Wireless Networks

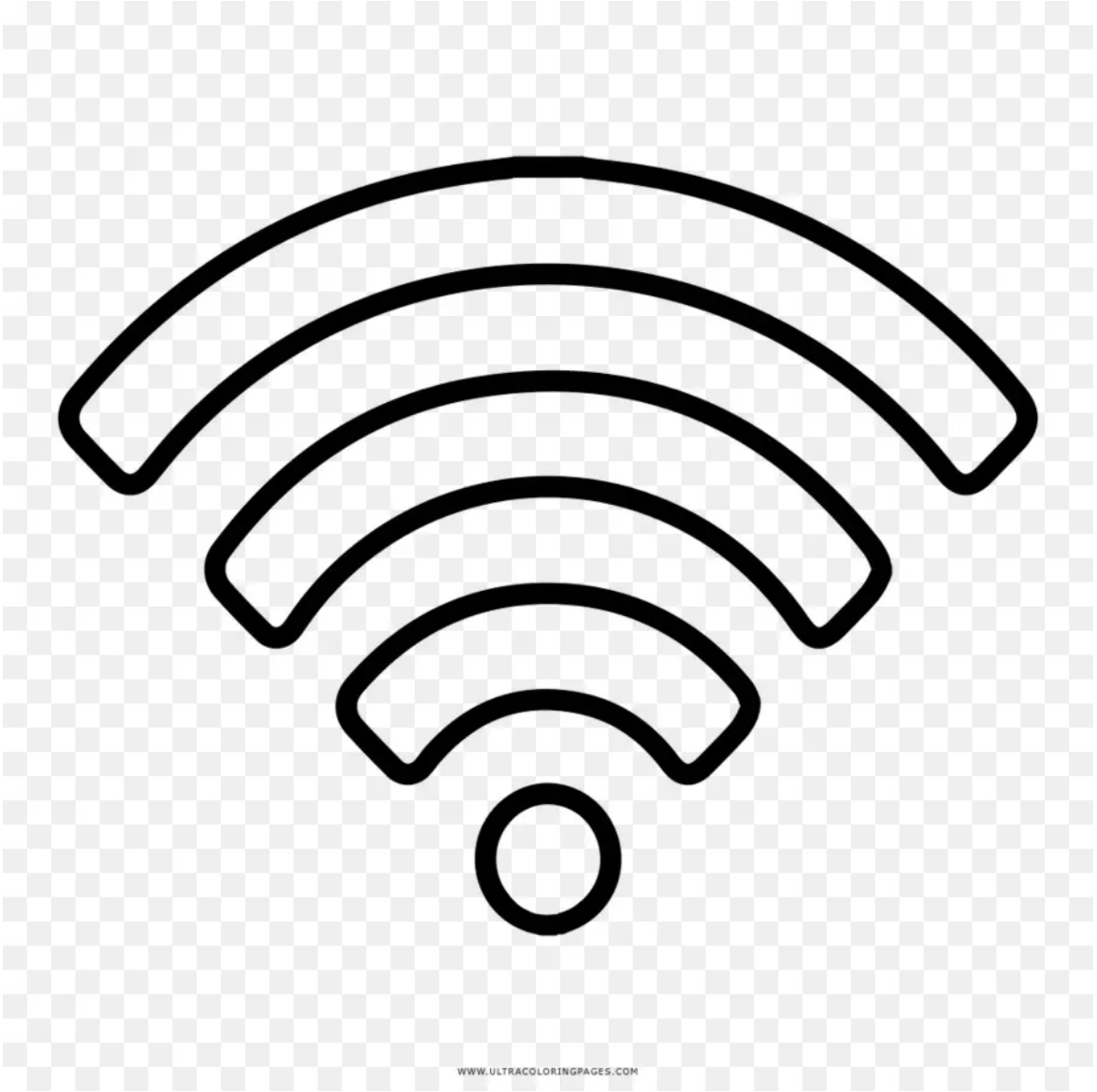
SEMtech!

Student Engagement & Mentoring in Technology

Thomas Holt Russell, M.Ed., D. Hon. (Cybersecurity)

