# Introduction

A company has asked you to evaluate their simple Wi-Fi setup so they can implement any of the recommendations that you make.

# Purpose

This assignment is designed to test your understanding of where the Wi-Fi settings can be located on a router.

# Resources

* Access to LinkedIn Learning

# Tasks

View the following LinkedIn Learning course:  
<https://www.linkedin.com/learning/wireless-networking-essential-training>

# Complete the quizzes as part of the LinkedIn Learning course.

# Deliverables

Upload the certificate from this LinkedIn course into Brightspace.

**Transcript :**

### **Ad hoc wireless LAN**

- [Narrator] When we connect to a wireless network, we typically think of looking for available wireless networks, connecting to one, maybe we provide some login credentials, and only then do we communicate with other devices on the network. However, there's an option to have an ad hoc wireless network. **With this type of network, we don't need any wireless infrastructure devices such as wireless access points**. **Instead, we've got two devices that communicate directly between themselves**. Now, *this type of network doesn't scale very well, it wouldn't be suitable as your primary type of wireless network for a business or really even a home, but it is very convenient for the occasional file transfer between devices*. A common example of an a**d hoc wireless LAN is Apple's AirDrop** feature between a couple of iPhones. We could have a couple of iPhones not connected to any sort of network infrastructure and they could directly exchange files like photos or videos, and this transfer is made without the need, again, for any sort of wireless access point, we're just using Bluetooth or Wi-Fi communication to talk directly between two different devices.

Adhoc :

No need for Wireless Infrastructure

Great for file transfers

Uses Bluetooth or WIFI

Example : Airdrop

**Infrastructure Wireless LAN :**

### Infrastructure wireless LAN

- [Instructor] The most common type of wireless LAN that we have is an **infrastructure wireless LAN**. Here, our wireless clients, like laptops or smartphones, they connect to wireless access points, and those **access points, they have a hardwired connection to the rest of the network**. And this type of network is also *very scalable*. **If we want to support additional wireless clients, we can simply add additional access points**, or if we want to extend the coverage area throughout a large building, **we could strategically place wireless access points throughout a building**. *That would allow us to roam with our wireless device around the building and seamlessly attach and communicate with the wireless access point that was closest to us at any moment*. And beyond the scalability of an infrastructure wireless LAN, these types of networks also give us additional management and monitoring features that we don't have with ad hoc wireless networks. For example, we could see the number of wireless clients currently attached to the network. We could check abate with utilization, and as another example, we could configure security features.

Wireless Clients connect to access points

Access point hardwired to the network (LAN)

Scalable by adding new access points

We can strategically place wireless access points through the building

**Mesh Access Points :**

Does not have to be connected via LAN

Flexibility

Retrasmits signalAutonomous Access Points :

Managed individually

Not centrally administered

Bad for scalaing

Lightweight Access Point :

Administration from one page

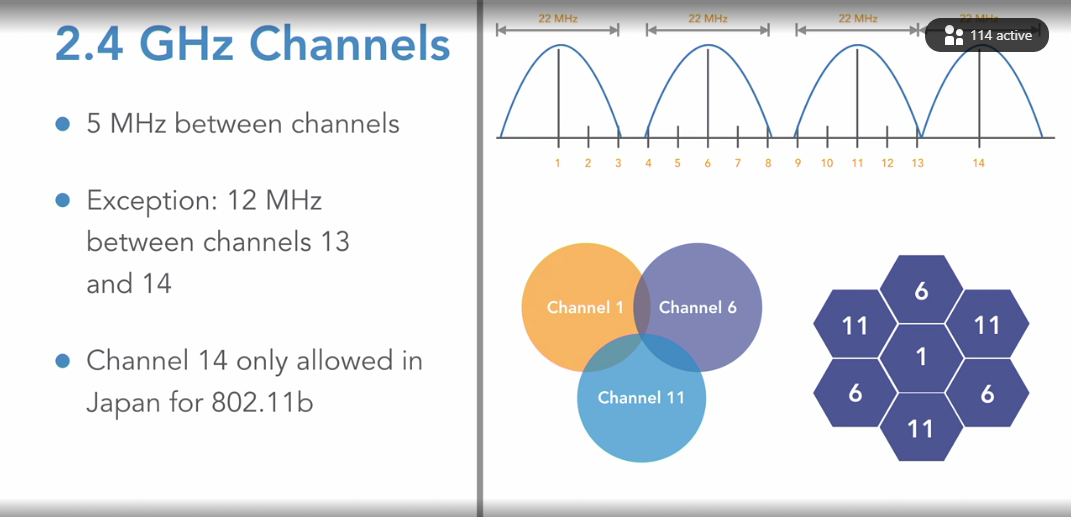
**Mesh wireless LAN**

- [Instructor] We know that we can extend the coverage of our wireless network by adding access points. However, **with our traditional infrastructural wireless LAN, those access points are hardwired into our network.** **And that's going to create a challenge for us if we need wireless coverage in an area that's not in close proximity to an ethernet switch into which we're going to be connecting our wireless access point.** Fortunately, we've got the option of using **mesh access points**. **This type of access point does not need to be connected into the wired infrastructure.** **As long as the mesh access point has power, it can receive signals from one access point, maybe back in the main building, and then regenerate, retransmit that wireless signal**. That's going to give us a lot of flexibility when it comes to access point placement. For example, let's say that we want to extend our wireless network into our company's parking lot, and there's a security guard letting people into the parking lot, so if they're there, then they deserve to be there, and **we want to extend wireless coverage to that parking lot. Well, what we could do is place an access point on the guard shack.** Assuming that we have power to the guard shack, but no ethernet connection, that would allow the access point on the guard shack to receive wireless communication from the main building and then retransmit that, covering up the parking lot area.

**Autonomous vs. Lightweight Access Points**

- [Instructor] Wireless access points can be managed in a couple of different ways. Specifically, we can have **autonomous APs,** or **lightweight AP**s. First, let's consider the **autonomous access points. Here, each access point is managed individually**. *They have no direct knowledge of one another*, *they're not centrally administered*. And that might be fine for a very small installation, but it's not going to scale well. As a second option, we can have **lightweight APs**. Here,**a wireless LAN controller lets us administer all of the APs from a single interface**. **And if we go with this lightweight AP option, there are a couple of protocols that you might run into that are used to communicate between the wireless LAN controller and the AP**s. **The first protocol is LWAPP**. That stands for **Lightweight Access Point Protocol**. However, that's an older protocol, it's becoming less popular in favor of **CAPWAP. That stands for Control and Provisioning of Wireless Access Points.** And when you're deciding on which option to go with, you should consider the cost of purchasing a wireless LAN controller against the convenience of having a single point of administration.

