SEMtech!
Student Engagement & Mentoring in Technology

Study Guide: Wireless Networks

Objective
Understand basic wireless networks, including standards, frequencies, antennas, security protocols, and placement best practices.

---

1. Introduction to Wireless Networking

Wireless networks allow devices like smartphones, tablets, laptops, TVs, thermostats, and IoT devices to connect without physical cables using radio waves.

Key Components:

- **Wi-Fi**: Most common wireless standard.
- **Access Point (AP)**: A device that connects wireless clients to a wired network.
- **Radio Transceivers**: Embedded in all Wi-Fi-capable devices.

---

2. Wireless Standards and Frequencies

IEEE 802.11 Standards Overview:

Wireless Standard Frequencies & Speed

Standard	Frequency	Max Speed
802.11	2.4 GHz	2 Mbps
802.11a	5.0 GHz	54 Mbps
802.11b	2.4 GHz	11 Mbps
802.11g	2.4 GHz	54 Mbps
802.11n	2.4/5.0 GHz	600 Mbps
802.11ac	5.0 GHz	1 Gbps+

SEMtech!
Student Engagement & Mentoring in Technology

REMEMBER:

- **2.4 GHz = Slower, Longer Range**
- **5.0 GHz = Faster, Shorter Range**

Choose based on device compatibility and physical layout.

2.4 GHz Wi-Fi

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

5.0 GHz Wi-Fi

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

Use 2.4 GHz when:

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.

Use 5.0 GHz when:

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.
-

---

3. Antennas and Signal Propagation

Antenna Types:

- **Omnidirectional**: Broadcasts in all directions (used in most home/office APs).
- **Directional**: Focused signal for long-range point-to-point use.

Signal Behavior:

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

---

4. Access Point Placement & Interference

Site Survey:

- Use tools to create **heat maps** of signal strength.

- Identify **dead zones** and **EMI (electromagnetic interference)** sources (microwaves, baby monitors, etc.).

Optimization Tips:

- Adjust the **channel** to avoid overlap with neighbors.
- Adjust **power levels** to manage coverage and avoid interference.

---

5. Wireless Security Essentials

SSID (Service Set Identifier):

- Public name of the network.
- Can be hidden to avoid casual detection.

Access Point Admin Password:

- Always **change default passwords**.
- Use strong credentials to prevent unauthorized config changes.

---

6. Wireless Access Controls

Wireless Access Controls

Method	Use Case	Limitations
Open Network	Public places	No authentication; insecure.
Pre-Shared Key (PSK)	Homes, small offices	Shared key; hard to manage users individually.
Enterprise Auth	Organizations with multiple users	Requires central auth server; supports user-based access.
Captive Portal	Hotels, cafes, airports	Redirects to login or terms of service page

---

SEMtech!
Student Engagement & Mentoring in Technology

7. 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

Tip: Use **WPA2** or **WPA3**. Never use **WEP** or **WPA**.

For public or untrusted Wi-Fi: Use a **VPN** for added encryption.

Practice Questions

Question 1:

Your organization recently experienced an eavesdropping attack. Which one of the following security enhancements would best protect against this type of attack?

A. Enabling WPA2
B. Enabling WEP
C. Changing SSIDs
D. Changing Channels

Answer: A – Enabling WPA2
Why? WPA2 encrypts wireless traffic, protecting against eavesdropping.
Why not the others?

- B: WEP is insecure.
- C: SSID changes don't secure data.
- D: Channel changes avoid interference, not attacks.

Question 2:

Student Engagement & Mentoring in Technology

Which wireless standard allows the highest speed using 2.4 GHz?

A. 802.11ac
B. 802.11b
C. 802.11g
D. 802.11n

Answer: D – 802.11n
Why? 802.11n can operate at 2.4 GHz and offers speeds up to 600 Mbps.
Why not the others?

- A: 802.11ac is faster but uses **5 GHz**.
- B: Slower (11 Mbps).
- C: Maxes at 54 Mbps.

Key Takeaways

- **Know your standards**: Memorize 802.11 variations by speed and frequency.
- **Use secure authentication**: Enterprise > PSK > Open.
- **Use encryption**: WPA2 or WPA3 only.
- **Optimize placement**: Use site surveys and heat maps.
- **Watch for interference**: Channels, EMI, and neighboring networks.