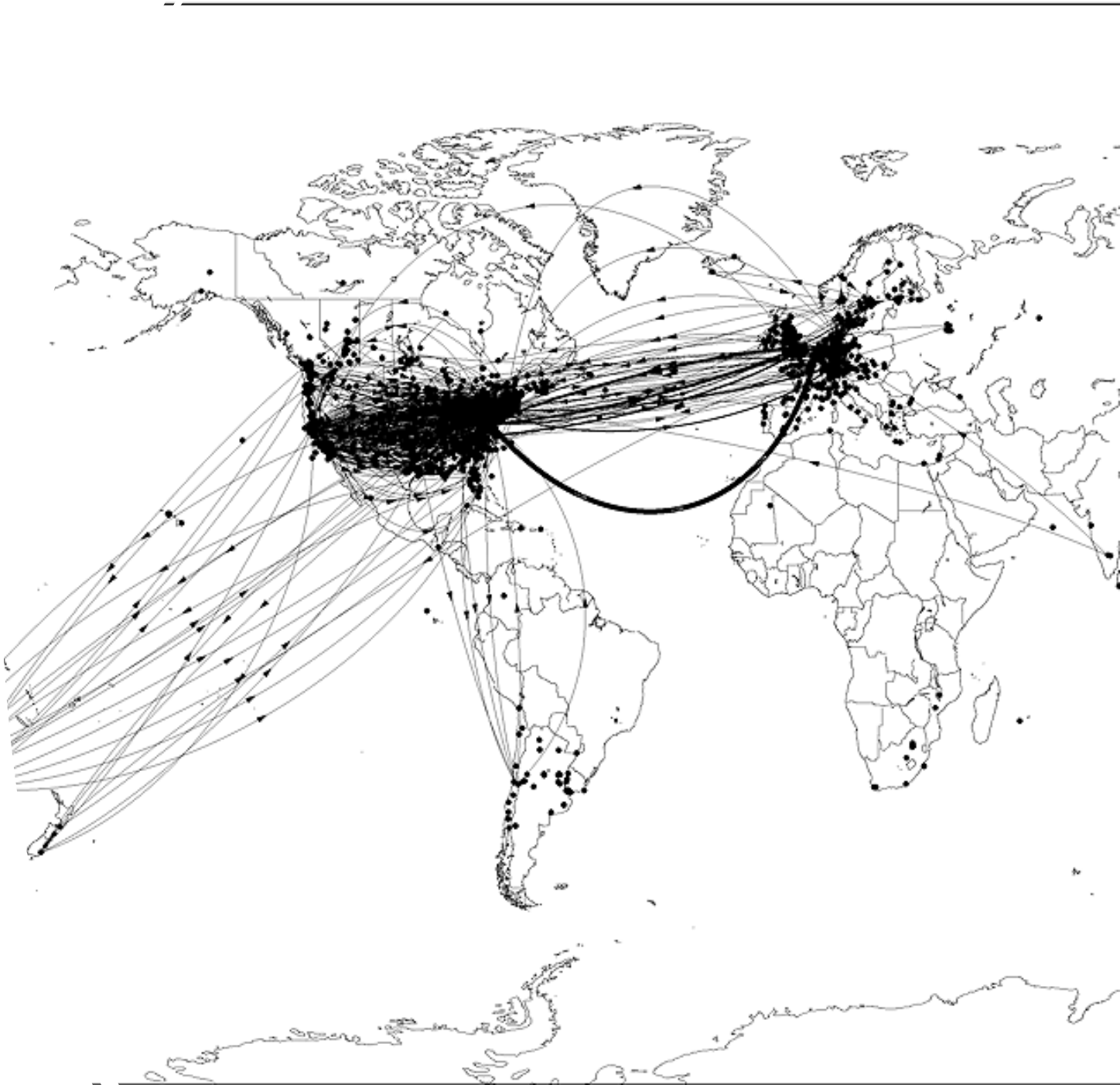
Introduction to Wireless Networking

- Wireless networks provide connectivity to various devices such as smartphones, laptops, and smart home systems.
- Importance of security in wireless networks as usage increases.



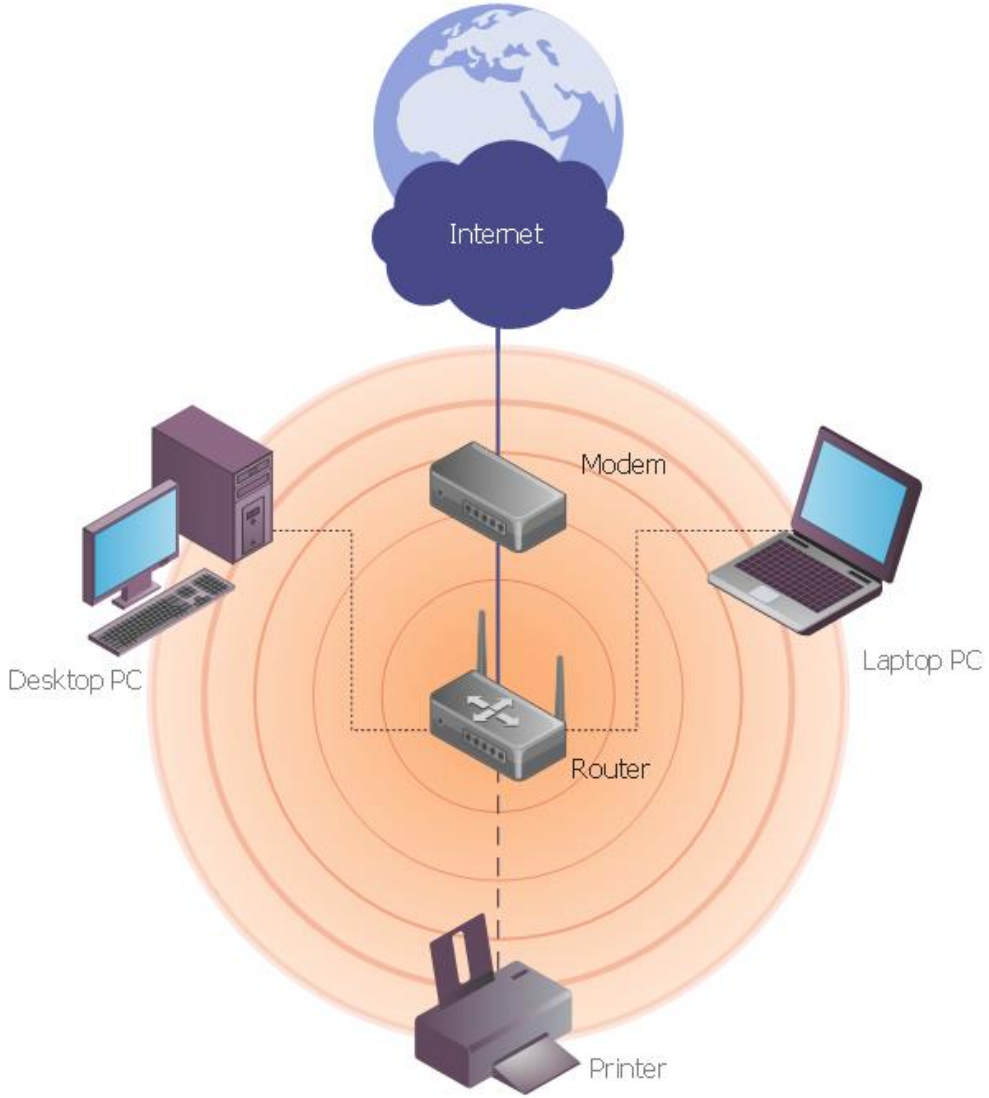
What is Wi-Fi?

- Wi-Fi is a set of standards developed by IEEE.
  - **Institute of Electrical and Electronics Engineers**
- Standardization allows interoperability of devices across the globe



Wi-Fi Technology

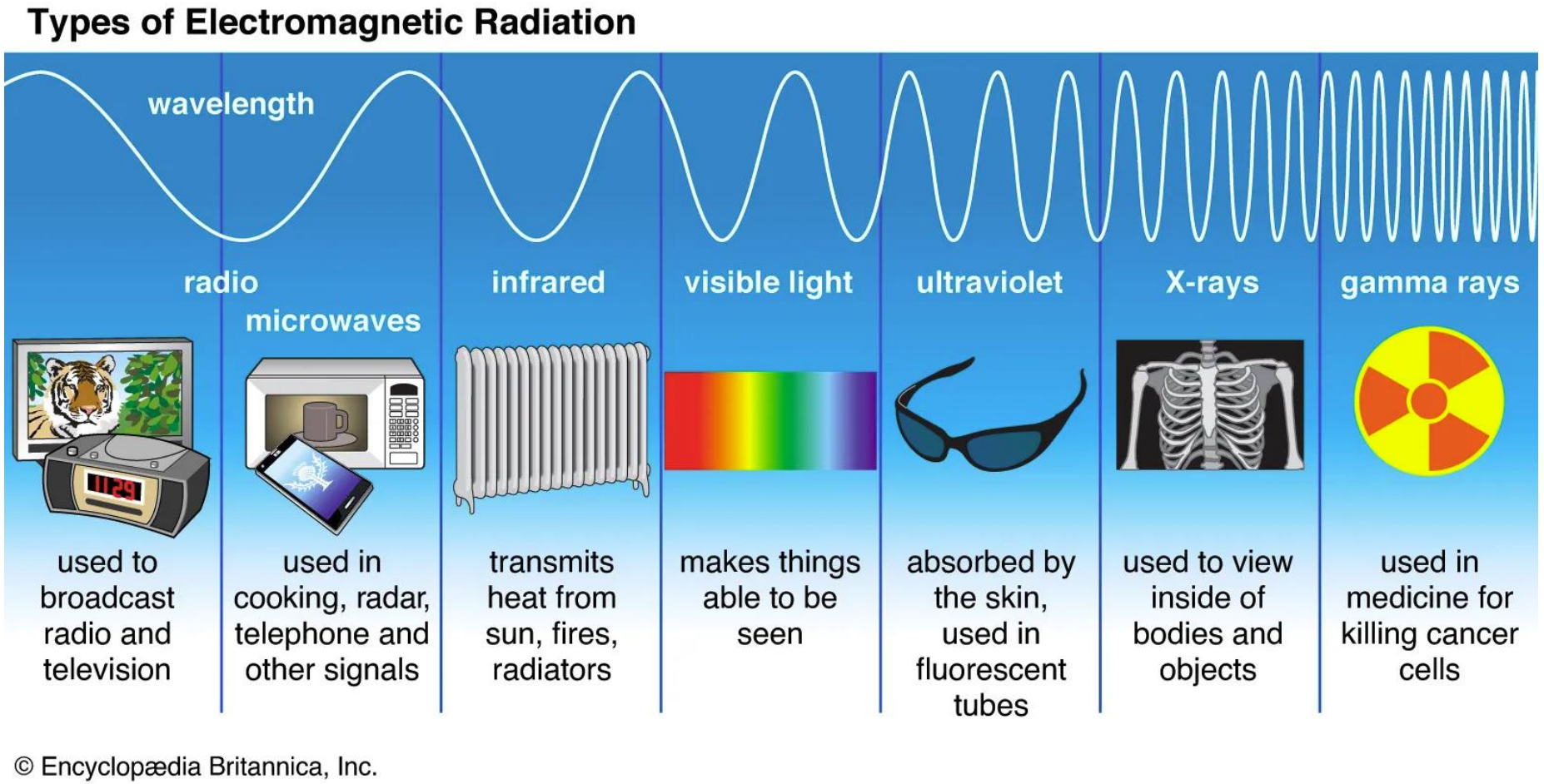
- Replaces traditional wired networks using radio transceivers.
- Allows devices to communicate with wireless access points (APs).
- APs connect wireless devices to wired networks.