**2.4 GHz channels**

- [Instructor] Wireless LANs typically use radio frequencies in one of two bands. **There's the 2.4 gigahertz band** and the **five gigahertz band**. In this video, let's consider the **2.4 gigahertz band. This band of frequencies is divided into different channels and we have five megahertz of bandwidth between each of those channels**, with ***one exception***. ***The exception is there's actually 12 megahertz of bandwidth between channel 13 and 14.*** However, **channel 14 is only allowed in Japan and then it's only allowed when you're using the very old, 802.11b wireless standard**, **so you'll probably not ever encounter a wireless network using channel 14.** ***But a big design consideration we have is preventing wireless access points from interfering with one another. To do that, we assign nearby access points to different channels. But there's a big point of confusion here, if you tell one access point to use channel one and another access point to use channel two, thinking that by using different channels you're preventing interference, that's not going to work***. **When we tell an access point to use a specific channel that channel frequency is the *center frequency* being used by the access point**, **but that access point is going to use 22 megahertz of bandwidth for transmitting and receiving on that channel**, **and even though we might be centered on channel six, as you can see on screen, the frequencies actually span other channels. To really have non-interfering channels we need** ***at least five channels of separation***. **And if we start with channel one, that means we could have channels one, six, and 11 that don't overlap**. ***And if we want to have lots of access points, to cover a large area within a building, we could position our access points so that the coverage area of one access point is bounded by the coverage area of another access point with a non-overlapping frequency***. *Consider a honeycomb design.* **Here we're starting with an access point, running on channel one**. **Its coverage area is bounded at the top by another access point who's using channel six**. **At the bottom we've got an access point, using channel 11, but if wanted to expand even further, in that region between the access points using channels one and six,** ***we could put in access points using channel 11***, ***and between the areas where we're using channels one and 11***, ***we could insert access points using channel six.* And we could continue this pattern indefinitely**. This would allow us to have a very large coverage area while avoiding channel interference.

**5 GHz channels**

Selecting transcript lines in this section will navigate to timestamp in the video

- In addition to the 2.4 ghz frequency band, another popular band of frequencies that are commonly used in a Wifi networks is the 5 ghz frequency band. And the good news is, the 5 ghz frequency band is not nearly as congested as our 2.4 ghz band. Instead of having only three non overlapping channels, we said we could have channels one, six, and eleven that did not overlap with the 2.4 ghz band. Instead of just having those three non overlapping channels, with the 5 ghz band we have lots of channels. In fact, we have over 29 overlapping channels. In here, I'm running a wifi analyzer on my computer and it's showing the channels that are being used by some access points in my network. Now something that's not obvious, is the way the channels are numbered. Notice down here, it looks like we're jumping from channel 36, directly to channel 40. It looks like we're skipping channels 37, 38, and 39 but, interestingly that's just the way the usable channels are sequentially numbered. We cannot send an access point to operate, for example on channel 37. So even though it looks like we're skipping numbers, these are really consecutive channel numbers. And normally, I'll tell my access point to choose aon its own in appropriate channel. So normally I don't have to do anything, it's going to listen to neighboring access points, and it's going to try to avoid overlapping frequencies. And even though I said that we have non overlapping channels here in the 5 ghz band, that's only if we're using 20 Mhz channels widths. Here, if you take a look at one of my access points, I'm using an 80 Mhz channel width. So in this case, I actually am spanning a few different channels. So if you're statically configuring your channels on the 5 ghz band, remember that one channel is not going to bleed into another, like we did with the 2.4 ghz band, but that's only guarantee that if you're using the 20 MHz channel width. If you start using a larger channel widths, like 40 Mhz, 80 Mhz, or even now 160 Mhz, you need to keep that in mind and spread your channels a little further apart to avoid them still bleeding from one into the other.



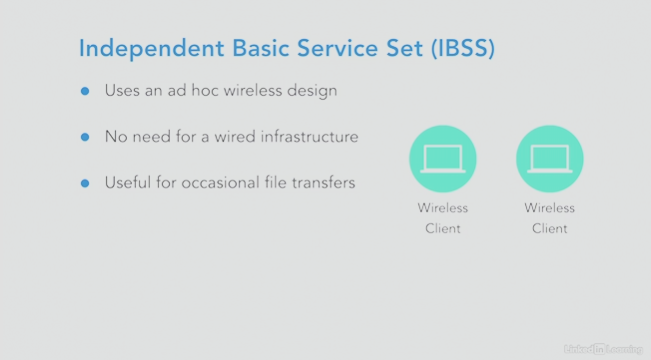
The 5GHz band is categorized into four divisions with at least four channels. They are,

1. **U-NII 1** – *36, 40, 44, 48*
2. **U-NII 2a** – *52, 56, 60, 64*
3. **U-NII 2c** – *100, 104, 108, 112, 116, 120, 124, 128, 132, 126, 140, 144*
4. **U-NII 3** – *149, 153, 157, 161, 165*

Independent Basic Service Set (IBSS)

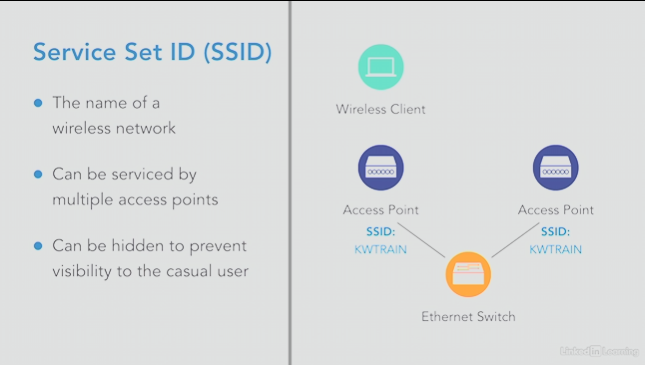
Selecting transcript lines in this section will navigate to timestamp in the video

- [Instructor] When we're on a wireless client, and we're looking at the list of wireless networks that we can join, we often say that those names that are showing up are the different SSIDs of the wireless networks. SSID, that stands for **Service Set identifier** , but we have some other service set terms that we need to know. And in this video we want to focus on the **Independent Basic Service Set**, or **IBSS**. Notice this term does not include ID because we're really not identifying anything. This is actually another way of describing the ad hoc wireless network that we discussed in a previous video where we have a direct connection between a couple of wireless devices, there's no need for a wired infrastructure. And a typical example of this would be when we want to send a file directly from one wireless client to another.



Service Set ID (SSID)

- [Instructor] Much more common than an independent service set, we have a wireless client communicating with a wireless access point. And joining a wireless network with a specific name. For example, here we have an SSID of KW train. That's the name of the network. That's the name of the wireless LAN. And our wireless client is going to talk with that access point. And when a client connects to an SSID, there are some other parameters that get exchanged beyond just hey, here's the name of the network. There's also going to be information about the type of security being used on the wireless LAN. And maybe we have quality of service settings that would be communicated as well. And one of the great things about a wireless network is that our clients can roam, they can go from one area of a building to another area of a building and attach to a nearby access point. And that's possible while staying on the same wireless network. In this case, we have a couple of access points that are both advertising at KW train as the SSID. That means that our wireless laptop could roam from one area of a building to another area of a building and connect to the nearest access point advertising kW train. And sometimes for security reasons, a network administrator will instruct a wireless access point not to advertise the SSID thinking that if a malicious user were trying to gain unauthorized access to the network, they wouldn't even know about this wireless network if they didn't see the advertised SSID. However, that only improves security just a bit because a knowledgeable user could do a packet capture of wireless traffic and they could see the SSID inside some of those frames. So that can give us a little bit of extra security. But in general, we need to turn to other security features, to better protect our wireless networks.



