Topic 4D: Compare Wireless Networking Types

Access Points:

An access point is a device that allows wireless devices (like laptop, phone) to connect to a wired network. It acts as a bridge between wireless networks and wired networks. The **Access Point** connects to the wired network (e.g. switch or router) via an **Ethernet** cable. It then broadcasts the wireless signal (Wi-Fi) that devices can connect to.

Wireless technology uses **radio waves** as the main transmission media. Radio system uses transmission and reception antennas tuned to specific frequencies to transmit the signals. These standards follow **IEE 802.11** standards commonly known as **Wi-Fi.**

Most Wi-Fi networks are configured in what is technically referred to as "**infrastructure mode**." **Infrastructure mode** is a wireless network configuration where all devices connect to the network through a **central device**, usually an **access point** (AP) or a **wireless router**. In the 802.11 documentation, this is referred to as an infrastructure "Basic Service Set" (BSS). The MAC address of the AP's radio is used as the **Basic Service Set Identifier (BSSID).**

The **BSSID** is a unique identifier for a specific **access point (AP)** in a Wi-Fi network. It's essentially the **MAC address** (Media Access Control address) of the wireless radio in the AP.
In simple terms, the BSSID helps devices (like laptops or smartphones) identify and connect to a specific AP within a network, especially when there are multiple APs broadcasting the same network name (SSID).

Remember, the **BSSID** is the MAC address of **Access Point** that your laptop connects to. Not your laptop's MAC address.

Example Scenario:

1. You're in a university library where the network name (SSID) is CampusWiFi.
2. There are multiple **access points** in different parts of the library.
3. Each **AP** broadcasts the same SSID (CampusWiFi), but each has a unique **BSSID** (e.g., AA:BB:CC:DD:EE:01, AA:BB:CC:DD:EE:02, etc.).
4. Your device connects to the nearest AP by using its **BSSID**.

An **access point** can establish a **wireless-only network**, but it can also work as a **bridge** to forward communications between the wireless stations and a wired network. The wired network is referred to as the "**distribution system**" (DS). The access point will be joined to the network in much the same way as a host computer is—via a **wall port** and **cabling** to an **Ethernet switch**. An enterprise network is likely to use **Power over Ethernet (PoE)** to power the AP over the data cabling. PoE means a technology that allows both **power** and **data** to be transmitted over a single Ethernet cable. This simplifies device installations and reduces the need for separate power supplies.

How Does PoE Work?

- In a PoE setup, a network cable (like Cat5e or Cat6) carries:
    1. **Electrical Power** to power devices like access points or IP cameras.
    2. **Data** for network connectivity.
- This is possible because Ethernet cables have multiple wires, and some are used to deliver power while others handle data transmission.

802.11A and the 5GHz Frequency Band:

Frequency Band can be defined as the overall range of the radio waves that can be used by Wi-Fi devices to communicate. Like if you have the Wi-Fi, router the range upto which you can connect to the router, is the frequency band. So, every Wi-Fi devices operates on a specific radio frequency range within an **overall frequency band.** There is major two **frequency bands.**

1. **2.4 GHz band**
   - This is like an "old, busy street." It's used by many devices like older Wi-Fi routers, Bluetooth devices, baby monitors, and even microwaves. So, we can say this band is more crowded and used by many devices beyond just Wi-Fi. If you are using Wi-Fi and someone turns on the microwave, then it can disrupt your internet connection briefly because the microwave emits signals in the 2.4GHz range as well.

   - It is better at propagating through solid surfaces, giving it the longest range. The **2.4 GHz signals travel farther** and penetrate walls better than the 5 GHz signals. While this is good for range, it also means your Wi-Fi can pick up interference from more distant devices, like a neighbor's router.

   - It has a longer range but lower speeds than 5GHz band. The nominal range is 50m (150 feet).
2. **5 GHz band**
   - This is like a "new, faster highway." It's less crowded, allowing faster speeds, but has a shorter range. Th**e 5 GHz standard** is less effective at penetrating solid surfaces and so does not support the maximum ranges achieved with **2.4 GHz standards**, but the band supports more individual channels and suffers less from **congestion** and **interference**, meaning it supports **higher data rates** at **shorter ranges**.
   - Modern devices (like smartphones, laptops, and gaming consoles) often prefer 5 GHz for better performance.
   - The nominal range is 30m (100feet).

Channels in Each Band:

A channel is a smaller range of frequencies within the frequency band that Wi-Fi uses to transmit data. So, since frequency bands have 2 ranges, the channel between these bands are also two types:

1. **2.4 GHz Band Channels**:
   - There are **14 channels** in this band (depending on the country), but only **3 non-overlapping channels** (1, 6, and 11) can be used at the same time without interfering with each other.
   - Example: If you and your neighbors all use channel 6, it's like driving in the same lane during rush hour—there's a traffic jam. But if you switch to channel 1 or 11, it's like moving to a free lane.
2. **5 GHz Band Channels**:
   - This band has **more channels** (around 23 non-overlapping ones), so devices can avoid interference more easily.
   - Example: It's like a highway with many open lanes—more room, less congestion.