Wireless Networking Standards

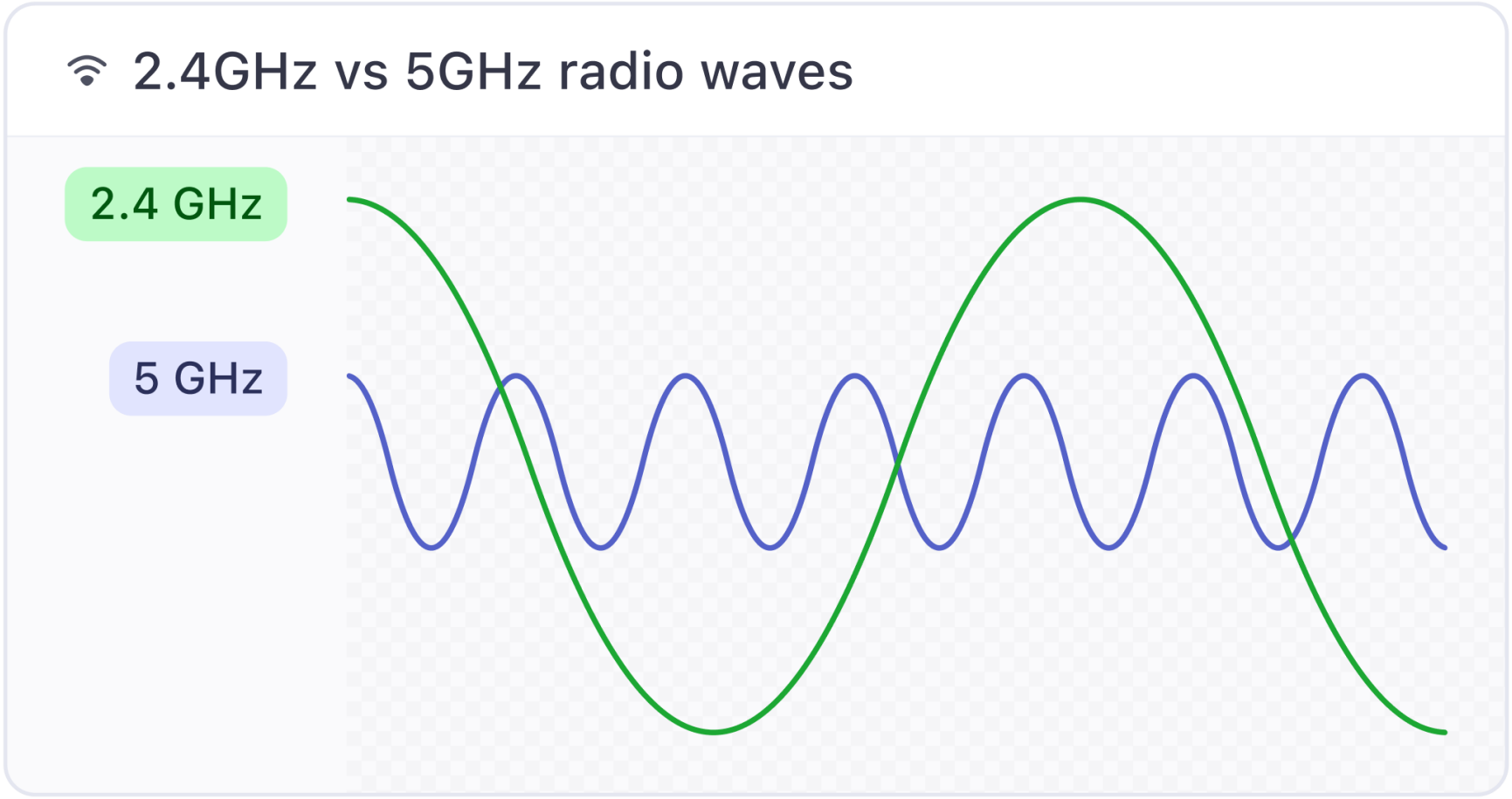
Standard	Frequency Range	Max Speed
802.11	2.4 GHz	2 Mbps
802.11a	5 GHz	54 Mbps
802.11b	2.4 GHz	11 Mbps
802.11g	2.4 GHz	54 Mbps
802.11n	2.4/5 GHz	600 Mbps
802.11ac	5 GHz	1 Gbps

Wi-Fi Standards



Electromatic Radiation

2.4 GHz vs 5 GHz



2.4 GHz Wi-Fi

- **Speed:** Slower
- **Range:** Longer
- **Bonus:** Better wall penetration, more crowded (microwaves, Bluetooth, etc.)

1. You’re far from the router (like in a house)

- Signal needs to go through walls and floors.
- Example: You're gaming in your bedroom upstairs while the router chills downstairs.

2. Outdoor coverage is needed

- Setting up Wi-Fi in your backyard, garden, or driveway.
- Example: You’re trying to watch Netflix in a hammock under a tree.

3. You’re using smart home devices

- IoT gadgets (smart bulbs, plugs, cameras) usually stick to 2.4 GHz.
- Example: Your security camera on the garage needs range, not Netflix.

