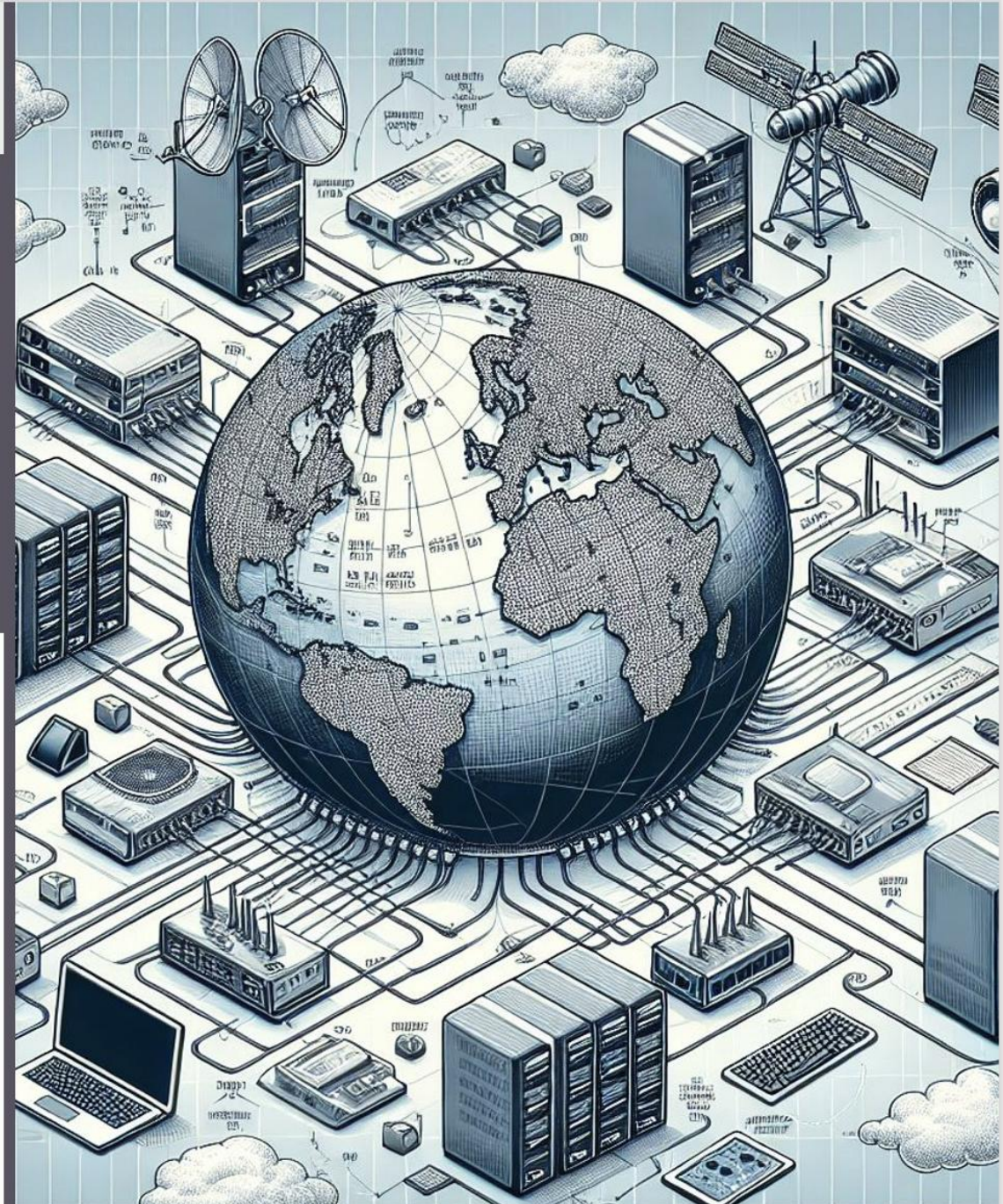


# CS 334/534 NETWORKING

**Dr. Ragib Hasan**

**Lecture 4.3:**  
More on WiFi

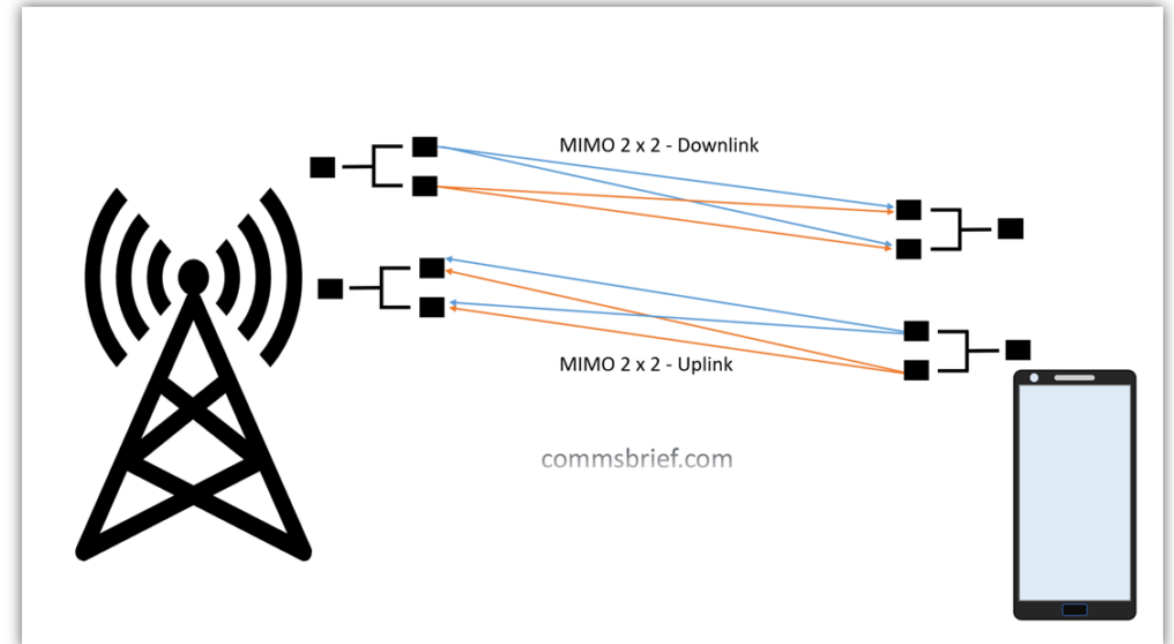


# Lecture goals

- Learn more about WiFi
  - Access Points
  - Wifi Configuration
  - Wifi Security
- 
- Book reference: Chapter 4, section 4.2.3 to 4.2.5.2

