Networking

Wireless Equipment & Standards

Wireless Equipment & Standards

- Guiding Question: How do different components and configurations of wireless networks work together to provide seamless, reliable and secure connectivity?

- Students will:
- Identify and compare the different IEEE 802.11 standards and Wi-Fi generations.
  - Explain how wireless frequencies, channels, and channel widths affect speed and interference.
  - Describe the function of band steering and how it improves network performance.
  - Describe the function of access points and compare autonomous vs. lightweight access point configurations.
  - Explain the role of wireless LAN controllers in managing large wireless networks.
  - Identify the differences between omnidirectional and directional antennas and when each is appropriate to use.

Wireless Communications

- Signals are delivered without cables, using electromagnetic energy transmitted through the airwaves.
- Enables users to move around
- Permits connections in areas where it would be difficult or dangerous to install wires.
- Key components:
  1. Access Points
  2. Wireless Controllers
  3. Antennas

Access Points & Controllers

Access Points connect wireless devices to a wired network.

- One AP is enough for a home; larger places need multiple APs.
- Roaming lets users move between APs without losing signal.
- Two types of APs:
  - **Autonomous AP:** Standalone with their own settings.
  - **Lightweight AP:** Managed by a central controller.

Wireless Controllers:

- Centralized control for multiple APs.
- Handles updates, load balancing, roaming.

Wireless Antennas

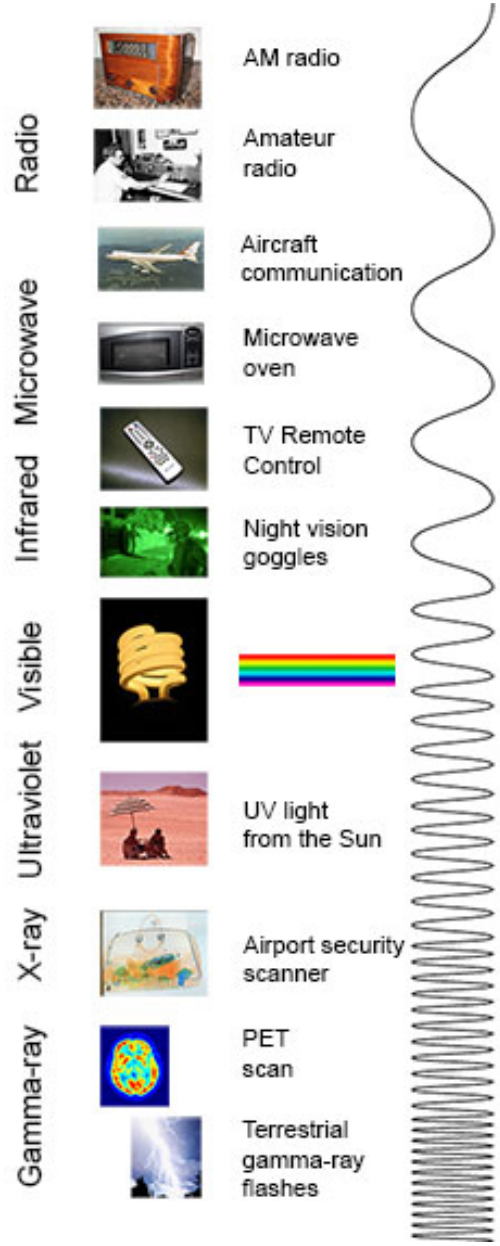
Antennas direct wireless signals:

- **Omnidirectiona**l: Signal in all directions (bubble). Good for general coverage.
- **Directional:** Focused signal in one direction (flashlight). Used for linking buildings.

Wireless Frequencies

- To broadcast across the air, wireless technologies use a frequency on the electromagnetic spectrum

- Wireless data delivery generally uses this portion of the spectrum. Notice that lots of other technologies are ALSO using that area!



Credit: NASA's Imagine the Universe

Understanding Wireless Networks

- Devices use **transceivers** to send and receive radio waves.
- These radio signals are split into frequency bands.
- Frequencies:
  - **2.4 GHz**: Longer range, goes through walls, more crowded.
  - **5 GHz**: Faster, less interference, shorter range.
  - **6 GHz**: Newest, very fast, but not all devices can use it yet.

Frequency Channels

Each frequency band is broken down into **channels**—smaller sections of the frequency.

- Can lessen interference by configuring channels properly:
- 2.4 GHz: Lots of overlap so best to use 1, 6, and 11 which are separate.
- 5 GHz: More channels easier to avoid overlap.

Channel Widths & Band Steering

Channel width affects how much data can be sent:

- 20 MHz: Most stable.
- 40 MHz: Faster, more risk of interference.
- 80/160 MHz: Very fast, but can clash with others.

Band Steering:

- Access points can "steer" devices to the best band (2.4 GHz or 5 GHz).
- Helps reduce crowding and boosts performance.

Wi-Fi Standards and Speeds

Wireless devices follow rules set by the IEEE, called the 802.11 standard (also known as Wi-Fi).

IEEE Standard	Wi-Fi Generation	Frequencies	Expected Speed
802.11a	-	5 GHz	54 Mbit/s
802.11b	-	2.4 GHz	11 Mbit/s
802.11g	-	2.4 GHz	54 Mbit/s
802.11n	Wi-Fi 4	2.4 / 5 GHZ	300 Mbit/s
802.11 ac	Wi-Fi 5	5 Ghz	600 Mbit/s - 2 Gb/s
802.11 ax	Wi-Fi 6 and 6E	2.4 / 5 / 6 Ghz	600 Mbit/s - 4.8 Gb/s
802.11 be	Wi-Fi 7	2.4 / 5 / 6 GHz	9.6 Gb/s

Wireless Rules Around the Globe

Different countries have different rules for using airwave frequencies.

- In the US, the **FCC** sets the rules.
- In Europe, the **ETSI** controls wireless use.

As it became more common for devices to travel globally, the **802.11h** standard was added. It helps compatibility with:

- **DFS**: Switches channels if radar is nearby.
- **TPC**: Lowers power to avoid interference.

Wireless Network Types

Network setups include:

- **Infrastructure:** Connect to an AP.
- **Mesh:** Nodes link to each other.
- **Point-to-Point (P2P):** Connect two distant locations.
- **Ad Hoc:** Devices connect directly.
  Also knowns as **IBSS** (Independent Basic Service Set)

Other Wireless Technologies

Beyond Wi-Fi:

- Cellular Networks (4G/5G) use cell towers for mobile connections.
- Satellite Internet serves remote areas but can be slower and weather-affected.

Wireless Naming - SSID, BSSID, and ESSID

- **SSID - Service Set Identifier**
  The name you see (e.g., "HomeNetwork").
- **BSSID - Basic Service Set Identifier**
  The hardware address of the specific access point.
- **ESSID – Extended Service Set Identifier**
  Used when many access points share the same SSID for bigger coverage.

Wi-Fi Security and Encryption

Wi-Fi needs to be secure since it's easy for outsiders to try and listen in. There are several types of security:

- **WEP**: Outdated, unsafe.
- **WPA**: Better than WEP but weak today.
- **WPA2**: Strong, widely used.
- **WPA3**: Newest, best security, encrypts each user's connection.

More Wi-Fi Security

Authentication Types:

- Pre-Shared Key (PSK): One password for everyone (homes).
- Enterprise (802.1X): Username/password for each person (schools, businesses).

Wireless Access Restrictions:

- Guest Wi-Fi: Separate network for visitors.
- May use captive portal pages for login or rules.
- Keeps the main network safer