5.0 GHz Wi-Fi

- **Speed:** Faster
- **Range:** Shorter
- **Bonus:** Less interference, but struggles with walls

1. You need speed and low latency

- Streaming 4K, video calls, or online gaming near the router.
- Example: You're in the living room, bingeing 4K shows while live-tweeting.
  Latency = The **time it takes** for data to travel from **your device** to **a destination** (like a server or another device) **and back again**.

2. There’s a lot of wireless congestion

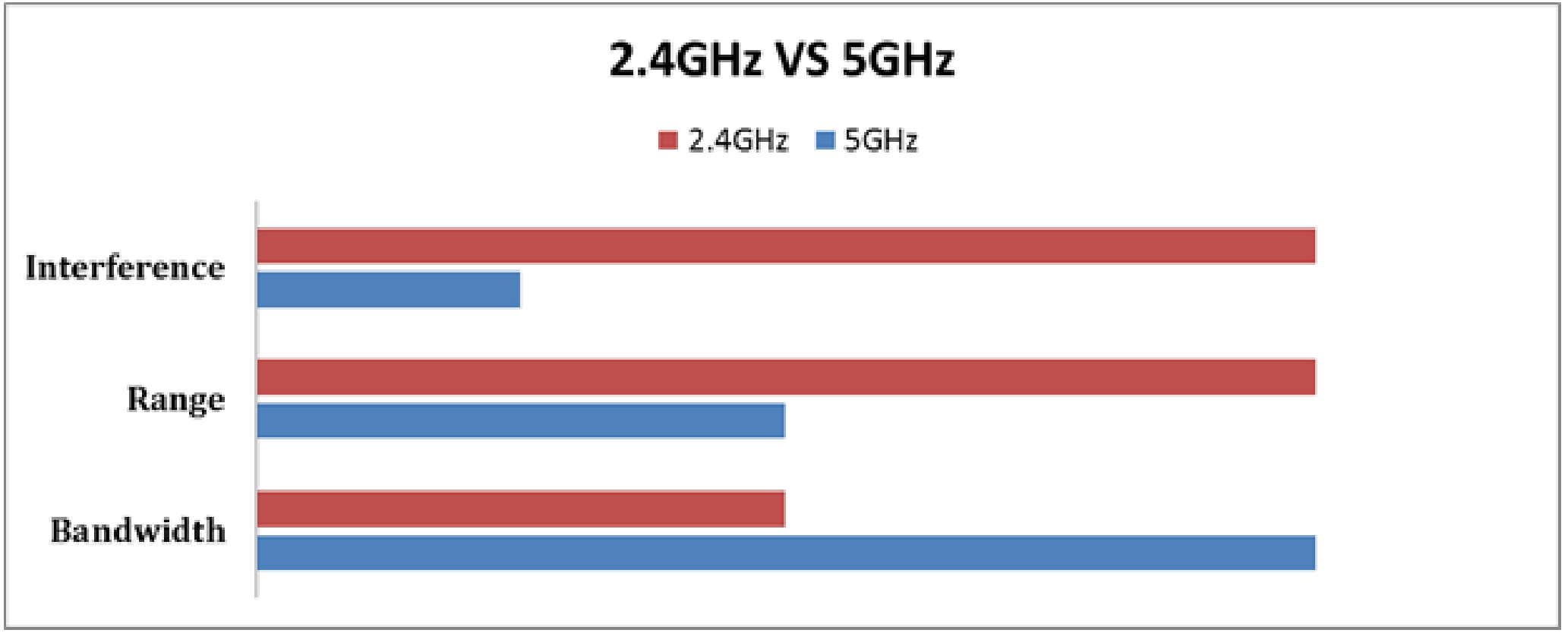
- 2.4 GHz is crowded with microwaves, baby monitors, and your neighbor’s Wi-Fi.
- Example: In a city apartment where 30 routers battle for dominance.

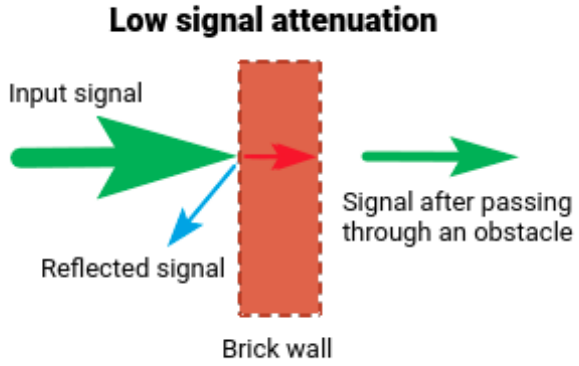
3. You're doing work that needs fast transfers

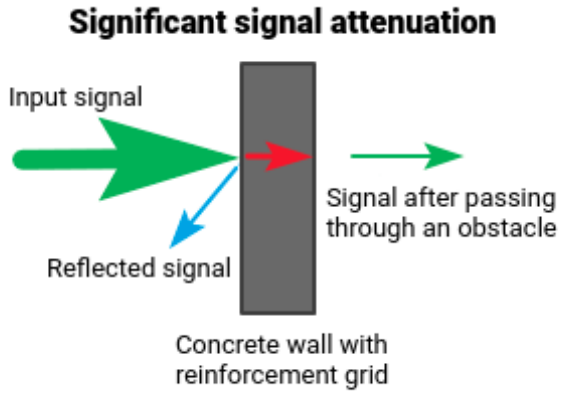
- Big file uploads/downloads, virtual machines, cloud development.

Frequency Ranges

- 2.4 GHz: Greater distance, slower speed.
- 5 GHz: Faster speed, shorter range.
- Choosing frequency depends on speed and range trade-offs.