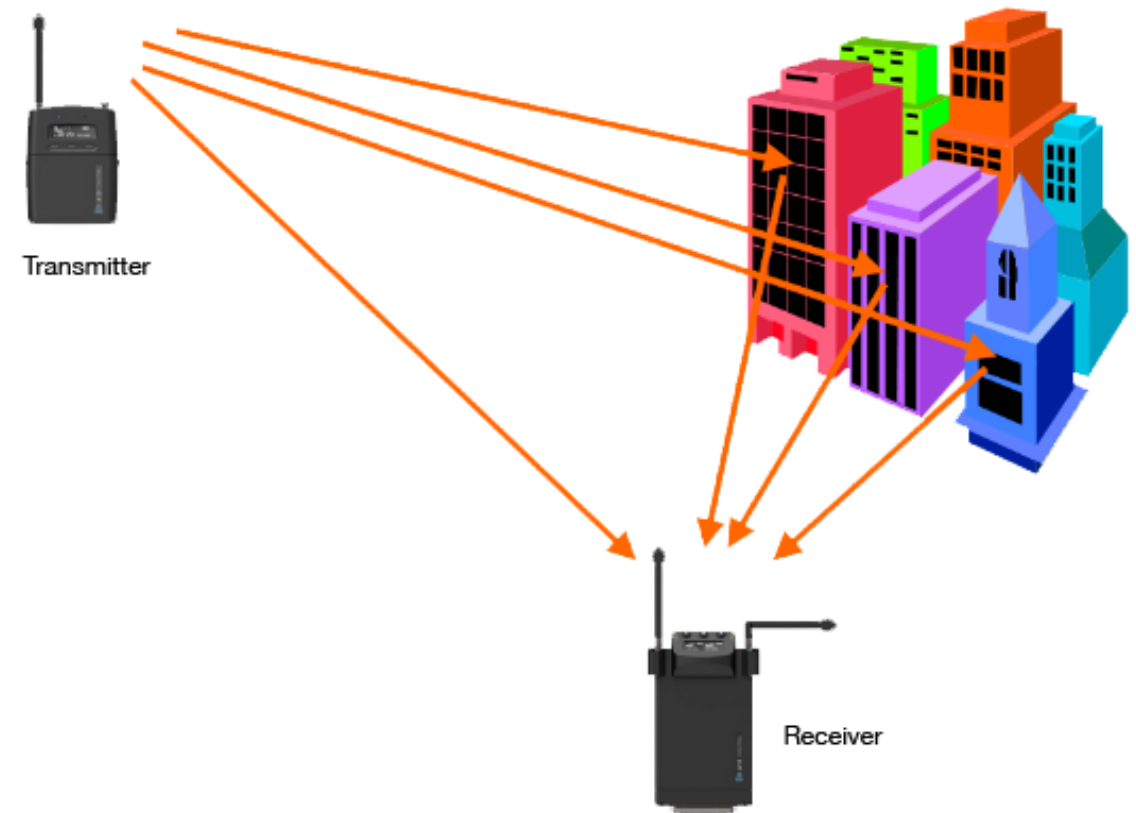
# MIMO (Multiple-Input-Multiple-Output)

- MIMO is a revolutionary antenna technique that **enables multiple simultaneous data streams**.
- Latest innovation to improve Wi-Fi and wireless data rates.
- Both sender and receiver to have multiple antennas (N antennas for N streams)
- All antennas operate on the same frequency but transmit different data streams.



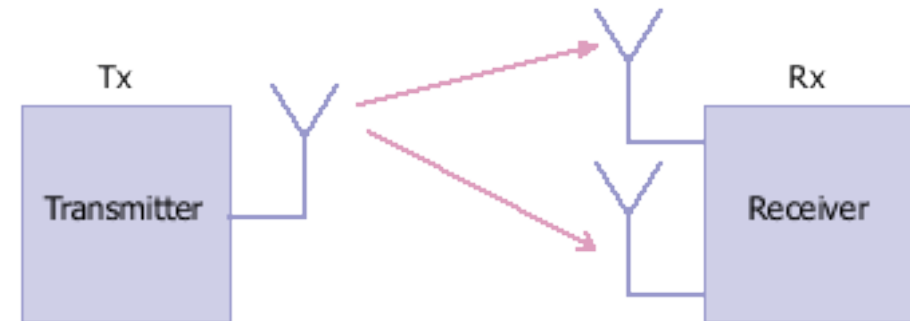
# MIMO (Multiple-Input-Multiple-Output)

- Traditional multipath interference causes **signal variations** (peaks and valleys)
- MIMO **leverages these variations** to improve data rates and reliability.
- **Dead zones (low signal areas)** can disrupt single-antenna reception.
- MIMO is ineffective in clear space but works well in **environments with multipath interference**.