IEE 802.11a and 5GHz Channel Layout:

802.11a is one of the original Wi-Fi standards introduced along with **802.11b.** It operates exclusively in the **5GHz frequency band** which differs from **802.11b** which operates at **2.4GHz frequency band**. It offers faster speeds compared to 802.11b but has a shorter range due to the higher frequency.

"Data Encoding" means how Wi-Fi converts digital data into radio signals for transmission. In **802.11a** standards, this encoding allows a theoretical maximum speed of **54Mbps.**
The 5 GHz band is divided into **smaller chunks** of frequencies called **channels**: each **20 MHz** wide. Devices connect to one channel at a time to send and receive data. In the 5 GHz band, you can have **23 separate channels** operating without interference. This is much better than the 2.4 GHz band, which only has **3 non-overlapping channels**.

A **non-overlapping channel** means that the signals transmitted on that channel **do not interfere** with signals on other channels. This is crucial for reducing interference and ensuring smooth Wi-Fi performance.
What Does "Overlapping" Mean?

- **Overlapping Channels**:
  Channels that share parts of their frequency range can "interfere" with each other, causing slower speeds and connection issues.

Example (2.4 GHz Band):

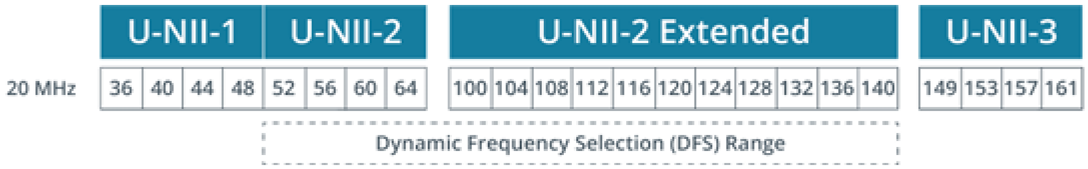
  - Channel 1: 2401 MHz to 2423 MHz.
  - Channel 2: 2406 MHz to 2428 MHz.
  - These channels overlap because they share the same frequency range (2406 MHz to 2423 MHz), which can create interference.

- **Non-Overlapping Channels**:
  Channels that don't share any part of their frequency range. These channels can operate simultaneously without interfering.

Example (2.4 GHz Band):

  - Channel 1: 2401 MHz to 2423 MHz.
  - Channel 6: 2431 MHz to 2453 MHz.
  - Channel 11: 2456 MHz to 2478 MHz.
  - These channels don't overlap, so they avoid interference.

Devices operating in the 5 GHz band must implement **dynamic frequency selection (DFS)** to prevent Wi-Fi signals from interfering with nearby radar and satellite installations.



Unlicensed National Information Infrastructure (U-NII) sub-bands form the 20 MHz channels used in the 5 GHz frequency band. Each sub-band is 5 MHz wide, so the Wi-Fi channels are spaced in intervals of four to allow 20 MHz bandwidth. Channels within the DFS range will be disabled if the access point detects radar signals.

Let's discuss the above image back-end informations. This is not necessary for the exam. But learn this to know the concepts:

1. What Are U-NII Bands?

The 5 GHz band is split into **four sections**, called **U-NII bands** (Unlicensed National Information Infrastructure). Each section has different rules. Think of these as parts of the road with different speed limits or restrictions.

- **U-NII-1**: Channels **36, 40, 44, 48**.
    - Open for Wi-Fi use. No special rules.
    - Commonly used at home.
- **U-NII-2**: Channels **52, 56, 60, 64**.
    - Needs **special permission** because these lanes are shared with radar (e.g., weather radar).
- **U-NII-2 Extended**: Channels **100 to 140**.
    - Same as U-NII-2. Shared with radar, so it needs special checks.
- **U-NII-3**: Channels **149, 153, 157, 161**.
    - Open for Wi-Fi use. No special rules.
    - Commonly used at home.

---

2. What is a Channel?

A **channel** is a small slice of the 5 GHz band where Wi-Fi devices can send and receive data.

- Think of channels as **lanes on a highway**.
- Devices use these lanes to avoid colliding with others on the same road.

---

3. What is DFS (Dynamic Frequency Selection)?

Some lanes (channels) are **shared with radars**, like the kind used by weather stations or airports. Wi-Fi must be careful not to interfere with them.

- **DFS is like a traffic cop**:
    - Your router listens to make sure radar isn't using the lane.
    - If radar is detected, your router **switches to another lane automatically**.
- **Why is this needed?**
    - To avoid interrupting important systems like radar or satellites.

Simple Real-Life Example:

1. **Home Wi-Fi Router**:
    - Your router is using channel **36 (U-NII-1)**. No radar here, so it works fine.
2. **Router on a DFS Channel** (e.g., Channel 100):
    - If radar is detected (e.g., at an airport), your router quickly **moves to a different channel** so it doesn't interfere with radar signals.