**Independent Basic Service Set (IBSS)**

Selecting transcript lines in this section will navigate to timestamp in the video

- [Instructor] When we're on a wireless client, and we're looking at the list of wireless networks that we can join, we often say that those names that are showing up are the different SSIDs of the wireless networks. **SSID, that stands for service set identifier**, but we have some other service set terms that we need to know. And in this video we want to focus on **the independent basic service set,** or IBSS. Notice this term does not include ID because we're really not identifying anything. This is actually another way of describing the ad hoc wireless network that we discussed in a previous video where we have a direct connection between a couple of wireless devices, there's no need for a wired infrastructure. And a typical example of this would be when we want to send a file directly from one wireless client to another.

A screenshot of a service set

Description automatically generated

From AI :

Independent Basic Service Set (IBSS) is a type of wireless network configuration that allows devices to communicate directly with each other without the need for a central access point (AP). This setup is also known as an ad hoc network.

**How IBSS Works**

*Peer-to-Peer Communication*: In an IBSS, devices (or stations) connect directly to each other. One device starts the network by advertising an SSID (Service Set Identifier), and other devices can join this network.

*No Central Infrastructure*: Unlike traditional networks that rely on a central AP to manage communication, IBSS networks are self-contained. This means there’s no need for additional hardware or infrastructure.

*Direct Data Transfer*: Data frames and traffic flow directly between devices, which can filter and process the data based on the MAC address of the receiver12.

**Applications of IBSS**

*Small Offices*: Ideal for small office environments where internet access isn’t required for communication.

*Temporary Networks*: Useful in situations where a quick, temporary network is needed, such as at conferences, meetings, or events.

*Remote Locations*: Suitable for areas without existing wireless infrastructure, like remote sites or temporary setups in places like airports or hotels.

**Advantages**

*Easy Setup*: Quick and simple to set up without needing any additional infrastructure.

*Cost-Effective*: No need for extra hardware like routers or access points.

*Mobility*: Devices can move freely within the network’s range without losing connectivity12.

**Disadvantages**

Limited Range: Typically covers a smaller area compared to networks with central APs.

Lower Flexibility: Not suitable for large networks or environments requiring extensive coverage12.

**Service Set ID (SSID)**

Selecting transcript lines in this section will navigate to timestamp in the video

- [Instructor] Much more common than an independent service set**, we have a wireless client communicating with a wireless access point**. And joining a wireless network with a specific name. For example, here we have an SSID of *KW train*. **That's the name of the network**. That's the name of the wireless LAN. And our wireless client is going to talk with that access point. **And when a client connects to an SSID, there are some other parameters that get exchanged beyond just hey, here's the name of the network. There's also going to be information about the type of security being used on the wireless LAN**. And maybe **we have quality of service settings that would be communicated as well**. And one of the great things about a wireless network is that **our clients can roam, they can go from one area of a building to another area of a building and attach to a nearby access point**. And that's possible while staying on the same wireless network. In this case, **we have a couple of access points that are both advertising at KW train as the SSID**. That means that our wireless laptop could roam from one area of a building to another area of a building and connect to the nearest access point advertising kW train. **And sometimes for security reasons, a network administrator will instruct a wireless access point *not to* advertise the SSID thinking that if a malicious user were trying to gain unauthorized access to the network, they wouldn't even know about this wireless network if they didn't see the advertised SSID**. However, **that only improves security just a bit because a knowledgeable user could do a packet capture of wireless traffic and they could see the SSID inside some of those frames**. So that can give us a little bit of extra security. But in general, we need to turn to other security features, to better protect our wireless networks. A close-up of a computer

Description automatically generated

Basic Service Set ID (BSSID)

Selecting transcript lines in this section will navigate to timestamp in the video

- [Instructor] We know that **we can have multiple access points servicing the same wireless LAN with the same name**. In other words, the same SSID. However, **these different access points each have unique MAC addresses that are associated with that SSID**. **This MAC address is called the basic service set identifier,** or **BSSID**. Now in this example on screen, **the access point on the left has an all ones MAC address corresponding to the SSID of KWTRAIN**. **And the access point on the right, it's got the all twos MAC address,** ***corresponding to the same SSID of KWTRAIN***. **And since the access points have unique MAC addresses for the same SSID, our wireless clients can communicate with a specific access point*, rather than just communicating with any access point that happens to answer to a specific SSID***. **This is going to allow our wireless clients to roam between access points. For example, as a wireless client roams from access point one to access point two as an example, the signal strength of access point two gets stronger as the wireless client approaches it. The wireless client can then start communicating with the MAC address. Again, that's the BSSID of access point two**. This allows the client to stay on the same wireless network, while communicating with the best access point relative to the wireless client's location at the moment.

A screenshot of a computer

Description automatically generated

**Extended Service Set ID (ESSID)**

Selecting transcript lines in this section will navigate to timestamp in the video

- [Instructor] Earlier, we said that a **basic service set** **represented the MAC address of an access point**. We also mentioned that **we could have multiple access points servicing a single wireless network**, and **if we took all of those basic service sets as a whole**, **which made up a single wireless network**, we would refer to that as an **extended service set ID, or an ESSID,** and if that sounds a lot like the definition of an SSID, just regular service set ID, it is. In fact, the term ESSID can be used interchangeably with SSID. However, in common practice, the term SSID is used a lot more frequently, so while SSID is definitely a term I want you to know, I also want you to know that it's just another way of saying the same thing. It's another way of expressing an SSID.  
A screen shot of a computer

Description automatically generated

**From AI :**

Service Set Identifier (SSID)

Definition: An SSID is a unique identifier (usually a string of characters) assigned to a specific wireless network. It is used by devices to identify and connect to a particular network.

Usage: When you connect to a Wi-Fi network, your device scans for available SSIDs to find and join the desired network. The SSID can be broadcast by the network's access point so that devices within range can see and connect to it.

Scope: The SSID is generally associated with a single access point or a basic Service Set (BSS). A BSS is the basic building block of a wireless network, consisting of a single access point and its associated clients.

Extended Service Set Identifier (ESSID)

Definition: The ESSID is essentially an SSID that is used in the context of an Extended Service Set (ESS). An ESS is a network configuration that includes multiple access points (APs) working together to provide seamless wireless coverage over a larger area.

Usage: In an ESS, all the access points share the same ESSID so that devices can move between different access points without losing their connection. The ESSID helps devices to stay connected as they roam across different parts of the network.

Scope: The ESSID applies to an entire Extended Service Set, which is a network made up of multiple BSSs. Each BSS in an ESS shares the same ESSID, allowing for a more extensive and contiguous wireless network.

Differences Between SSID and ESSID

Scope:

SSID: Refers to a single BSS. In simple terms, it's used for a single access point's network.

ESSID: Refers to a collection of BSSs that form an ESS. It is used for a network with multiple access points providing coverage over a larger area.