Wireless Signal Propagation

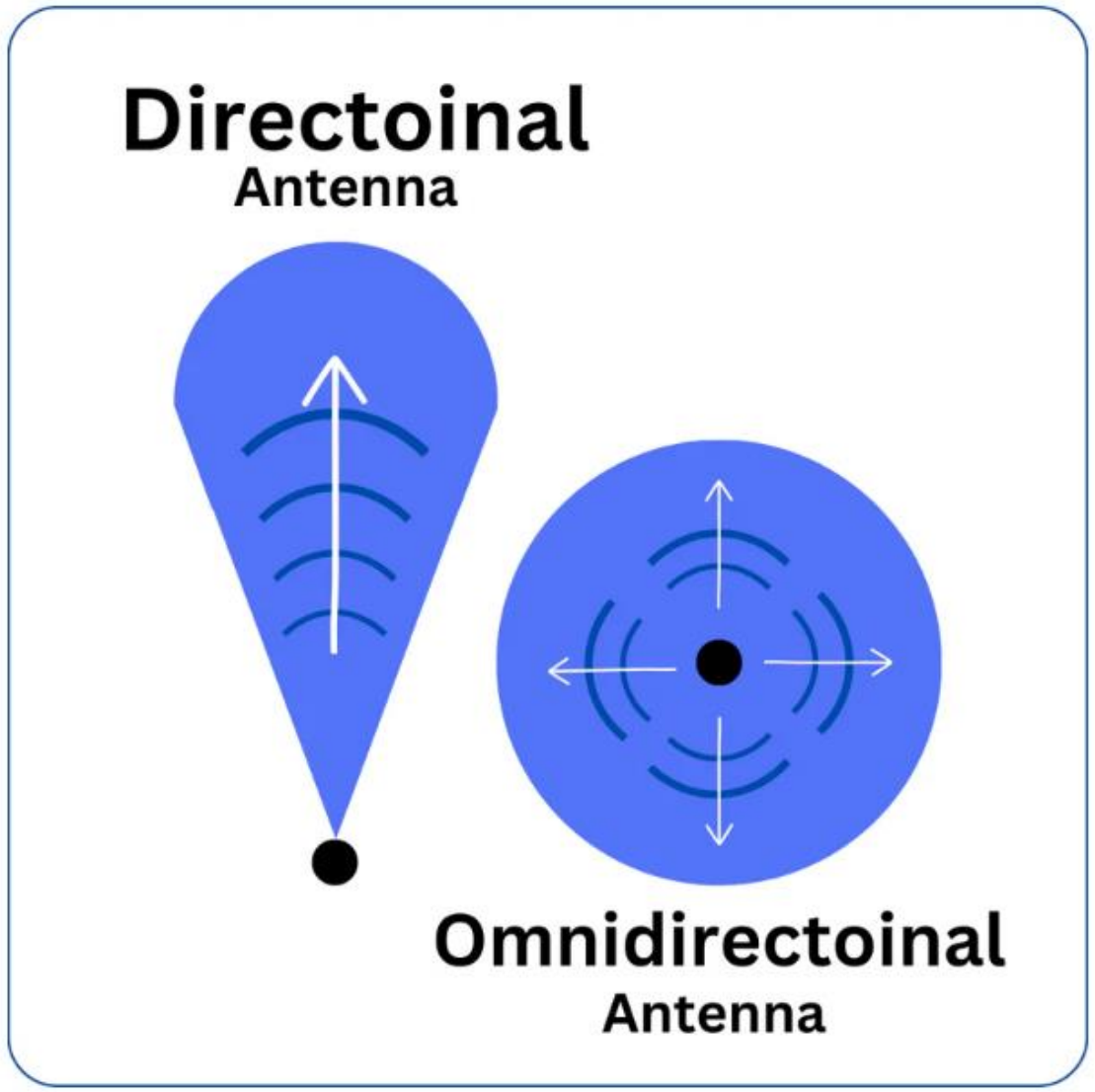
- Wi-Fi signals are radio transmissions.
- Signals can be picked up by anyone with the right equipment.
- Factors such as building materials and antenna placement affect signal strength.

Wireless Antennas

- **Omnidirectional Antennas:** Broadcast signals in all directions.
- **Directional Antennas:** Focus the signal in one direction, ideal for point-to-point connections.

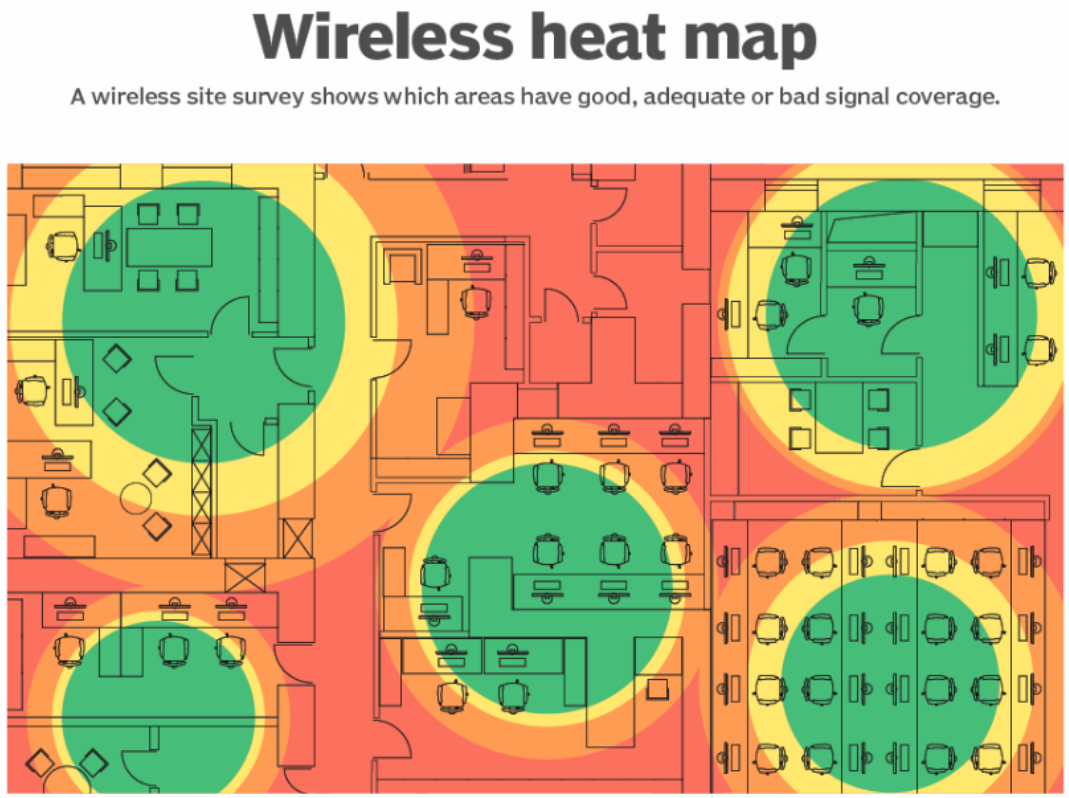
Signal Behavior:

- **Attenuation**: Weakening of signal due to walls, interference, or distance.
- **Beamforming (802.11ac)**: Dynamically directs signals toward the device.



Wireless Device Placement

- Site surveys help determine optimal placement of access points.
- Heat maps show strong and weak signal areas.
- **Image Suggestion:** Example of a heat map generated during a wireless site survey.