SEMtech!
Student Engagement & Mentoring in Technology

Videos to Watch

Computer Networks (Khan Academy) - AP Computer Science Principles

IP addresses and DNS | Internet 101 | Computer Science | Khan Academy

Packet, routers, and reliability | Internet 101 | Computer Science | Khan Academy

WIFI (wireless) Standards and Generations Explained

SEMtech!
Student Engagement & Mentoring in Technology

Wireless Encryption

WEP (Wired Equivalent Privacy) is an outdated and insecure wireless security protocol that was originally designed to provide a level of data protection on Wi-Fi networks equivalent to that of wired networks. Introduced in the late 1990s as part of the IEEE 802.11 standard, WEP uses static encryption keys (either 40-bit or 104-bit) and the RC4 stream cipher to encrypt data. However, it has significant vulnerabilities, such as weak key management and predictable encryption patterns, which make it highly susceptible to attacks like key cracking within minutes using common tools. Due to these flaws, WEP has been officially deprecated and replaced by more secure protocols like **WPA** and **WPA2**, making it unsuitable for any modern network that values data privacy and integrity.

WPA (Wi-Fi Protected Access) was introduced in 2003 as a major upgrade to WEP, aiming to fix its numerous security flaws while providing stronger encryption and user authentication for wireless networks. WPA uses **TKIP (Temporal Key Integrity Protocol)**, which dynamically changes encryption keys and includes mechanisms like message integrity checks to prevent tampering and replay attacks. While WPA was a big step up from WEP, it was always intended as a transitional solution, still relying on the aging **RC4** cipher and eventually showing vulnerabilities of its own. Despite being more secure than WEP, WPA has largely been phased out in favor of **WPA2** and **WPA3**, which offer more robust protection using modern encryption methods like AES.

WPA2 (Wi-Fi Protected Access 2) is a security protocol introduced in 2004 as the successor to WPA, offering significantly improved protection for wireless networks. Unlike its predecessor, WPA2 uses **AES (Advanced Encryption Standard)**, a strong and modern encryption algorithm that provides robust confidentiality and is approved for government use. WPA2 also implements **CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol)** for integrity and key management, replacing the vulnerable TKIP used in WPA. WPA2 comes in two main modes: **Personal (WPA2-PSK)** for home networks using a shared password, and **Enterprise (WPA2-Enterprise)**, which uses a RADIUS server and 802.1X for advanced authentication. It remains one of the most widely used standards, although it's now gradually being replaced by **WPA3**, which addresses WPA2's remaining weaknesses like brute-force attacks on weak passwords.

WPA2 (Wi-Fi Protected Access 2) is a security protocol introduced in 2004 as the successor to WPA, offering significantly improved protection for wireless networks. Unlike its predecessor, WPA2 uses **AES (Advanced Encryption Standard)**, a strong and modern encryption algorithm that provides robust confidentiality and is approved for government use. WPA2 also implements **CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol)** for integrity and key management, replacing the vulnerable TKIP used in WPA. WPA2 comes in two main modes: **Personal (WPA2-PSK)** for home networks using a shared password, and **Enterprise (WPA2-Enterprise)**, which uses a RADIUS server and 802.1X for

advanced authentication. It remains one of the most widely used standards, although it's now gradually being replaced by **WPA3**, which addresses WPA2's remaining weaknesses like brute-force attacks on weak passwords.

Wireless Device Placement Basics:

Where you place your **Access Points (APs)** or **wireless routers** can *make or break* your network performance. You want signal strength to be **strong, even, and interference-free**.

Best Practices for Placement:

1. **Central Location**
   - Place the AP near the *center* of the coverage area.
   - Wi-Fi radiates in all directions — think of it like a light bulb, not a laser beam.
2. **Height Matters**
   - Mount it on a wall or ceiling, away from the floor.
   - Think "eye-level or higher" — Wi-Fi hates crawling through furniture.
3. **Avoid Obstructions**
   - Walls, floors, mirrors, fish tanks (yes, seriously), and metal objects all kill signal.
   - Place the device in open space when possible.
4. **Minimize Interference**
   - Keep away from microwaves, cordless phones, baby monitors, and *angry Bluetooth speakers*.
   - Especially critical for 2.4 GHz, which is more crowded.
5. **Use Dual-Band Wisely**
   - 2.4 GHz travels farther, better for distance.
   - 5 GHz is faster but weaker through walls — place 5 GHz APs closer to users.
6. **Don’t Hide It!**
   - Shoving your AP in a closet might look tidy, but your signal’s gonna suffer.
   - If you can’t see the AP, your signal probably can’t either.

In Larger Spaces:

- Use **multiple APs** to eliminate dead zones.
- Use a **site survey** (heat map tools) to visualize coverage.
- Set channels properly to avoid overlap (especially on 2.4 GHz).