Why do the routers need to switch if the radar is detected?

Let's say you are streaming on Netflix on channel 100, and an airport near you starts operating on the same channel, then your router detects it and switches to the channel 36 (let's suppose). If the router is not configured to switch automatically when the airport starts on the same channel, then it is considered as illegal because airport needs the radar data like another plane is approaching in the same radar, then it is very important for the Airplane Controlling Station to know exactly which plane are in which radar, right now so that collision can be avoided. So, to prevent this from happening, the channel needs to be switched so that your router channel does not interfere with that radar.

802.11B and 802.11G and the 2.4 GHz frequency band:

802.11b is one of the earliest Wi-Fi standards, introduced in 1999. It offers a maximum speed of **up to 11 Mbps**, which is very slow by today's standards. This standard operates on the **2.4 GHz frequency band**, which allows for good range, meaning the signal can travel relatively far and penetrate walls. However, because it uses this crowded frequency, 802.11b is prone to interference from devices like cordless phones and microwaves, which can slow down the connection. 802.11b was widely used in its time but has mostly been replaced by faster and more efficient Wi-Fi standards.

The **2.4 GHz frequency band** is a commonly used radio wave range for Wi-Fi, Bluetooth, and other devices. It is popular because of its ability to travel farther and penetrate obstacles like walls, making it ideal for larger spaces or older buildings. However, the downside of 2.4 GHz is that it can become easily congested because many devices, including cordless phones, baby monitors, and microwaves, operate on the same frequency. This interference can cause slower speeds and disruptions. In simple terms, the 2.4 GHz band is like a crowded two-lane road that supports many vehicles (devices), which can result in traffic jams.

The 2.4 GHz band is subdivided into up to **14 channels**, spaced **at 5 MHz** intervals from **2,412 MHz** up **to 2,484 MHz.** Because the spacing is only 5 MHz and Wi-Fi needs 20 MHz channel bandwidth, 802.11b channels overlap quite considerably. This means that interference is a real possibility unless widely spaced channels are chosen (1, 6, and 11, for instance). Also, in the Americas, regulations permit the use of channels 1 11 only, while in Europe, channels 1–13 are permitted, and in Japan, all 14 channels are permitted.

802.11G frequency band:

802.11g was introduced in 2003 as a significant upgrade to 802.11b. It increased the maximum speed to **54 Mbps**, which is almost five times faster than 802.11b. Like 802.11b, it operates on the **2.4 GHz frequency band**, which provides good range but is susceptible to interference. A major benefit of 802.11g is that it is **backward compatible** with 802.11b, meaning older devices using 802.11b could still connect to an 802.11g router, although they would operate at the slower speed. This compatibility made **802.11g** a popular standard for several years before newer standards were developed.

Key Exam Points to Remember

1. **802.11b**: Operates at up to 11 Mbps and uses the 2.4 GHz frequency band.
2. **802.11g**: Operates at up to 54 Mbps, uses the 2.4 GHz band, and is backward compatible with 802.11b.
3. **2.4 GHz frequency band**: Offers longer range but suffers from interference and slower speeds compared to higher-frequency bands like 5 GHz. And has **14** lanes.
4. **Interference**: Devices such as microwaves, cordless phones, and baby monitors can disrupt Wi-Fi signals on the 2.4 GHz band.

802.11 N standard:

The **802.11n** also called **Wifi-4** standard was introduced in 2009 as a big improvement over earlier Wi-Fi standards like 802.11b and 802.11g. It is much faster, with speeds of up to **600 Mbps**, depending on the configuration. One of the main features of 802.11n is its ability to use both the **2.4 GHz** and **5 GHz frequency bands**, making it a **dual-band** standard. By using the less crowded 5 GHz band, 802.11n avoids much of the interference common with 2.4 GHz networks, while still maintaining compatibility with older devices on the 2.4 GHz band.

Another key improvement of 802.11n is the use of **MIMO** (**Multiple Input, Multiple Output)** technology. This means it can use multiple antennas to send and receive data, allowing for faster speeds, better reliability, and improved performance in environments with lots of obstacles or interference. MIMO also increases the range of

the network. For example, with 802.11n, you might get a stronger signal and better speeds even when you're farther away from the router compared to older standards.
In real-life terms, if you're streaming HD videos, downloading large files, or playing online games on a network with an 802.11n router, your experience will be much smoother and faster compared to networks using 802.11b or 802.11g. This standard laid the foundation for modern Wi-Fi and is still in use in many homes and businesses today.

Channel Bonding

One major improvement in 802.11n is channel bonding, which allows two smaller channels (20 MHz each) to combine into a larger 40 MHz channel. This increases bandwidth, making Wi-Fi faster. However, channel bonding works best on the 5 GHz band, because the 2.4 GHz band doesn't have enough room for multiple wide channels in areas with overlapping networks or devices. Think of it like doubling the width of a road—cars (data) can move faster, but it's only possible if there's enough space available. For instance, in a busy apartment building, 5 GHz is better suited for channel bonding since 2.4 GHz is already overcrowded.