Network Size:

SSID: Typically associated with smaller or simpler networks with only one access point.

ESSID: Associated with larger, more complex networks where multiple access points work together to provide seamless coverage.

Network Roaming:

SSID: Roaming between different SSIDs (i.e., different networks) generally involves disconnection and reconnection.

ESSID: Allows for smooth roaming between access points within the same network, as all access points broadcast the same ESSID.

Practical Example

Imagine a large office building with Wi-Fi coverage on multiple floors. Each floor has its own access point. If all these access points are configured to use the same ESSID, employees can move around the building with their devices without needing to reconnect to different networks. They just stay connected to the same ESSID, and the network takes care of switching between access points as needed.

In summary, while the terms SSID and ESSID can sometimes be used interchangeably, the ESSID typically refers to the identifier used in a network with multiple access points, allowing for larger and more flexible wireless coverage.

**Multiple Basic Service Set ID (MBSSID)**

Selecting transcript lines in this section will navigate to timestamp in the video

- [Instructor] An access point has the ability to advertise more than one SSID. For example, **on screen we have each access point advertising both a KWTRAIN SSID, in addition to a KWGUEST SSID**. And as we mentioned earlier**, a wireless access point can roam around a building and connect to an appropriate access point, while remaining on the same wireless network. And that was possible because each access point had a unique MAC address corresponding to a wireless network**. And **that unique MAC address was called the basic service set identifier**, or the **BSSID**. Well in this example, since each access point has more than one SSID, each access point also has more than one MAC address. They have more than one BSSID. That's where we get the term multiple basic service set ID, or MBSSID. **It's an access point servicing more than one wireless network or SSID, each with its own unique MAC address.**

A screenshot of a computer

Description automatically generated

**From AI :**

The concept of Multiple Basic Service Set ID (MBSSID) is an advanced feature in wireless networking that allows a single access point to serve multiple networks using different SSIDs, each with its own unique MAC address. Let’s break down how this works and address your question about MAC addresses.

What is MBSSID?

Definition: Multiple Basic Service Set ID (MBSSID) is a feature that allows an access point (AP) to broadcast multiple SSIDs, each associated with a different Basic Service Set (BSS). This means that a single AP can support multiple virtual networks, each with its own SSID and BSSID.

Purpose: MBSSID is used to provide multiple virtual networks or "virtual APs" from a single physical AP. This can be useful for segmenting network traffic, providing different levels of access, or supporting multiple service levels (e.g., guest networks, corporate networks).

How Does MBSSID Work?

Multiple SSIDs:

An access point configured with MBSSID can broadcast multiple SSIDs simultaneously. Each SSID is associated with a separate BSS, even though they are all managed by the same physical AP.

Unique BSSID for Each SSID:

Each SSID within an MBSSID setup is associated with a unique Basic Service Set Identifier (BSSID). The BSSID is essentially the MAC address of the AP’s radio interface that is broadcasting that particular SSID.

Multiple MAC Addresses:

Although each MAC address is unique to a network interface, an AP can have multiple virtual interfaces, each with its own MAC address. In an MBSSID setup, the AP uses different MAC addresses for each SSID to distinguish between the different virtual networks.

For example, an AP might have one physical radio interface but can be configured with multiple virtual interfaces. Each virtual interface can have its own MAC address, enabling the AP to handle multiple BSSs and SSIDs simultaneously.

Why Can One AP Have Multiple MAC Addresses?

Virtual Interfaces: Modern access points can create multiple virtual interfaces on a single physical radio interface. Each virtual interface can have its own MAC address. This capability allows the AP to broadcast different SSIDs and serve multiple BSSs.

Network Segmentation: By using different MAC addresses, the AP can provide network segmentation. For instance, one SSID might be for internal corporate use, while another is for guest access. Each of these virtual networks operates independently, even though they are served by the same physical device.

Practical Example

Consider a single AP in a business that needs to support both employee devices and guest devices:

Employee Network: An SSID like CompanyNetwork might be used with a specific BSSID/MAC address, offering full access to corporate resources.

Guest Network: Another SSID like GuestNetwork might be used with a different BSSID/MAC address, providing internet access but restricting access to internal resources.

Both SSIDs are broadcasted by the same physical access point, but they use different MAC addresses for their respective BSSs. This setup ensures that traffic can be appropriately routed and managed according to the network's policies.

**Direct-Sequence Spread Spectrum (DSSS)**

- [Instructor] In WiFi networks, **we might send one bit of data using a frequency range that spans two megahertz**. ***However, we might run into interference because somebody else has a device like a Bluetooth game controller, or maybe a baby monitor that's running on the same frequency***. And **to help combat that potential interference**, **which could corrupt the binary bit we're trying to send*, we could use an auto-correcting coding scheme called Barker 11 coding***. **Specifically, we're going to be using a wider range of frequencies**. **A 22 megahertz frequency range**, and **we're going to be sending 10 extra bits*, meaning that we're sending a total of 11 bits***. **And those extra bits are called** **chip**s. **And if there is interference, hopefully there will be enough surviving chips to allow the series of bits to be correctly interpreted as the original bit that we were transmitting**. **In this sequence of 11 bits that we're sending**, **each of which uses a two megahertz frequency range**, that **sequence is called a symbol**. And this type of data transmission technique was commonly used in the older 802.11b wireless standard, where as we saw when we talked about the 2.4 gigahertz band earlier in this course***, we saw that a single channel spanned 22 megahertz***. Well now we see where that number comes from. We're sending 11 bits, each of which consume a two megahertz frequency range, and that gives us a total of a 22 megahertz frequency range.

A diagram of a waveform

Description automatically generated

A diagram of a curve

Description automatically generated

**Frequency Division Multiplexing (FDM)**

Selecting transcript lines in this section will navigate to timestamp in the video

- [Instructor] With direct sequence spread spectrum that we talked about in our previous video, we used the entire 22 megahertz frequency range of a channel to send a single bit, and there was a lot of overhead due to that Barker 11 coding scheme. A more efficient way to carry this data is to use frequency division multiplexing, or FDM. With FDM, our single channel is divided into non-overlapping sub-channels. In fact, we don't even use the entire 22 megahertz channel width. We only use a 20 megahertz channel width. And each of these sub-channels, they carry a different signal. This is really similar to how a cable TV system works, it carries different television shows over the same cable. Each show is on its own channel, in other words, each show has its own range or frequencies. However, there is a concern. Even though these frequencies are technically non-overlapping, they're right next to each other, and even the slightest deviation from a signal's allocated frequency range could cause one signal to leak over a little bit into the adjacent sub-channel. We're going to take a look in our next video what I had to address that issue.