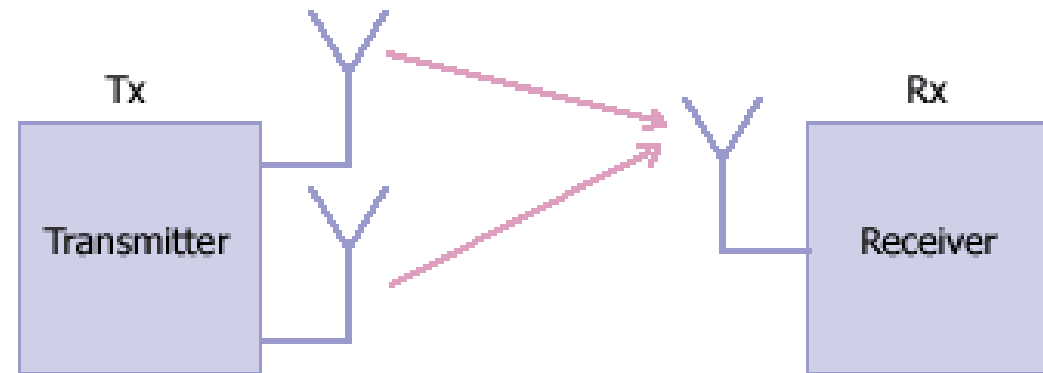
# MIMO Variations

- SIMO (Single-Input-Multiple-Output):
  - Receiver has multiple antennas.
  - Picks the stronger of the two received signals.
  - Ensures reception if at least one antenna is outside a dead zone.



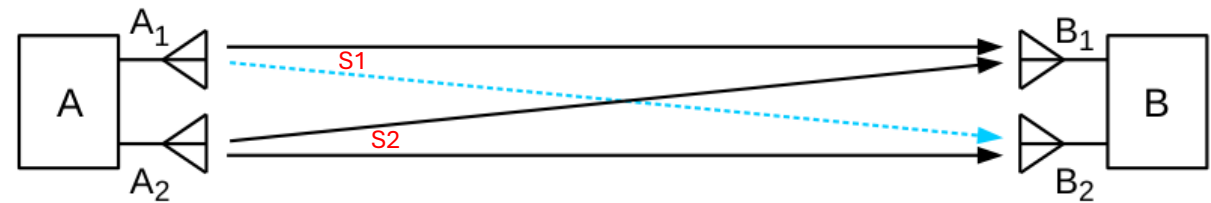
# MIMO Variations

- MISO (Multiple-Input-Single-Output):
  - Transmitter has multiple antennas.
  - Selects the antenna with the stronger signal to the receiver.
  - Requires feedback from the receiver to determine the best antenna.



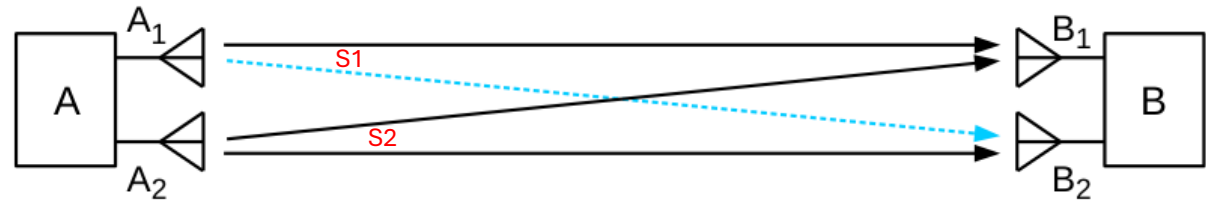
# MIMO Example

- Sending Antennas: A1 and A2
- Receiving Antennas: B1 and B2
- A1 is sending the signal S1
- A2 is sending the signal S2



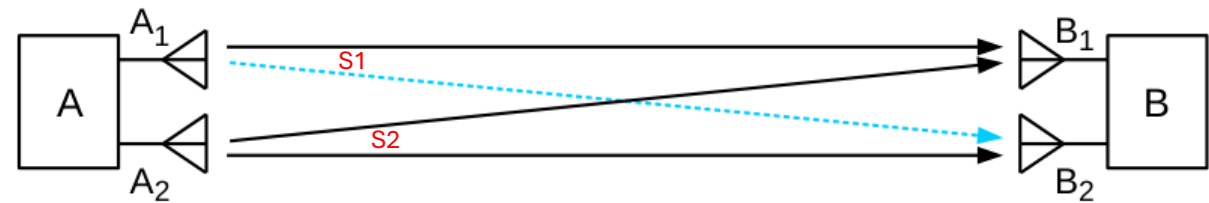
# MIMO Example

- Four physical signal paths:
  - A1-to-B1
  - A1-to-B2
  - A2-to-B1
  - A2-to-B2
- A1-to-B2 signal half the strength of the other three (blue dashed).



# MIMO Example

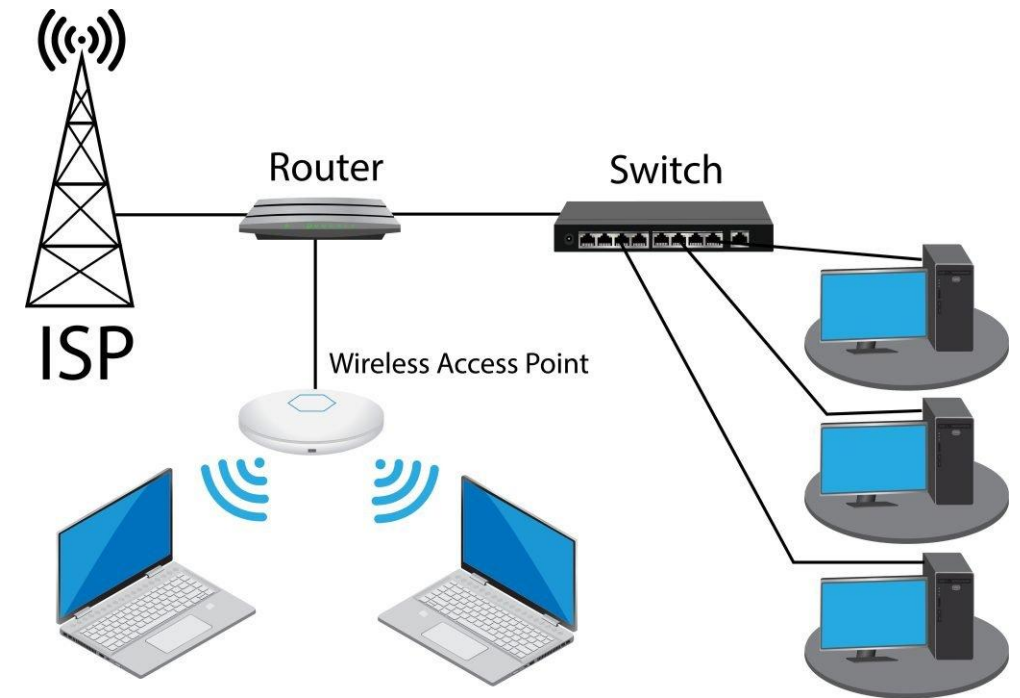
- Signal received by B1:  $S1 + S2$
- Signal received by B2:  $S1/2 + S2$
- From these, B can readily solve for the two independent signals S1 and S2
- The antennas are each more-or-less omnidirectional