One important limitation is that some 5 GHz channels are non-contiguous (not next to each other) or may be blocked if the router detects radar signals, such as those used by weather systems or airports. This can limit the effectiveness of channel bonding in some areas.

MIMO Technology

Another key innovation in 802.11n is **MIMO** (**Multiple Input, Multiple Output**). MIMO uses **multiple antennas** to send and receive more data streams at the same time, improving both speed and reliability. The configuration is represented as **1x1**, **2x2**, or **3x3**, where the first number is the number of transmitting antennas and the second is the number of receiving antennas. For example:

- A **2x2** configuration can send two data streams and receive two streams, doubling the performance compared to a single antenna setup.
- A **3x3** setup can go even faster by handling three streams simultaneously.

Speeds and Bandwidth

The **nominal data rate** of 802.11n depends on the configuration and channel width. Each MIMO stream supports **72 Mbps** on a 20 MHz channel or **150 Mbps** on a 40 MHz bonded channel. Routers and access points are often labeled with their maximum total speeds, such as **N300**, **N450**, or **N600**:

- **N300**: A 2x2 router using a 40 MHz channel can provide 300 Mbps (150 Mbps x 2 streams).
- **N600**: A dual-band router with 2x2 MIMO can offer 300 Mbps on both the 2.4 GHz and 5 GHz bands, adding up to 600 Mbps total bandwidth.

For example, if you have an N600 router at home, it can stream HD videos on multiple devices without lag, especially if your laptop and phone are connected to the 5 GHz band.

Real-Life Example

Imagine you're in a house with an 802.11n router. Your router supports dual-band operation, meaning it can use both 2.4 GHz and 5 GHz bands. Your older tablet connects to the 2.4 GHz band because it doesn't support 5 GHz, but your newer laptop connects to 5 GHz for faster speeds. If the router has **2x2 MIMO**, both devices can get stable connections without slowing each other down. Additionally, if you're streaming a movie on your laptop using a 40 MHz bonded channel on the 5 GHz band, the movie loads quickly and streams without buffering. Meanwhile, someone else in the house browsing the web on the 2.4 GHz band doesn't experience interference.

Key Exam Points to Remember

1. **Frequency Bands**: 802.11n works on both **2.4 GHz** and **5 GHz**, and dual-band devices can use both simultaneously.

2. **Channel Bonding**: Combines two 20 MHz channels into a single **40 MHz channel** for faster speeds, mainly effective on the **5 GHz band**.
3. **MIMO**: Uses multiple antennas (1x1, 2x2, or 3x3) to send and receive more data streams, increasing speed and reliability.
4. **Speeds**: Up to **600 Mbps** with 40 MHz channels and 4 MIMO streams.
5. **Router Labels**: Look for labels like **N300** or **N600**, where the number indicates total bandwidth across all streams and bands.

Wi-Fi 5 (802.11ac):

Wi-Fi 5, also known as **802.11ac**, was introduced in 2013 and is a major upgrade over Wi-Fi 4 (802.11n). It is designed to operate exclusively on the **5 GHz frequency band**, meaning it avoids the crowded **2.4 GHz** band that suffers from interference caused by other devices like cordless phones and microwaves. Because the 5 GHz band has more available channels and less interference, Wi-Fi 5 provides much faster speeds and better performance, especially in environments with many connected devices.

A big improvement in Wi-Fi 5 is the use of **channel bonding**, which combines channels into wider ones (up to 160 MHz) to carry more data at once, similar to turning a single-lane road into a multi-lane highway. It also introduces **MU-MIMO** (Multi-User Multiple Input, Multiple Output), which allows multiple devices to communicate with the router at the same time without slowing each other down. For example, in a busy household where one person is streaming 4K video, another is gaming online, and someone else is downloading large files, Wi-Fi 5 ensures that all these activities happen smoothly without interference.

Another innovation is **beamforming**, which focuses the Wi-Fi signal directly toward connected devices instead of broadcasting it equally in all directions. This results in a stronger and more reliable connection, especially for devices farther away from the router.

Wi-Fi 5 also supports incredibly high speeds. A single stream can handle up to **433 Mbps**, and with multiple streams and bonded channels, speeds can reach **1.3 Gbps or higher** on modern routers. For example, if you're using a Wi-Fi 5 router labeled **AC1750**, this means the router can handle up to **1,300 Mbps** on the 5 GHz band and **450 Mbps** on the 2.4 GHz band (some routers still include limited support for 2.4 GHz).

Key Features of Wi-Fi 5 (802.11ac)

1. **Operates on 5 GHz only**: Avoids interference from devices on 2.4 GHz.
2. **Speeds**: Up to **1.3 Gbps or higher**, depending on the number of streams and bonded channels.
3. **Channel bonding**: Combines channels to create wider ones (up to 160 MHz), allowing more data to pass through.
4. **MU-MIMO**: Supports multiple devices simultaneously without performance drops.
5. **Beamforming**: Directs Wi-Fi signals toward devices for stronger, more reliable connections.
6. **Backward compatibility**: Still works with devices that use older standards like Wi-Fi 4 (802.11n).