What Is Wireless Interference?

Interference is when **other signals** or **obstacles** disrupt your Wi-Fi signal, causing:

- Slower speeds

- Dropped connections
- High latency
- Angry users

Think of it like trying to have a convo at a loud concert. Your voice = Wi-Fi signal, the crowd = interference.

Types of Interference:

1. Co-Channel Interference (CCI)

- Happens when multiple APs use the *same channel*.
- Devices politely take turns → slows everything down.
- Fix: Use **non-overlapping channels** (1, 6, 11 on 2.4 GHz).

2. Adjacent-Channel Interference (ACI)

- Occurs when APs use *overlapping* channels (like 2, 3, 4…).
- Causes **signal mixing** and packet loss.
- Fix: Stick to those golden, non-overlapping channels.

3. Non-Wi-Fi Interference

- Other electronics can emit noise in the same frequency range:
  - **Microwaves**
  - **Bluetooth**
  - **Baby monitors**
  - **Cordless phones**
  - Even **Christmas lights**

4. Physical Obstacles

- Walls (especially concrete or metal)
- Furniture
- Mirrors
- Water (like fish tanks and even humans!)
- These block or reflect the signal, especially at 5 GHz.

Student Engagement & Mentoring in Technology

Key Facts by Frequency:

Frequency	Interference Susceptibility
2.4 GHz	More interference (crowded frequency)
5 GHz	Less interference, but worse at penetrating walls

🔧 How to Reduce Interference:

- **Change channels** manually if auto-select is failing.
- **Switch to 5 GHz** when possible.
- **Move devices/APs** away from noise sources.
- **Use wired connections** for high-demand devices (your PS5 thanks you 🎮).
- **Limit overlapping APs** in business networks.

What Is SSID?

SSID (Service Set Identifier) is the **name** of a wireless network that devices see when they scan for available Wi-Fi.
It's like the "Welcome" sign for your Wi-Fi party.

When your phone says:

*"Connect to **CoffeeShop_WiFi**?"*
That **CoffeeShop_WiFi** is the SSID.

1. RC4 (Rivest Cipher 4)

- **Type:** Stream cipher
- **Used in:** WEP and WPA (with TKIP)
- **Speed:** Fast
- **Security:** Broken — vulnerable to key recovery and packet injection
- **Status:** Obsolete — retired faster than floppy disks.

RC4 is like that fast-talking friend who can't keep secrets — efficient but super insecure.

---

2. TKIP (Temporal Key Integrity Protocol)

- **Type:** Key management + encryption wrapper
- **Used in:** WPA
- **Pairs with:** RC4
- **Improved:** Added per-packet key mixing and integrity checks (MIC)
- **Security:** Better than WEP, but still vulnerable today
- **Status:** Deprecated

TKIP was the **"Band-Aid fix"** for WEP — better, but still not secure enough for serious business. Think of a "temporary patch" that overstayed its welcome.

---

3. AES (Advanced Encryption Standard)

- **Type:** Block cipher
- **Used in:** WPA2 and WPA3
- **Security: Top-tier** — widely trusted and used even by governments
- **Key Sizes:** 128, 192, or 256 bits
- **Speed:** Slower than RC4, but still fast and secure on modern hardware

AES is the **bodyguard of Wi-Fi encryption** — strong, reliable, and respected.

---

4. CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol)

- **Type:** Protocol that **uses AES** for encryption + message integrity
- **Used in:** WPA2 and WPA3
- **Security:** Strong — includes counter mode (for confidentiality) and CBC-MAC (for integrity)
- **Replaces:** TKIP
- **Status:** Gold standard (until WPA3's SAE took the wheel)

CCMP is like AES's tactical gear — not just strong encryption but also **message authenticity** and **anti-replay** protection.

Quick Comparison Table					
Term	**Type**	**Used In**	**Encryption**	**Security Level**	**Status**
RC4	Stream Cipher	WEP, WPA (w/TKIP)	Weak	Broken	Retired
TKIP	Key Protocol	WPA	RC4	Weak-ish	Deprecated
AES	Block Cipher	WPA2, WPA3	Strong	Strong	Active
CCMP	AES-based Protocol	WPA2, WPA3	AES	Very Strong	Active

SEMtech!
Student Engagement & Mentoring in Technology

- RC4 and TKIP = old, insecure bros from the WEP/WPA days.
- AES and CCMP = the modern muscle of WPA2 and WPA3.

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