A diagram of a frequency

Description automatically generated

**Orthogonal Frequency Division Multiplexing (OFDM)**

Selecting transcript lines in this section will navigate to timestamp in the video

- [Narrator] In our previous video we mentioned that, with frequency division multiplexing, or FDM, we could have adjacent subchannels interfere with one another. A way to prevent that potential interference is to send those adjacent subchannels at right angles to one another. When the waveforms are at right angles to one another, we say that they are orthogonal to one another. And if they're orthogonal to one another, they're not going to interfere with each other. That's the benefit of using OFDM, or orthogonal frequency division multiplexing. In other words, since we're sending these adjacent subchannels at right angles to one another, they don't interfere with each other. And we're going to see later that this technique of OFDM, it's going to be used by the 802.11n and 802.11ac wireless standards.

A diagram of a line and a diagram of a line

Description automatically generated

**Quadrature Amplitude Modulation (QAM)**

Selecting transcript lines in this section will navigate to timestamp in the video

- [Narrator] We mentioned in the previous video that we could reduce interference between adjacent sub-channels, by sending those sub-channels at right angles to one another. And in antenna theory, that's something that we can control. The angle of a transmission. Something else we can control is the amplitude, or the power, the height of a waveform. So let's say we created a grid, and for simplicity, let's just identify 16 points on this grid. Then, we could angle a waveform and adjust its amplitude, or its height, such that the top of a waveform would hit one of these 16 dots. Now, consider that number of 16. How many binary bits does it take to give us 16 different combinations? The answer's four. That means we could assign a unique four bit pattern to each of these dots. And that means, if we angle a waveform and adjust its amplitude to intersect with one of those dots, that single waveform could represent four bits of data. Instead of just a single bit. That's going to make our transmission much more efficient. It's a lot like throwing darts at a dartboard. When you hit a certain section on a dartboard, there's an associated number of points that you receive. Similarly, when you hit a certain dot on this grid, there's an associated string of bits that you're representing. And by the way, the term that we give to this grouping of dots is called a constellation because as we get more and more dots, it starts to look somewhat like a star field. And this technology is called Quadrature Amplitude Modulation. Q-A-M, which is pronounced QAM. In this case, since we're using 16 dots, this is called 16-QAM. However, some of our wireless standards as we're going to be seeing later on in the course, use 64-QAM, which can represent 6 bits with a single waveform. Or 256-QAM, which can represent 8 bits. Or even 1,024-QAM, which lets a single waveform represent 10 bits. That makes our transmission much much more efficient than representing a single bit with a single or more than one waveform.

A screen shot of a diagram

Description automatically generated

A screenshot of a graph

Description automatically generated

**Basic Concept of QAM**

* **Quadrature Amplitude Modulation (QAM)**: In QAM, two signals are modulated to represent data. These signals are typically sine waves that are 90 degrees out of phase with each other, hence "quadrature." By varying the amplitude of these two signals, QAM encodes data into combinations of different amplitude levels.

**How QAM Works**

1. **Two Carries in Quadrature**:
   * QAM uses two carrier signals that are 90 degrees out of phase (i.e., in quadrature). One carrier is usually referred to as the in-phase component (I), and the other as the quadrature component (Q).
2. **Amplitude Modulation**:
   * The amplitude of each carrier signal is varied according to the data being transmitted. The combination of these two amplitude-modulated signals creates a unique signal constellation.
3. **Signal Constellation**:
   * The resulting signal can be represented on a two-dimensional plane where the X-axis represents the amplitude of the I component and the Y-axis represents the amplitude of the Q component. Each unique combination of amplitudes corresponds to a distinct symbol.

**Types of QAM**

* **16-QAM**:
  + **Constellation**: 16-QAM has 16 different symbols, represented as points in a 4x4 grid on the signal constellation diagram. Each symbol represents a unique combination of 4 bits of data.
  + **Bit Rate**: Each symbol can encode 4 bits, so the bit rate is higher than simpler modulation schemes like Binary Phase Shift Keying (BPSK) or Quadrature Phase Shift Keying (QPSK), but lower than higher-order QAM schemes.
* **64-QAM**:
  + **Constellation**: 64-QAM has 64 different symbols, arranged in an 8x8 grid. Each symbol represents a unique combination of 6 bits.
  + **Bit Rate**: With each symbol encoding 6 bits, 64-QAM offers a higher data rate compared to 16-QAM. However, it is more susceptible to noise and signal degradation due to the closer spacing of the symbols.
* **256-QAM**:
  + **Constellation**: 256-QAM has 256 symbols, typically arranged in a 16x16 grid. Each symbol represents 8 bits of data.
  + **Bit Rate**: This allows for very high data rates since each symbol encodes 8 bits. However, the signal is more sensitive to noise and interference due to the even closer spacing of the symbols.

**How QAM Works in Practice**

1. **Encoding Data**:
   * Data to be transmitted is first converted into a series of bits. These bits are then grouped into symbols according to the QAM scheme being used (e.g., 16, 64, or 256 symbols).
2. **Modulation**:
   * The symbols are used to modulate the amplitudes of the I and Q components of the carrier signals. The combination of these modulated signals creates the final transmitted signal.
3. **Transmission**:
   * The modulated signal is transmitted over the communication channel. At the receiver, the signal is demodulated to recover the original data.

**Trade-offs**

* **Higher Data Rates**: Higher-order QAM (like 64-QAM or 256-QAM) allows for higher data rates because more bits are encoded in each symbol.
* **Susceptibility to Noise**: Higher-order QAM is more susceptible to noise and signal degradation. As the number of symbols increases, the distance between them decreases, making it harder to distinguish between symbols in noisy environments.

**Summary**

* **16-QAM**: Encodes 4 bits per symbol, offering moderate data rates with moderate resistance to noise.
* **64-QAM**: Encodes 6 bits per symbol, providing higher data rates but with increased sensitivity to noise.
* **256-QAM**: Encodes 8 bits per symbol, offering very high data rates but with even greater susceptibility to signal degradation.

QAM is widely used in digital communication systems, including Wi-Fi, digital TV, and modems, to efficiently transmit large amounts of data over various types of communication channels.

**Channel bonding**

Selecting transcript lines in this section will navigate to timestamp in the video

- [Presenter] Earlier we talked about having a wireless channel consume a 20 megahertz frequency range. And one thing we can do to allow us to send more information for more wireless devices is to increase the width of that channel by combining adjacent channels. If we combine two adjacent channels, that's going to give us a 40 megahertz channel width. And that's possible with 802.11n, as an example. And with 802.11ac and .11ax, we can go even further. We can combine four 20 megahertz channels to give us a single channel with an 80 megahertz channel width. We could even combine eight channels to give us a 160 megahertz channel width. That's another way to increase overall throughput. We're increasing the throughput by increasing the frequency range that can be used by a single channel.

A diagram of a row of chairs

Description automatically generated

**Beamforming**

Another WiFi enhancement is beamforming. With beamforming, instead of just radiating out a wireless signal in all directions, we can actually focus the access point's transmissions towards specific wireless clients. And the way that's possible is the access points can use multiple waveforms. For example, **if you have two identical overlapping waveforms, the high points of those waveforms get added together and the resulting waveform is twice as high. That's something called constructive interference**. Conversely, if you take a waveform and make a copy of it, and you flip it upside down on top of the original waveform and you add those together, they add up to zero. That's the way that noise cancellation headsets work. They listen to the background noise in your environment and they play that noise back, except the waveform is inverted. **That causes those waveforms to be 180 degrees out of phase. And the result is silence. That's called destructive interference**. And using these concepts of constructive and destructive interference, we can point or focus our radio waves towards a wireless client. And **this feature was originally introduced back in 802.11n**. But it got better in 802.11ac, and it continues to get even better in 802.11ax.