What to Remember for the Exam

1. **802.11ac = Wi-Fi 5.**
2. Operates only on the **5 GHz band**.
3. Introduced **MU-MIMO, beamforming,** and **channel bonding** for faster and more efficient communication.
4. Maximum theoretical speed: Over **1 Gbps**.
5. Suitable for streaming HD/4K, online gaming, and handling multiple devices efficiently.

Wi-Fi 6 (802.11ax):

Wi-Fi 6, also known as **802.11ax**, is the newest Wi-Fi standard, introduced in 2019. It builds on the foundation of Wi-Fi 5 (802.11ac) and is designed to handle the increasing number of devices in our homes and workplaces. Wi-Fi 6 works on **both the 2.4 GHz and 5 GHz bands**, making it more versatile than Wi-Fi 5, which only operates on the 5 GHz band. It also introduces several advanced technologies to make networks faster, more efficient, and better at handling many devices at the same time.

One of the biggest improvements in Wi-Fi 6 is its ability to handle congestion. In real life, think about a packed stadium, airport, or busy office building where hundreds of devices are competing for the same Wi-Fi. Older Wi-Fi standards struggle in these situations, but Wi-Fi 6 introduces a feature called **OFDMA** (Orthogonal Frequency Division Multiple Access). This breaks each Wi-Fi channel into smaller parts, allowing multiple devices to send and receive data simultaneously without waiting in line. It's like turning a single bus into multiple smaller shuttles, so everyone gets to their destination faster.

Wi-Fi 6 also includes **MU-MIMO (Multi-User, Multiple Input, Multiple Output)**, an upgraded version from Wi-Fi 5. It allows even more devices to connect and communicate at once. For example, in a smart home with dozens of devices—like smart lights, TVs, thermostats, and security cameras—Wi-Fi 6 ensures all devices stay connected without slowing down the network.

Another important feature is **Target Wake Time (TWT)**, which improves battery life for connected devices like smartphones and IoT gadgets. Wi-Fi 6 can schedule when devices "wake up" to send or receive data, so they use less power when they're idle. For example, a smart thermostat will only connect to the network when it needs to, conserving its battery.

Wi-Fi 6 also supports **higher speeds**. A single stream can handle up to **1.2 Gbps**, and with multiple streams and wider channels, total speeds can exceed **9.6 Gbps** in ideal conditions. While you may not need these speeds for most everyday tasks, they're great for demanding activities like 8K streaming, VR gaming, or transferring large files on a network.

Key Features of Wi-Fi 6 (802.11ax)

1. **Dual-band operation**: Works on both **2.4 GHz** and **5 GHz** bands.
2. **Faster speeds**: Theoretical speeds up to **9.6 Gbps**, though real-world speeds are usually much lower.
3. **OFDMA**: Allows multiple devices to communicate simultaneously, reducing congestion.
4. **Improved MU-MIMO**: Handles more devices at once, great for homes or offices with many connected gadgets.
5. **Target Wake Time (TWT)**: Saves battery life for connected devices by scheduling communication.
6. **Better range**: Improved signal efficiency allows for slightly better coverage compared to Wi-Fi 5.
7. **Backward compatibility**: Works with older Wi-Fi devices, though they won't benefit from Wi-Fi 6 features.

What to Remember for the Exam

1. **Wi-Fi 6 = 802.11ax.**
2. Operates on **2.4 GHz and 5 GHz** bands.
3. Improves congestion handling with **OFDMA** and upgraded **MU-MIMO**.
4. **Faster speeds**: Up to **9.6 Gbps** in ideal conditions.
5. Includes **Target Wake Time (TWT)** for better battery life in connected devices.
6. Designed for dense environments (homes, offices, airports, etc.) with many connected devices.

Wireless LAN Installation Considerations:

What is an SSID?

An **SSID (Service Set Identifier)** is the **name of a Wi-Fi network**. When you connect to a wireless network, the SSID is the name you see on the list of available Wi-Fi networks. It helps devices identify and connect to the correct network. For example, if your home Wi-Fi network is named "Home_Network," that's the SSID.

- **Length and Characters**: An SSID can be up to **32 characters long**. To avoid compatibility issues, it's best to use only **letters, numbers, hyphens (-), and underscores (_)** when naming your network. Avoid special characters like "@" or spaces.

Configuring an Access Point (AP)

When setting up a wireless access point (AP), you need to configure several options to optimize the network. Here's what you should know:

1. Single or Separate SSIDs for Each Band

Most modern access points support **dual-band operation** (2.4 GHz and 5 GHz). You have two choices when naming the network:

- **Same SSID for Both Bands**: If both bands share the same name, the router and device will work together to decide which band has the strongest signal and connect to it automatically. This is convenient but may not always pick the best band for speed.
- **Separate SSIDs for Each Band**: You can give each band a different SSID, like "Home_2.4GHz" and "Home_5GHz." This allows you to manually choose which band to connect to. For example, you might connect your phone to the 5 GHz band for faster speed, while your smart thermostat uses 2.4 GHz for better range.