# Access Point (AP)

---

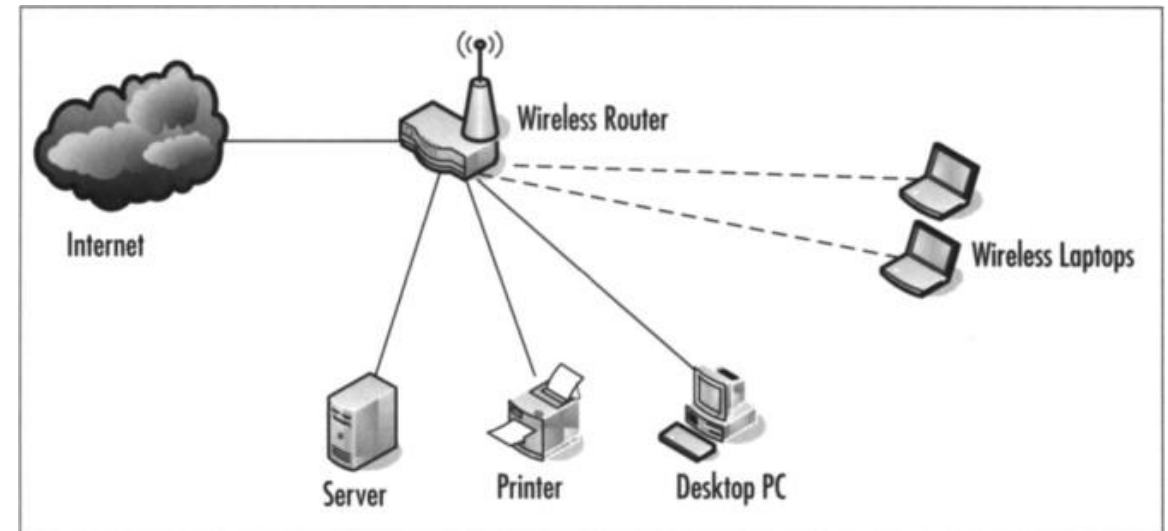
- **Access Point (AP)** is a network device that serves as a central hub for wireless communication in an **infrastructure-mode Wi-Fi network**
- It allows Wi-Fi-enabled devices (stations) to **connect to a wired network**, providing internet access and **enabling communication between devices**.
- The AP manages **data transmission** between connected devices by **receiving, processing, and forwarding packets**, ensuring seamless network operation.



# Wi-Fi Configurations:

## Infrastructure Mode (Most Common):

- Devices communicate **only through the access point**
- AP connects devices to the **outside world** and forms a **true LAN**
- Example: Connecting our phone or laptop to a home Wi-Fi router to access the internet.
- **Drawback:** Slight inefficiency due to two-step forwarding