A graph on a white background

Description automatically generated

A screen shot of a computer

Description automatically generated

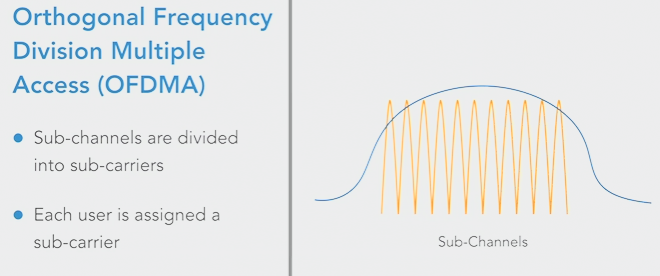
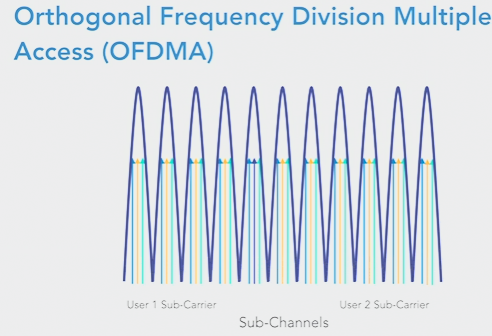
**MU-MIMO**

Something else that can increase our speeds is MU-MIMO. **MU-MIMO stands for multi-user, multiple input, multiple output**. Basically, **we're talking about having multiple antennas inside of our access points**. ***Way back in 802.11n, we had a single spatial stream, meaning that we could transmit one stream of communication at any one time***. For example, if I needed to talk to both wireless clients from this access point on screen, I would have to send the signal twice. ***Once to one client, and then I'll have to send it to the other client***. ***I would have to take turns***. **However, with the current versions of 802.11ac and now 802.11ax, we can have multiple antennas that simultaneously transmit out to multiple clients**. As an example, let's say that here we have two spatial streams, where I can simultaneously communicate from my access point to both wireless clients. That's going to give us increased throughput in larger networks.



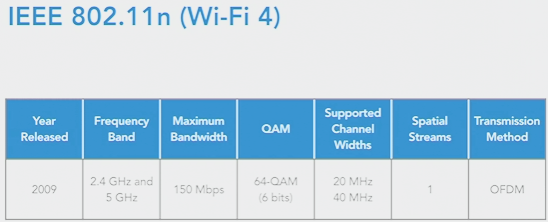
**Orthogonal Frequency Division Multiple Access (OFDMA)**

Earlier in this course, **we discussed orthogonal frequency-division multiplexing**, or **OFDM**. And there, we took a single frequency range and we divided it up into multiple sub-channels. And that way, each user could have a different sub-channel. However as we have more and more wireless clients, we might have too many wireless clients trying to transmit at the same time. To address that issue, we can use something called **orthogonal frequency-division multiple access, or OFDMA. With OFDMA, each of those sub-channels get subdivided into sub-carriers, and each user can then be assigned to a sub-carrier**. It's going to look something like this. In this example, the blue arrows represent user one's sub-carrier. And the yellow arrows represent user two's sub-carrier. This allows multiple users to simultaneously transmit using the same sub-channel. And as we're going to see later, this is one of the technologies that gives 802.11ax such a high throughput.



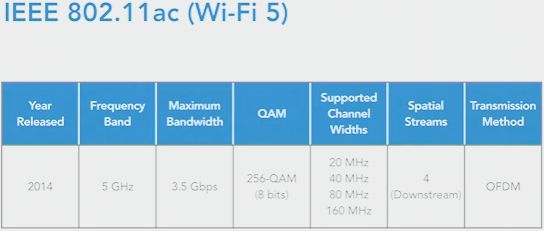
IEEE 802.11n (Wi-Fi 4)

Now, let's start to compare some recent IEEE wireless standards, beginning with the **IEEE 802.11n wireless standard. This is also known as Wi-Fi 4. 802.11n has been around for a while. It was released back in 2009**, and you might remember that we had two frequency bands that we could use, the 2.4 and the five gigahertz bands? **Well, 802.11n can operate on one or both of those bands at the same time**. And the flavor of **quadrature amplitude modulation that we're using is 64-QAM**, and that allows us to represent six bits with a single wave form. And **it's possible to combine a couple of our adjacent 20 megahertz channels to form a channel with a channel width of 40 megahertz**. Also, 802.11n, the standard says **we only support a single spatial stream,** and the **transmission method that we're using is OFDM**.



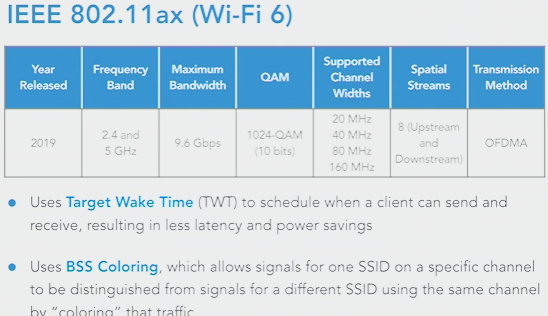
IEEE 802.11ac (Wi-Fi 5)

- [Instructor] In our previous video, we took a look at some of the characteristics of the IEEE 802.11n standard. Now let's contrast that with the 802.11 ac standard, which is also known as Wi-Fi 5. **802.11 ac** came out about five years after the .11n standard, **being released in 2014**. And one big difference is that **IEEE 802.11 ac only operates in the five gigahertz band**. It doesn't use the 2.4 gigahertz band at all. And **its maximum bandwidth is significantly higher, at 3.5 gigabits per second**. And that's due in part to **its ability to represent eight bits with a single wave form. It does that using 256 QAM**. And we can combine a couple of our **20 megahertz channels into a single 40 megahertz channel**. Or we could combine four of those regular channels into an 80 megahertz channel. **Or on some equipment, not all, but on some equipment, we can combine eight of those 20 megahertz channels into a single 160 megahertz channel**. And beginning with 802.11 ac, we can support **MIMO by sending as many as four spacial streams at once**. However, that's downstream only going from the access point out to our endpoints. And finally, just like 802.11n **802.11 ac also uses OFDM**, orthogonal frequency-division multiplexing for its encoding.