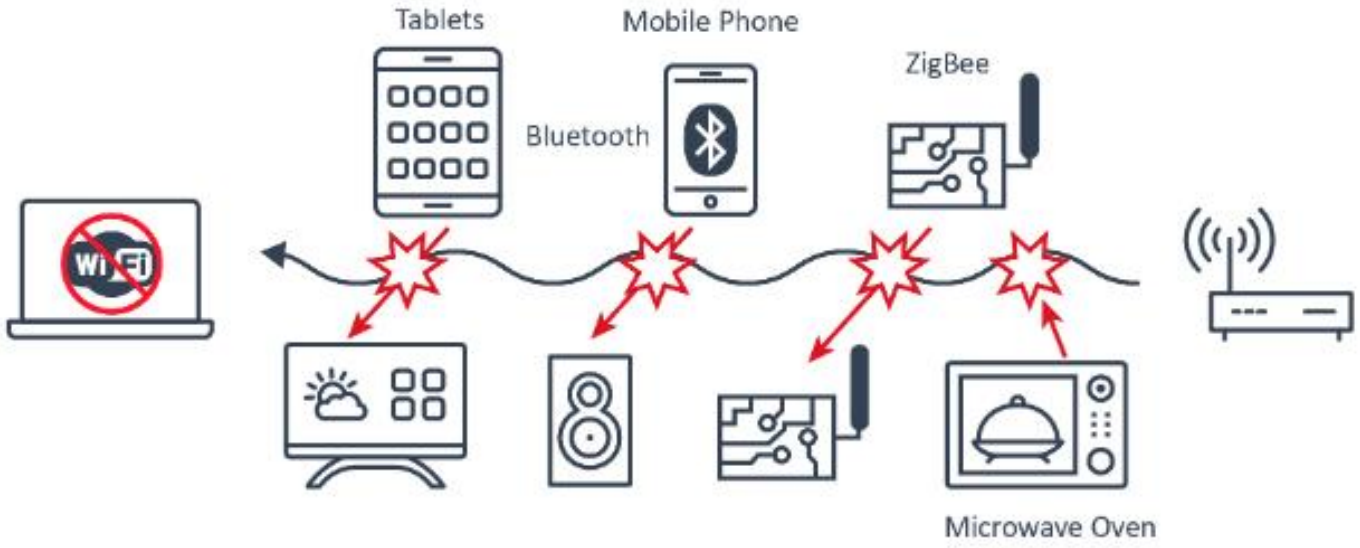


Site Survey:

- Use tools to create **heat maps** of signal strength.
- Identify **dead zones** and **EMI (electromagnetic interference)** sources (microwaves, baby monitors, etc.).

Wireless Interference

- Interference can come from other wireless networks or devices (e.g., baby monitors, microwaves).
- Adjusting wireless channels can reduce interference.

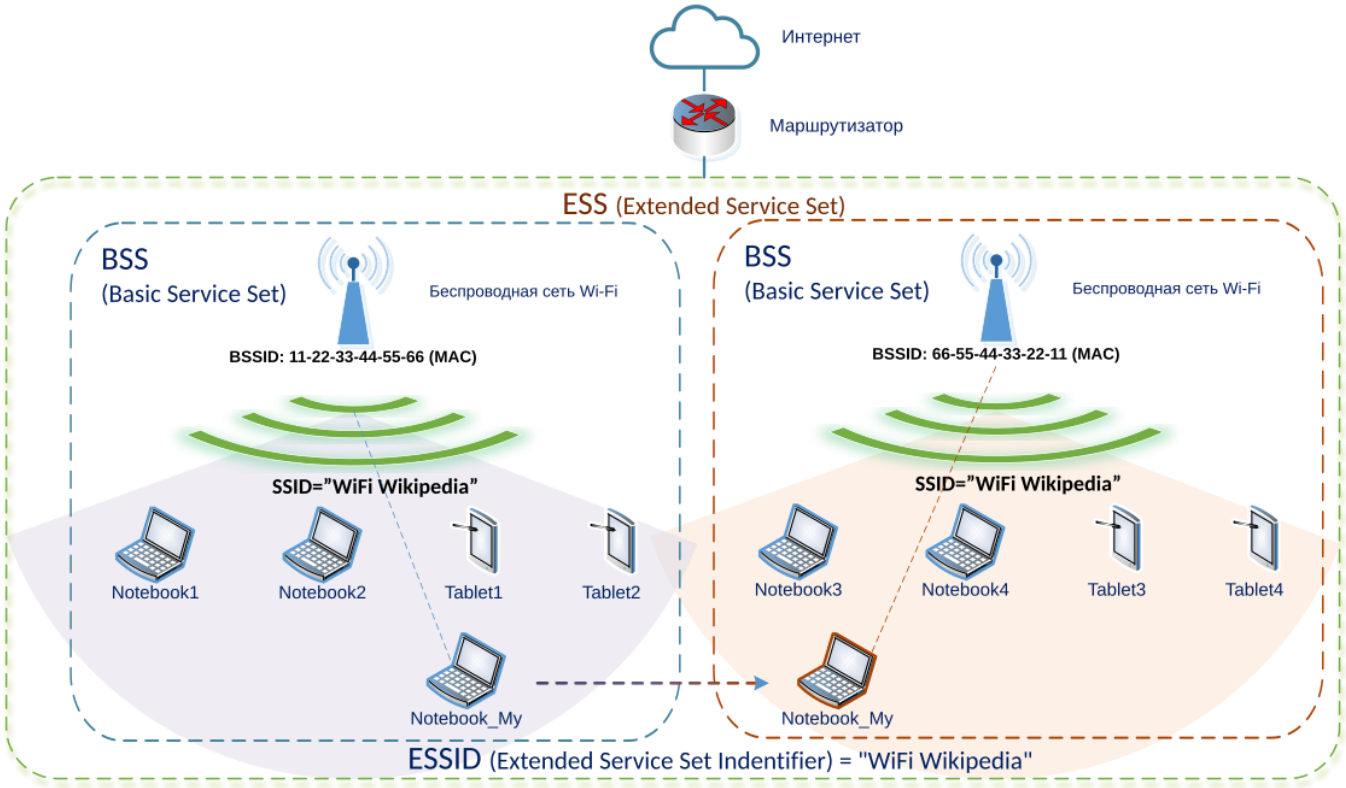


Wireless Security Threats

- Wireless networks are susceptible to eavesdropping.
- Use of encryption is essential to protect network traffic.

SSID Management

- Each wireless network broadcasts an SSID (network name).
- Disabling SSID broadcasting hides the network.