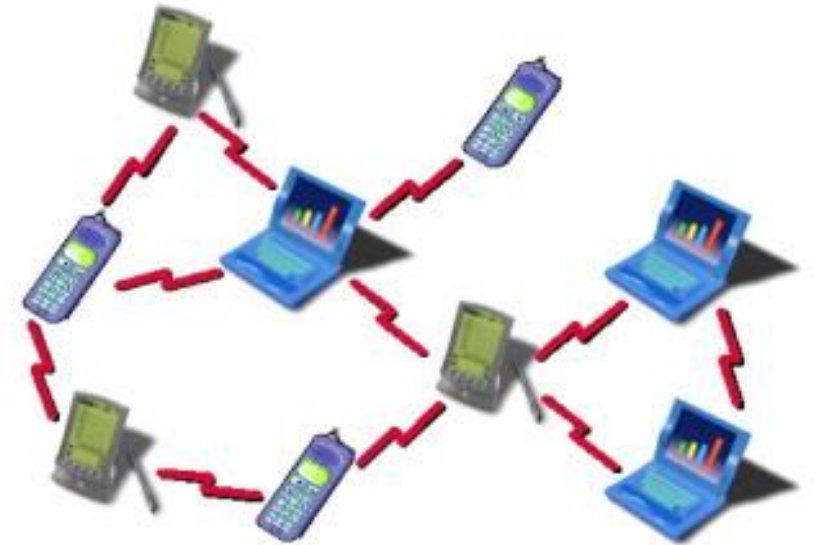


# Wi-Fi Configurations:

---

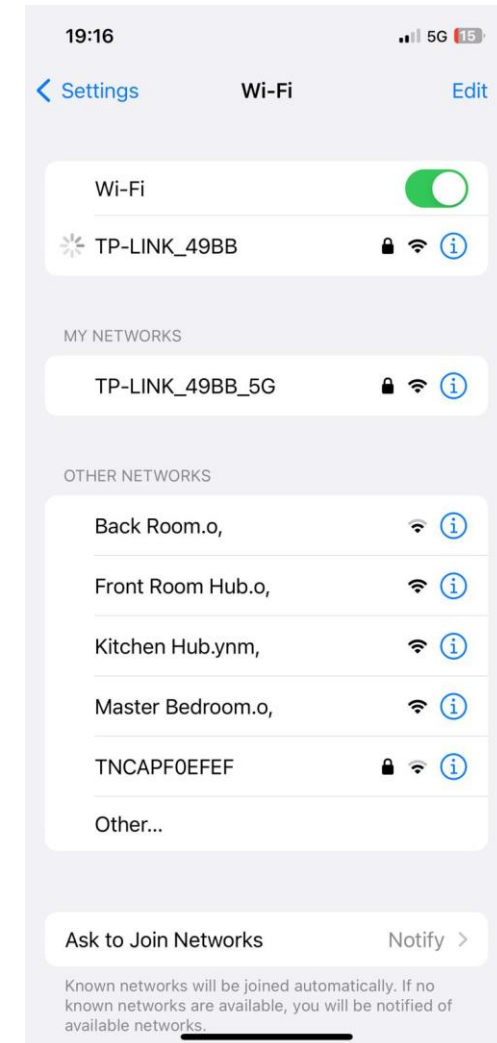
## Ad Hoc Mode (Decentralized):

- Devices communicate **directly** or through intermediate nodes.
- Often used for **simple, temporary networks** without internet.
- **More complex ad hoc networks exist** (e.g., Mobile Ad Hoc Networks – MANETs)
- Can involve **hidden-node issues**, where two nodes can only reach each other via a third node.
- Example: Two laptops connecting directly via Wi-Fi to share files without using a router.



# Service Set Identifiers (SSIDs)

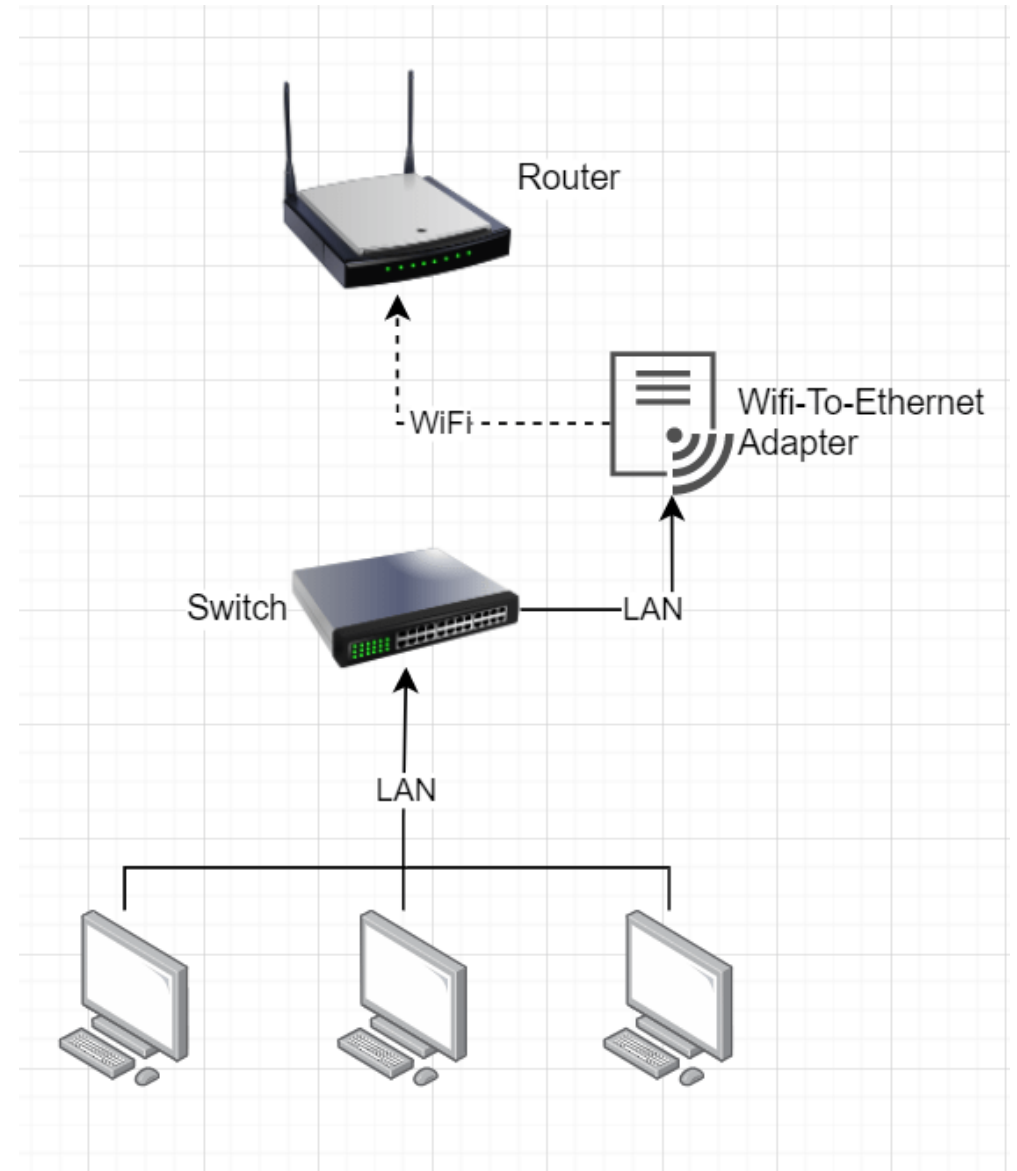
- SSIDs is the **name of a Wi-Fi network** that allows devices to identify and connect to it.
- Infrastructure mode: Uses **human-readable names** (e.g., "HomeWiFi", "CoffeeShop\_FreeWiFi")
- Ad hoc mode: Uses pseudorandom strings resembling **MAC addresses**
- Access points can **support multiple SSIDs** simultaneously
- Different SSIDs can have **different security levels** (e.g., "guest" vs "secure")



