CCNA: Introduction to Network

**Module 4 – 4.6: Wireless Media**

**1. 802.11 Standards (Wi-Fi):**

* **802.11a:** Older standard, **used 5 GHz frequency**, higher data rates than 802.11b, but shorter range.
* **802.11b:** Older standard, **used 2.4 GHz frequency**, lower data rates, longer range. Prone to interference.
* **802.11g:** **Used 2.4 GHz**, higher data rates than 802.11b, backward compatible.
* **802.11n:** Used both **2.4 GHz and 5 GHz**, multiple antennas (MIMO), significantly higher data rates.
* **802.11ac (Wi-Fi 5):** **Primarily 5 GHz**, even higher data rates, wider channels.
* **802.11ax (Wi-Fi 6):** Both **2.4 GHz and 5 GHz**, improved efficiency, higher capacity, better performance in congested environments (OFDMA, MU-MIMO).
* **802.11be (Wi-Fi 7):** **Tri-band (2.4GHz, 5GHz, and 6GHz**), even higher speeds, lower latency, more capacity.

**Key things to remember about each standard:** Frequency band, data rate, range, and any significant features.

**II. Wireless Network Topologies:**

* **Ad Hoc:** Direct, **peer-to-peer connection** between wireless devices, no central access point. Used for small, temporary networks.
* **Infrastructure:** Uses **an access point (AP**) as a central connection point for all wireless devices. The AP connects to the wired network. This is the most common type of wireless network.
* **Mesh:** Devices act as both clients and routers, extending the range of the network. Used in situations where cabling is difficult.

**III. Wireless Network Components:**

* **Wireless NICs:** Internal or external adapters that allow devices to connect to a wireless network. They transmit and receive radio signals.
* **Access Points (APs):** Devices that provide wireless connectivity. They act as a bridge between wireless and wired networks. They broadcast the SSID, handle authentication, and manage wireless traffic.
* **Antennas:** Used to transmit and receive radio signals. Omnidirectional antennas radiate signals in all directions, while directional antennas focus the signal in a specific direction.

**IV. Wireless Signal Characteristics:**

* **Frequency:** The number of radio waves that pass a point in a given time. Measured in Hertz (Hz).
* **Wavelength:** The distance between two consecutive peaks of a radio wave. Related to frequency.
* **Attenuation:** The decrease in signal strength as it travels through the air or encounters obstacles.
* **Interference:** Unwanted radio signals that can disrupt wireless communication. Sources of interference include other Wi-Fi networks, Bluetooth devices, microwaves, and other electronic devices.
* **Reflection:** When a radio wave bounces off a surface.
* **Diffraction:** When a radio wave bends around an obstacle.
* **Scattering:** When a radio wave is dispersed in multiple directions by small objects.

**V. Wireless Security:**

* **Open Authentication:** No security, anyone can connect.
* **WEP:** Older, weak encryption protocol. Easily cracked and should not be used.
* **WPA:** Improved security over WEP, but still has vulnerabilities.
* **WPA2:** Current standard, uses stronger encryption (AES). Recommended for most wireless networks.
* **WPA3:** The latest standard, offers even stronger security and improved authentication.

**VI. Configuration:**

* **SSID (Service Set Identifier):** The name of the wireless network.
* **Channel:** The frequency band used by the wireless network. Choosing the right channel can help reduce interference.
* **Security Key/Password:** Used to authenticate users and prevent unauthorized access.

**VII. Challenges and Considerations:**

* **Limited Bandwidth:** Wireless networks typically have lower bandwidth than wired networks.
* **Security Risks:** Wireless networks are more vulnerable to eavesdropping and unauthorized access.
* **Interference:** Wireless signals are susceptible to interference from other devices.
* **Range Limitations:** Wireless signals have a limited range.
* **Mobility Issues:** Handing off connections between access points can sometimes cause brief interruptions.