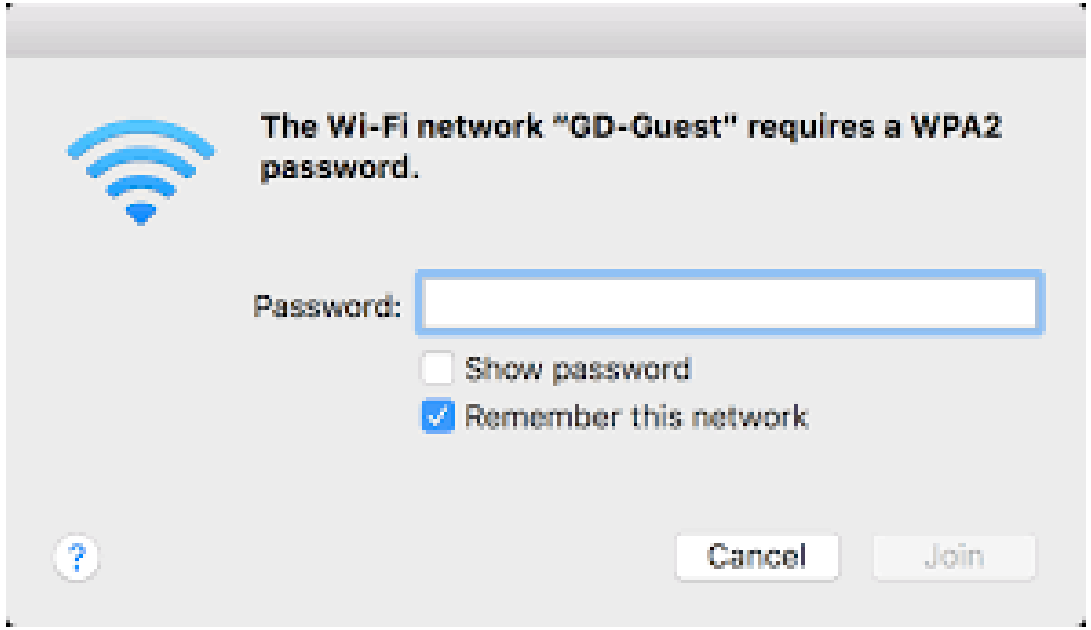


Access Point Passwords

- Change default passwords on wireless access points immediately.
- Use strong passwords known only to network administrators.

Wireless Access Controls

- **Open Networks:** No authentication, accessible to all.
- **Pre-Shared Keys:** Common for small networks but not ideal for large environments.
- **Enterprise Authentication:** Requires username and password for access.
- **Captive Portals:** Common in public spaces like hotels and cafes.



Wireless Encryption Protocols

Standard	Security Status	Encryption	Mode
Open	Insecure	None	None
WEP	Insecure	RC2	None
WPA	Insecure	RC4	TKIP
WPA2	Secure	AES	CCMP
WPA3	Secure	AES	CCMP + SAE

Security Protocols

Wired Equivalent Privacy (WEP)

- The original approach. Suffer from security vulnerabilities. Security professionals no longer consider WEP secure.

Wi-Fi Protected Access (WPA)

- A newer technology. Replace WEP back in 2003. However, has vulnerabilities. Makes it a poor choice for use on wireless networks.
-

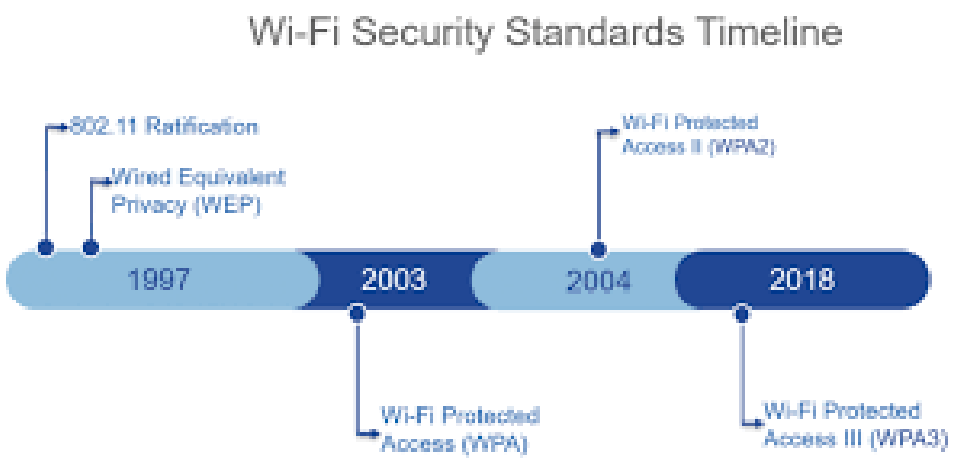
Wi-Fi Protected Access v2 (WPA2)

- In 2004, WPA2 was released as an upgrade to WPA. Security researchers have discovered some potential issues with WPA2, but it is still considered secure and it is widely used.
-

Wi-Fi Protected Access v3 (WPA3)

- As of 2020, new wireless devices are required to support WPA3 standard. Simultaneous Authentication of Equals (SAE), is a secure key exchange protocol technique that provides a secure initial setup of encrypted wireless communications.

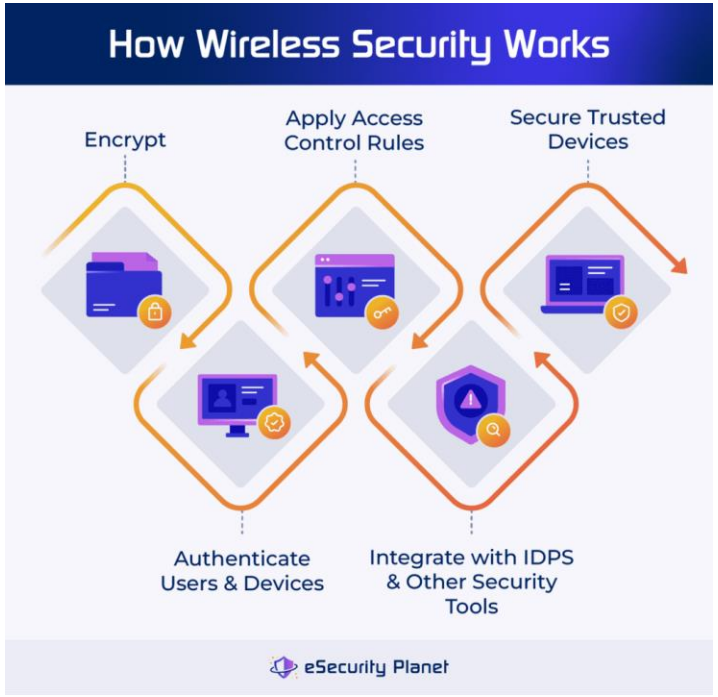
Wireless Encryption Explained



- **WEP:** Outdated and insecure.
- **WPA:** Improved security but still has vulnerabilities.
- **WPA2:** Current standard, widely used.
- **WPA3:** Latest standard, required for new devices.

Enhancing Security with VPNs

- VPNs provide encryption even on insecure networks.
- Ideal for public Wi-Fi in hotels, cafes, and airports.