# Interoperability with Ethernet

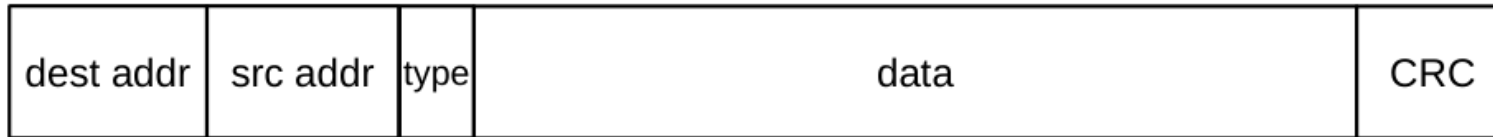
---

- Wi-Fi is designed to be fully compatible with Ethernet.
- If device A is on Wi-Fi and device B is on Ethernet (connected via AP), data is forwarded seamlessly.
- AP acts as an Ethernet switch to transfer data between networks.
- Key Difference: Ethernet and Wi-Fi headers have different formats.

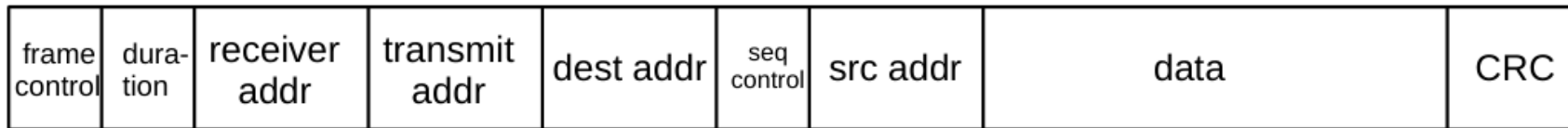


# Interoperability with Ethernet

---



Ethernet



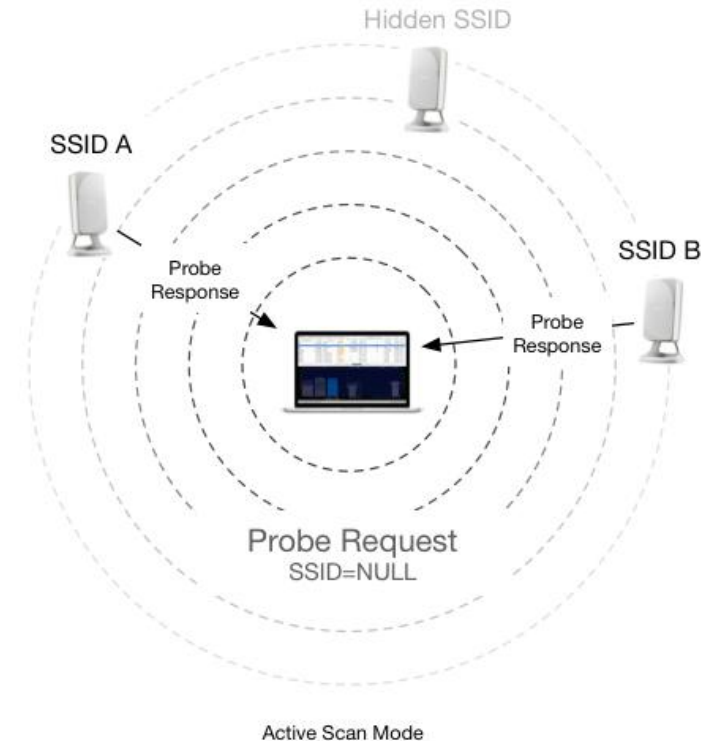
Wi-Fi Data

Fig. 26:: Top: Ethernet packet format; Bottom: Wi-Fi packet format (typical)

# Wi-Fi Probe Request?

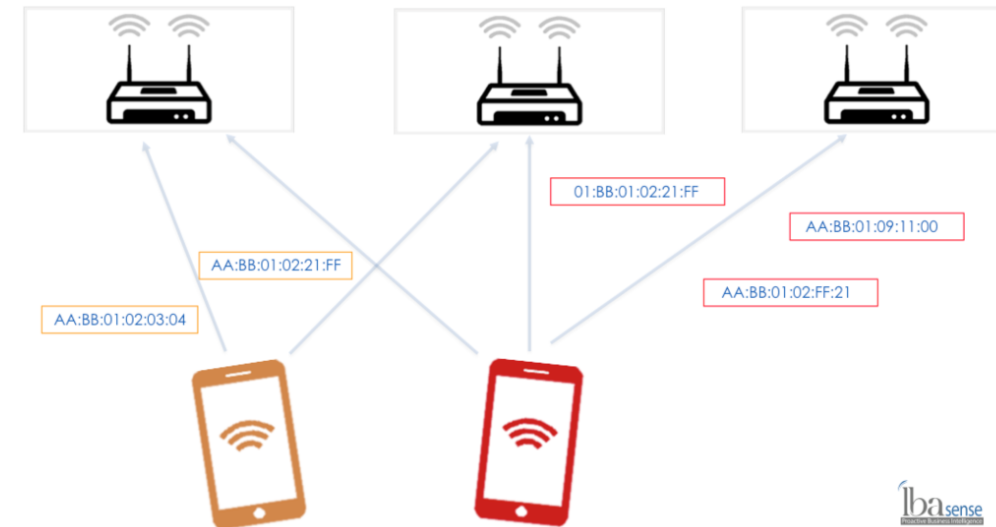
A Wi-Fi probe request is a **type of management frame** sent by a Wi-Fi-enabled device to **discover available Wi-Fi networks**.