IEEE 802.11ax (Wi-Fi 6)

- At the time of this recording, t**he newest wireless standard is 802.11ax, also known as Wi-Fi 6**. **It was released in 2019** and **it operates on both the 2.4 and 5 gigahertz bands**. It's got a **very fast theoretical maximum bandwidth of 9.6 gigabits per second**, and its implementation of **1024-QAM lets us represent 10 bits with a single waveform**. And it supports the same channel with options that we saw with .11ac. The **number of simultaneous spatial streams that we can send out has increased to eight**. **But in addition to those eight downstream spatial streams, we can also have eight upstream spatial streams**. And another big difference with 802.11ax is its use of **OFDMA, orthogonal frequency division multiple access, which, as we saw earlier, takes sub-channels and divides them into sub-carriers**. Another huge advantage of 802.11ax is its use of the **Target Wake Time feature. With this feature, our wireless clients are not contending for access to the airwaves**. **Instead, they're told when they can transmi**t. But specifically, **the access point tells the wireless client when to transmit and when it can go into a low power mode when it's not transmitting**. That's not only going to give us better power efficiency**, it's going to reduce the number of collisions that occur when we have lots of wireless clients simultaneously trying to transmit**. And another feature called **BSS Coloring, where BSS stands for basic service set.** That feature helps us reduce interference. Specifically, **we can have nearby access points advertising different SSIDs, but using the same channel and 802.11ax can quote unquote color those transmissions**, so they're associated with the appropriate SSID in order to prevent interference with nearby access points using a different SSID. And that's the comparison between 802.11n 802.11ac and 802.11ax.



-------------

---------------------------------

------------------------------------------------

**The need for wireless security**

Let's consider the need for wireless security. As a metaphor, ask yourself, would you consider putting an Ethernet jack from your network in the parking lot of your building? Of course not, that's not secure. However, if we don't properly secure our wireless networks, then their signals extend outside of our building. That's essentially what we're doing. So we clearly need to secure our wireless networks. But what does that mean exactly? Well, **there are two primary things that we want to achieve with wireless security**. The first is **authentication**. We want to make sure that **someone connecting to our network has appropriate credentials to do so**. **And if anyone were to intercept that wireless communication, we don't want them to be able to interpret the data**. The way we accomplish that is through **encryption**, which scrambles up the data, **making it unreadable to anyone other than the intended recipient.** And over the next few videos, we're going to be taking a look at the history of wireless network security, and see what the best options are today for securing our wireless networks.

**Wired Equivalent Privacy (WEP)**

- Built into the original 802.11 standard was a security feature called WEP. And **WEP stands for** **Wired Equivalent Privacy**. And the name **implies that WEP gives your wireless communication the same privacy that you would have with a wired communication link**. And that's not true, at all. Let's take a look at some of the characteristics of Wired Equivalent Privacy. First, **it was part of the original 802.11 standard**, so it's been around for a while. And it uses the **RC4 encryption algorithm**. But it's really how that encryption algorithm is implemented that makes WEP so weak. Here's what's going on. **With the RC4 encryption algorithm, we use something called an initialization vector**, or **IV** for short. And this **IV is combined with the shared secret key that we configure on our access point, and our wireless clients**. And that's applied to the string of data we want to encrypt, and the resulting encrypted string of data is called **ciphertext**. And with **WEP, the IV was only 24 bits in length**. And the **key could be either 40 bits or 104 bits in length**. But since the **IV was only 24 bits long**, **it became mathematically possible to capture enough encrypted packets and determine what the shared secret key was**. In fact, **if you were able to capture about 30000** **packets** containing **initialization vectors, you had about a 50/50 shot of getting that shared secret key**. **And once you captured around 800000 initialization vectors,** it was almost a guarantee that you would be able to calculate that shared secret key. **In fact, on average, it takes about three minutes to crack a web password**. So we do not want to use it. Also, the **idea of having the same key configured on our access point and all of our wireless clients, that doesn't scale very well**. So it's clear we need some enhancements. And in our next video, we'll consider some different key distribution modes, and then, we'll consider some stronger wireless security options.



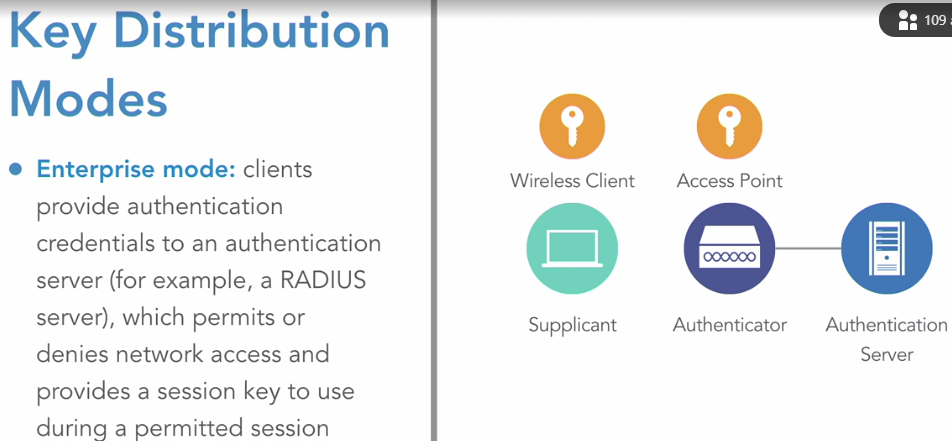
Key distribution modes

Selecting transcript lines in this section will navigate to timestamp in the video

- [Instructor] The encryption algorithms that we use on our wireless networks use a key, which is a long string of characters that an eavesdropper would not know, and that would prevent them from decrypting our encrypted transmission. And we've got a couple of modes of key distribution. The first mode is pre-shared key, or PSK mode, also known as personal mode. Here, we go to an access point and we configure it with a pre-shared key. Then we go to a wireless client and we configure it with the same pre-shared key. In fact, we go to all of our wireless clients on the network and we configure all of them with the same pre-shared key. But imagine what would happen if that key became compromised. We would have to go reconfigure that key on all of our devices. So while having a pre-shared key might be fine for a home environment or for a small office environment, it doesn't scale very well. For larger networks, we probably want to consider enterprise mode. With enterprise mode, the client typically logs in. In fact, a client usually sends authentication credentials to an authentication server. Maybe they're providing a username and a password. And if that authentication server says, yes, they have authenticated successfully, then the server is going to send out a session key, which is only valid for this session, to both the wireless client and to the access point. And that session key is going to be used to encrypt transmission between that wireless client and the access point, only for the duration of that one session.