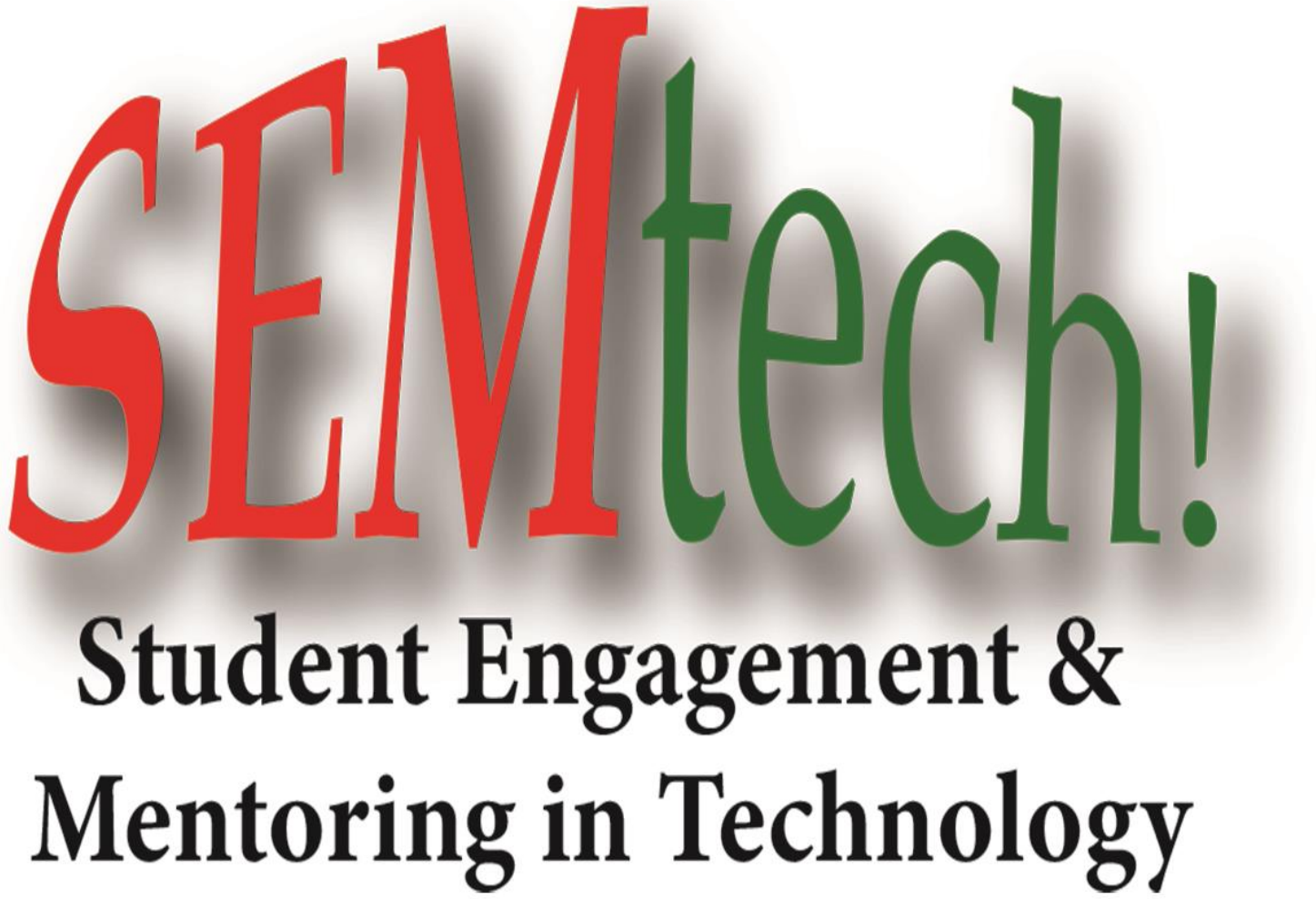


Conclusion

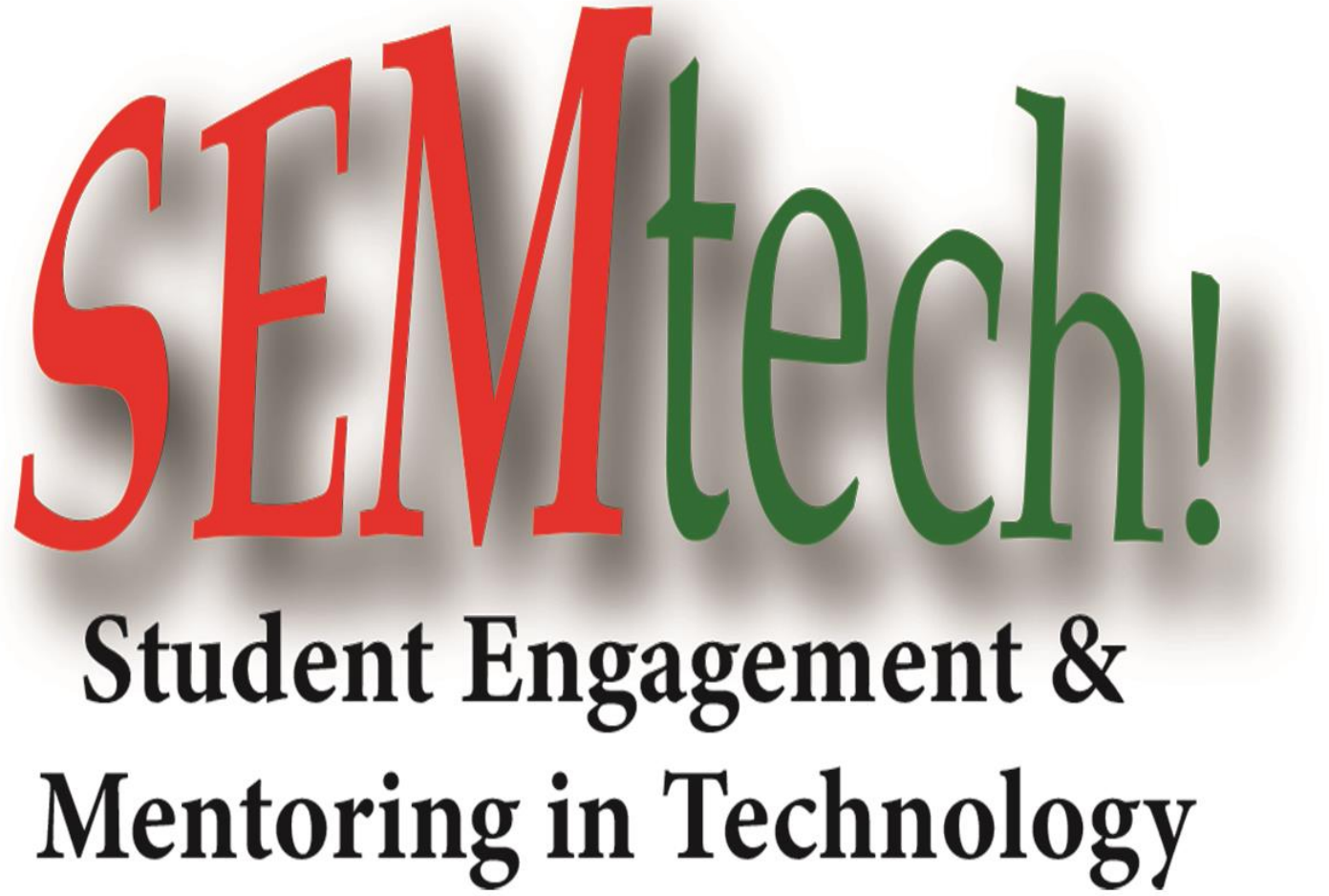
- Proper installation and security practices are essential for wireless network efficiency and safety.
- Use encryption, strong passwords, and appropriate device placement for optimal performance.

Q&A

????Questions and Answers?????



The End Wireless Networks



Thomas Holt Russell, M.Ed., D. Hon. (Cybersecurity)