2. Operation Mode

Each frequency band (2.4 GHz or 5 GHz) can be configured to support specific Wi-Fi standards (e.g., Wi-Fi 4, Wi-Fi 5, or Wi-Fi 6). This determines which devices can connect:

- **Legacy Support**: If you have older devices that only support 802.11b/g, you'll need to enable compatibility for those standards. However, supporting older standards can slow down the entire network. For example, if a very old laptop connects using 802.11b, the access point may operate at a lower speed for all devices on that band.
- **Modern Standards**: If all your devices support newer standards (like 802.11n or 802.11ac), you can set the AP to only allow those for better performance.

3. Channel and Channel Bonding

- **Channel Selection**: Wireless networks use specific channels to send and receive data. If you have multiple access points in the same area (like in a large office or apartment building), their channels should not overlap to avoid interference. For example, in the 2.4 GHz band, nonoverlapping channels are 1, 6, and 11.
- **Channel Bonding**: This combines two adjacent channels into one to create a wider channel (e.g., 40 MHz instead of 20 MHz). This allows for more bandwidth, meaning faster data transfer. However, channel bonding can cause more interference, especially in the crowded 2.4 GHz band. It's usually more practical in the 5 GHz band, where there are more channels available and less interference.

Wi-Fi Analyzers:

A **Wi-Fi analyzer** is a tool (either hardware or software) that helps you analyze and troubleshoot Wi-Fi networks. It shows you important details about nearby Wi-Fi networks, such as signal strength, channels in use, and sources of interference. Network technicians use Wi-Fi analyzers to optimize a wireless network's performance and resolve connectivity issues.

Think of a Wi-Fi analyzer like a "Wi-Fi traffic monitor." It gives you a detailed view of what's happening in your network and identifies any "traffic jams" (issues like overlapping channels, weak signals, or interference).

What Does a Wi-Fi Analyzer Do?

Here are some key functions of a Wi-Fi analyzer:

1. **Detect Nearby Networks**:
   A Wi-Fi analyzer can list all the Wi-Fi networks within range. For example, if you're in an apartment building, it will show the names (SSIDs) of your neighbors' networks.
2. **Measure Signal Strength**:
   It shows the signal strength of each network. For instance, if your home network has a weak signal in certain rooms, the analyzer will help you find the dead zones.
3. **Identify Channel Usage**:
   Wi-Fi analyzers display which channels are being used by nearby networks. If multiple networks are on the same channel, they can interfere with each other. For example, if your network is on channel 6 and your neighbors' networks are also on channel 6, you may experience slow speeds. The analyzer can help you find a less crowded channel.
4. **Detect Interference**:
   The tool can detect interference from other wireless devices (like baby monitors, cordless phones, or microwaves) that may affect your Wi-Fi performance.
5. **Optimize Network Performance**:
   By using the data provided by the analyzer, you can adjust your router's settings to improve performance. For example, you can switch to a less crowded channel or move the router to a better location.

Examples of Wi-Fi Analyzers

1. **Software-Based Wi-Fi Analyzers**:
   These are apps or programs you can install on a smartphone, tablet, or computer. Examples include:
   - **NetSpot** (Windows/macOS)
   - **Acrylic Wi-Fi Home** (Windows)
   - **Wi-Fi Analyzer** (Android)

For instance, using the **Wi-Fi Analyzer** app on your phone, you can see which channels are overcrowded and switch your router to a better one.

2. **Hardware Wi-Fi Analyzers**:
   These are specialized devices used by professionals. They provide advanced features like detecting hidden networks, signal heatmaps, and diagnosing complex interference issues. Tools like **Fluke Networks AirCheck** are examples of hardware analyzers.

Wi-Fi Signal strength is measured in decibels relative to **1 milliwatt (dBm).**

Decibels (dB) and Signal Strength

- **Signal strength** for Wi-Fi is measured in **decibels relative to 1 milliwatt (dBm)**.
- **Values closer to 0 are better.** For example:
  - **-30 dBm** = Very strong signal (great connection).
  - **-65 dBm** = Good signal (acceptable for most uses).
  - **-80 dBm or worse** = Weak signal (prone to packet loss or dropped connections).