- When a device is not connected to a Wi-Fi network, it actively scans by broadcasting probe requests.
- These requests contain the device's MAC address and may also include the names (SSIDs) of previously connected networks (if the device is trying to reconnect).
- Nearby Wi-Fi access points (APs) respond with probe responses, listing available networks.



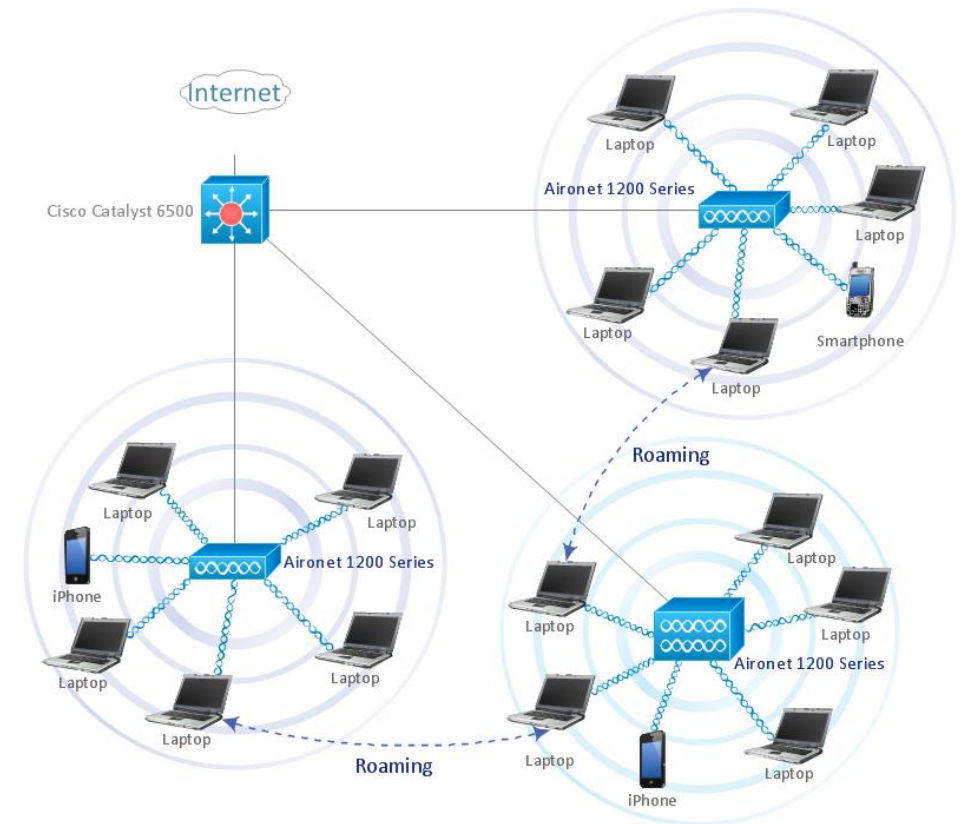
# MAC Address Randomization

- Devices regularly transmit probe requests with MAC address on all channels.
- Traditional fixed MAC addresses enable customer tracking.
- Random MAC addresses enhance privacy protection.
- Challenges and Limitations:
  - Regular MAC changes can break existing connections.
  - Some sites authenticate users via MAC addresses.
  - Network services might require stable MAC addresses.
  - MAC randomization doesn't prevent all tracking methods



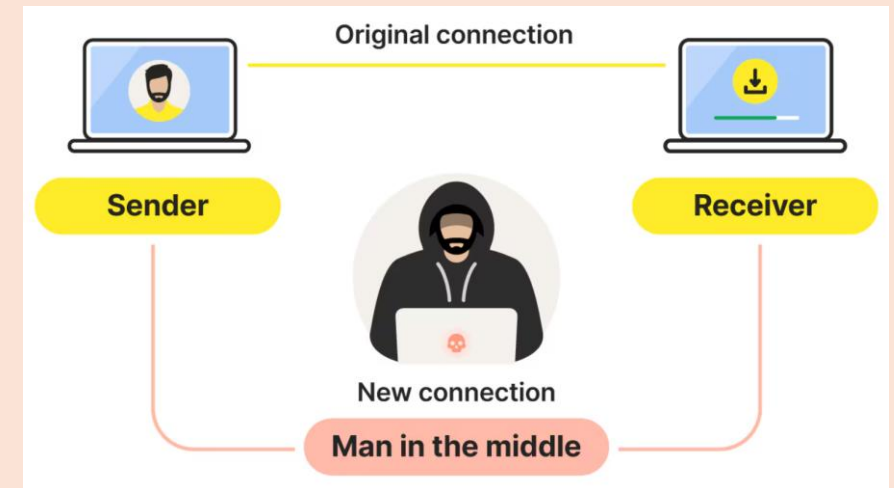
# Wi-Fi Roaming and Extended Service Set (ESS)

- A configuration with multiple access points and a single SSID is called ESS.
- ESS allows large areas to be covered by multiple access points.
- Multiple access points share the same SSID, enabling roaming.
- A station stays connected to its original access point until signal strength drops.
- Once signal strength falls, the station seeks a stronger access point with the same SSID.



# Wi-Fi Security

- Unencrypted Wi-Fi traffic presents **significant security risks**, as anyone within range can **intercept communications** using an appropriate receiver.
- With larger antennas extending this vulnerability zone even further.
- The solution is the application of encryption protocols and authentication mechanisms in the network.