Think of signal strength like hearing someone's voice:

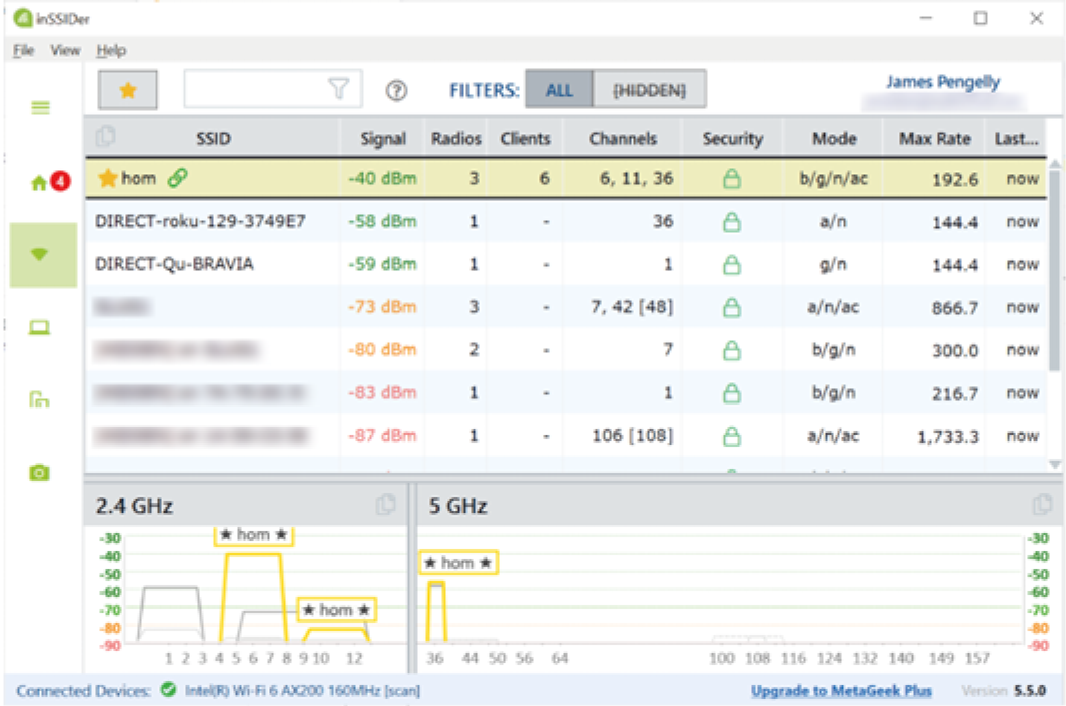
- A strong signal (-30 dBm) is like hearing someone speaking loudly next to you.
- A weak signal (-80 dBm) is like someone whispering from across a crowded room—it's harder to understand.

Signal-to-Noise Ratio (SNR)

- **SNR** compares the strength of the Wi-Fi signal to the background noise.
- A **higher SNR is better** because it means the signal is stronger relative to the noise.
    - Example: If the signal is **-65 dBm** and the noise is **-90 dBm**, the SNR is **25 dB**, which is good.
    - If the noise rises to **-80 dBm**, the SNR drops to **15 dB**, and the connection will degrade significantly.

Imagine listening to music:

- A high SNR (strong signal, low noise) is like listening to music in a quiet room.
- A low SNR (weak signal, high noise) is like trying to listen to music in a noisy crowd—hard to enjoy, and you might miss parts.



SSID	Signal	Radios	Clients	Channels	Security	Mode	Max Rate	Last...
★ hom	-40 dBm	3	6	6, 11, 36	🔒	b/g/n/ac	192.6	now
DIRECT-roku-129-3749E7	-58 dBm	1	-	36	🔒	a/n	144.4	now
DIRECT-Qu-BRAVIA	-59 dBm	1	-	1	🔒	g/n	144.4	now
[redacted]	-73 dBm	3	-	7, 42 [48]	🔒	a/n/ac	866.7	now
[redacted]	-80 dBm	2	-	7	🔒	b/g/n	300.0	now
[redacted]	-83 dBm	1	-	1	🔒	b/g/n	216.7	now
[redacted]	-87 dBm	1	-	106 [108]	🔒	a/n/ac	1,733.3	now

Metageek inSSIDer Wi-Fi analyzer software showing nearby access points. (MetaGeek, LLC. © Copyright 2005-2021)

Long-Range Fixed Wireless:

Long-Range Fixed Wireless is a type of wireless communication used to provide high-speed internet or network connectivity over long distances without using cables. It is called "fixed" because the antennas or devices used for the connection are installed at **fixed locations**, such as on rooftops, towers, or poles, rather than being mobile like a smartphone or laptop.

How It Works

1. **Transmitter and Receiver**: A central antenna (transmitter) broadcasts a wireless signal to one or more receiving antennas at remote locations.
2. **Line-of-Sight Communication**: Long-range fixed wireless often requires **line of sight**, meaning there must be a clear, unobstructed path between the antennas (no buildings, trees, or hills in the way).
3. **Frequency Bands**: It typically operates on licensed or unlicensed frequencies in the **microwave** (GHz) spectrum. For example, **2.4 GHz** and **5 GHz** bands may be used, along with higher frequencies like 24 GHz for even longer ranges.
4. **Range**: Depending on the setup and frequency, it can cover distances of **several miles**, making it ideal for rural areas or locations where laying cables isn't practical.

Advantages

- **Cost-Effective**: Cheaper than laying fiber optic cables over long distances.

- **Quick Deployment**: Faster to set up compared to physical infrastructure like cables.
- **Reliable**: Can provide stable connections in areas where traditional wired connections are unavailable.

Disadvantages

- **Line of Sight Requirement**: Physical obstacles (trees, hills, buildings) can block or weaken the signal.
- **Interference**: Subject to weather interference (e.g., heavy rain) or congestion on unlicensed frequencies.
- **Limited Bandwidth**: While adequate for many applications, it may not match the speeds of fiber-optic networks.

Personal Area Networking:

Bluetooth:

Bluetooth is a short-range wireless technology that allows devices to communicate with each other. It's commonly used for transferring data, connecting peripherals, or streaming audio between devices without cables. Bluetooth works over distances of about **10 meters (33 feet)**, though newer versions can extend this range upto **(100 feet)**.

Bluetooth is ideal for **personal area networks (PANs)**—small networks that connect nearby devices, like your phone and wireless headphones. Bluetooth operates in the **2.4 GHz frequency band**, the same range used by Wi-Fi. However, it uses a method called **frequency hopping** to avoid interference. This means it changes its frequency up to 1,600 times per second while transmitting. Devices must go through a pairing process to establish a secure connection. Once paired, they remember each other and reconnect automatically when in range. **Bluetooth 4.0 (Bluetooth Low Energy, BLE)**: Introduced **low-power** operation, ideal for devices like fitness trackers and smartwatches.

Radio Frequency Identification:

RFID (Radio Frequency Identification) is a wireless technology that uses radio waves to identify and track objects, animals, or people. It works by sending data between an **RFID tag** (attached to the object) and an **RFID reader** (which scans the tag). RFID is commonly used for tracking, access control, and inventory management.

The tag contains a tiny microchip and antenna. It stores information, like a product ID, serial number, or other data.

RFID tags can be:

- **Passive**: Powered by the energy from the reader's signal (no battery).
- **Active**: Have their own battery for a longer range.

The reader sends out a signal that powers up the tag (for passive tags) and reads the data stored on it. The tag sends the stored data back to the reader, which processes the information and sends it to a computer system. It is commonly used in Inventory Management, Access Control, Payment Systems, Animal Tracking, Supply Chain, etc.

Near Field Communications:

Near Field Communication (NFC) is a short-range wireless technology that allows devices to communicate when they are very close to each other—typically within **4 centimeters (about 2 inches)**. It's commonly used for contactless payments, data sharing, and pairing devices.

Think of NFC as a specialized version of RFID designed for very close-range communication.

NFC allows two devices to exchange information when they are brought close together. For example, a smartphone and a payment terminal can communicate to complete a transaction.

Some Questions and Answers:

You are assessing standards compatibility for a Wi-Fi network. Most employees have mobile devices with single-band 2.4 GHz radios. Which Wi-Fi standards work in this band?

Wi-Fi 6 (802.11ax), Wi-Fi 4 (802.11n), and the legacy standards 802.11g and 802.11b.

You are explaining your plan to use the 5 GHz band predominantly for an open plan office network. The business owner has heard that this is shorter range, so what are its advantages over the 2.4 GHz band?

Each numbered channel in a 2.4 GHz network is only 5 MHz wide, while Wi-Fi requires about 20 MHz. Consequently, there is not much space for separate networks, and the chances of overlap are high. Numerous other product types of work in the 2.4 GHz band, increasing the risk of interference. Using 5 GHz will present a better opportunity to use channel bonding to increase bandwidth. As an open plan office does not have solid walls or other building features to block signals, the slightly reduced range of 5 GHz signaling should not be a significant drawback.

Can 802.11ac achieve a higher throughput to a single client by multiplexing the signals from both 2.4 and 5 GHz frequency bands? Why or why not?

No. First, a client can only use one radio at a time and so cannot connect simultaneously to the 2.4 GHZ and 5 GHz bands. Secondly, 802.11ac works only at 5 GHz; 802.11ac access points use the 2.4 GHz band to support 802.11b/g/n clients. The 802.11ac standard can increase bandwidth by using multiple input output (MIMO) antenna configurations to allocate more streams, such as 2x2 or 3x3.

You are setting up a Wi-Fi network. Do you need to configure the BSSID?

No. You need to configure the service set identifier (SSID), unless you want to rely on the default value. The SSID is a name for users to recognize the network by. The basic SSID (BSSID) is the MAC address of the access point's radio. As this is coded into the device firmware, it does not need to be configured. Stations use the BSSID to send frames to the access point.

True or false? Only a single network name can be configured on a single access point.

False. Each band can be assigned a different service set identifier (SSID) or network name. Access points also allow the configuration of multiple SSIDs per radio, such as configuring a secure network for known clients and an open network for guests.

True or false? A long-range fixed wireless installation operating without a license is always illegal.

False. These installations may use unlicensed spectrum but must not exceed the effective isotropic radiated power (EIRP) defined for the frequency band by regulations.