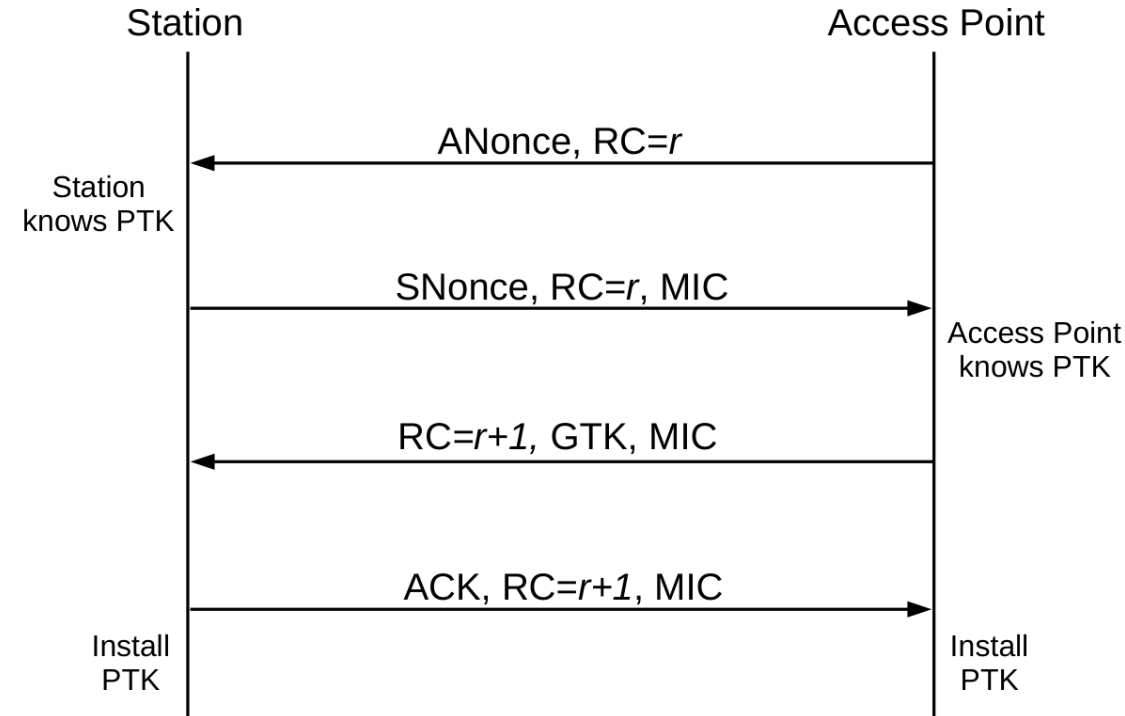
## WPA2 (Wi-Fi Protected Access 2)

- Uses AES encryption with CCMP for stronger security.
- Believed to be secure, but has a vulnerability in the Wi-Fi Protected Setup protocol.
- Uses a pre-shared key (PSK) for smaller personal networks.
- PSK is typically a secure hash of a passphrase.
- Difficult to change the key or revoke access for individual users.



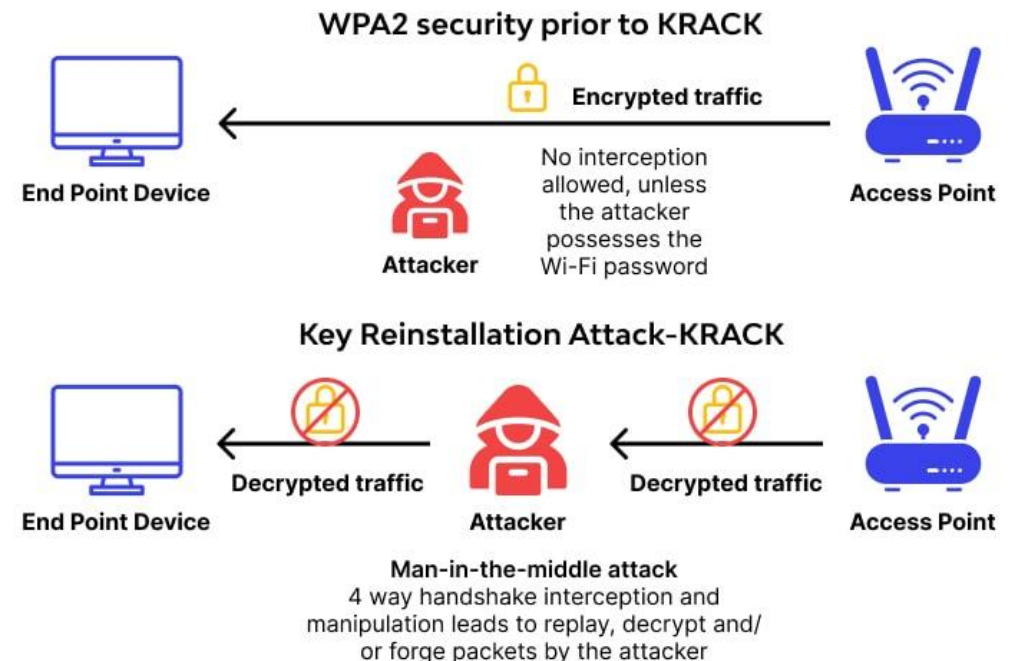
# Four-way WPA2 handshake

- AP sends nonce & replay counter (RC) to station.
- Station sends its nonce and Message Integrity Code (MIC) to prove knowledge of the master key.
- AP computes pairwise transient key (PTK), verifies MIC to authenticate station.
- AP sends signed message to station with optional group temporal key (GTK) which is encrypted with PTK.
- Final acknowledgment from the station.
- The replay counter (RC) prevents an attacker from reusing old handshake packets.



# Key Reinstallation Attack - KRACK

- The attacker stops or delays one of the messages from the station to the access point.
- The access point then retransmits the same message (third handshake packet).
- This causes the encryption to reset and reuse the same keystream (pattern used for encryption), making it easier for the attacker to guess the encryption key.
- This causes the encryption to reset and reuse the same keystream (pattern used for encryption), making it easier for the attacker to guess the encryption key.



# WPA2-Enterprise

- Unlike WPA2-Personal, WPA2-Enterprise assigns a unique key to each device, preventing key reuse across devices.
- The keys are managed by an authentication server (RADIUS), ensuring better control over key management and preventing unauthorized reinstallation of keys.
- Allows immediate revocation of individual user access.