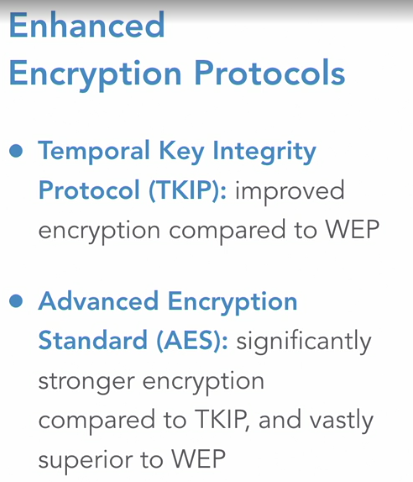
**Key distribution modes**

- [Instructor] The encryption algorithms that we use on our wireless networks use a key, which is a long string of characters that an eavesdropper would not know, and that would prevent them from decrypting our encrypted transmission. And we've got a couple of modes of key distribution. **The first mode is pre-shared key**, or **PSK mode,** also known as **personal mode**. Here, we go to an access point and we configure it with a pre-shared key. Then we go to a wireless client and we configure it with the same pre-shared key. In fact, **we go to all of our wireless clients on the network and we configure all of them with the same pre-shared key**. But imagine what would happen **if that key became compromised. We would have to go reconfigure that key on all of our devices**. So while having a pre-shared key might be fine for a home environment or for a small office environment, it doesn't scale very well. **For larger networks, we probably want to consider enterprise mode**. **With enterprise mode, the client typically logs in**. In fact, **a client usually sends authentication credentials to an authentication server**. Maybe **they're providing a username and a password**. **And if that authentication server says, yes, they have authenticated successfully, then the server is going to send out a session key**, **which is only valid for this session**, **to both the wireless client and to the access point**. And **that session key is going to be used to encrypt transmission between that wireless client and the access point, only for the duration of that one session.**



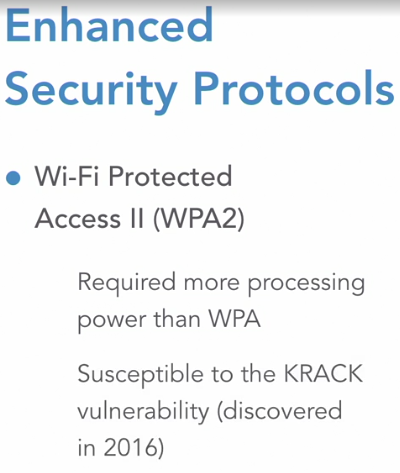
**Enhanced encryption protocols**

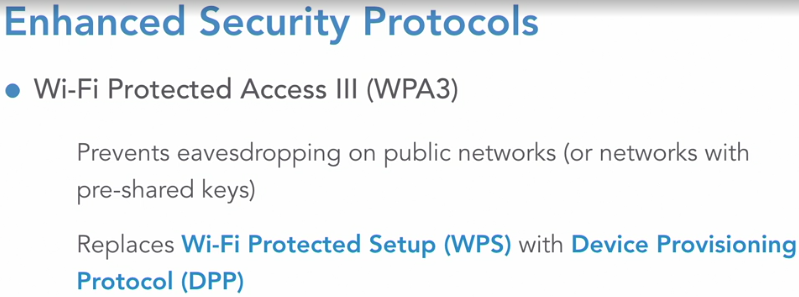
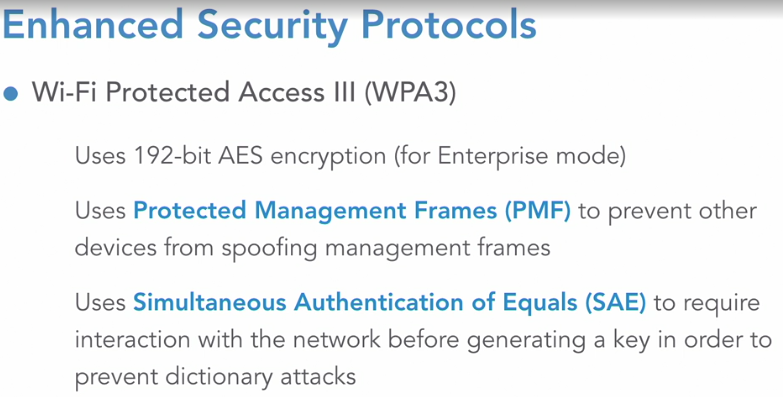
We said that **WEP gave us very limited security because of the way it implemented the RC4 encryption algorithm**. So let's consider some enhancements that can give us better security. **After WEP was discovered to be quite vulnerable to attack**, **TKIP was introduced for wireless security**. And **TKIP stands for Temporal Key Integrity Protocol,** **and *it dramatically improved on the encryption provided by WEP***. **It does still use that RC4 algorithm as the underlying encryption algorithm**, **but it changed how that initialization vector was combined with the key**, and **it also used a longer initialization vector**. It uses a **48-bit initialization vector, as opposed to *WEP's 24-bit initialization vecto****r*. And that's going **to make it mathematically much more difficult to derive the shared secret key**. And **going a step beyond TKIP, we have AES**, which stands for **Advanced Encryption Standard**. And that **is significantly stronger than TKIP and vastly superior to WEP**. Now in our next video, let's consider how these encryption protocols are going to be used in our wireless security standards.



**Enhanced security protocols**

After the web security standard, came out **Wi-Fi Protected Access or WPA**. And it used **TKIP for encryption**. And **the idea was to use it as a temporary measure to get away from WEP because WEP was so weak and we wanted to be able to just upgrade the software on the access points without having to upgrade the hardware**, because **if we went directly from RC4 to AES, that might put too much processor demand on our existing access points and clients**. However, **it was long before attackers developed a way to break WPA security**. And then came **WPA2**. In fact, **in order to become Wi-Fi certified as of 2006**, **your device had to support WPA2**. And **WPA2 required that your device be able to support AES**. **Even though you could optionally run TKIP instead, you had to have the option of running AES if the user wanted to**. And as newer wireless devices were released with more processing power, **it became reasonable to use AES as the encryption algorithm**. But specifically, **we used 128-bit AES**. And for years, WPA2 became the gold standard for a wireless security. However, **in 2016, it was discovered that WPA2 was susceptible to a vulnerability called KRACK**. Then came **WPA3, It was released in 2018.** **And here, in Enterprise mode, we used a 192-bit key as compared with the 128-bit key that WPA2 used for AES,** **just in Enterprise mode.** **We still use a 128-bit key for AES if we're using a personal mode or pre-shared key mode**. **And when WPA3 was introduced, it came out with something called Protected Management Frames or PMFs**. **This is going to prevent another device from spoofing management frames that attempt to connect to an access point for administrative purposes**. **Something else that was added with WPA3 was Simultaneous Access of Equals or SAE**. **This requires someone to interact with the network before a key can be generated**. **This can prevent an offline attack, like a dictionary attack**. So you have to be talking with the network before you can be given a key. **And also, think about when you're in a public area and you're sharing an open access point with other users or maybe you're in a pre-shared key environment and everybody else has the same pre-shared key that you do, what's to prevent one user from eavesdropping on another user?** Well, that was an issue. **But with WPA3, it was able to prevent eavesdropping on public networks and on networks where everyone has the same pre-shared key**. **Another enhancement is that Wi-Fi Protected Setup or WPS is gone. The purpose of WPS was to make it easy to add a wireless client to the network**. **You could press a button on your wireless access point and you would be able to provision a new device very easily, but it had a vulnerability as well**. **So WPS has been replaced with Device Provisioning Protocol or DPP for short.** Of course, securing our wireless networks will probably continue to be a game of leapfrog or a vulnerability is discovered, followed by a fix, followed by another vulnerability and so on. **But at the time of this recording, WPA3 is considered to be the best option among the widely available security protocols**.





**Installing an Autonomous AP**

Linksys wireless router setup

- In this chapter we're going to be setting up a typical wireless router that we might find in a home or in a small business. Specifically we're going to be setting up this Linksys wireless router. And wireless routers from other vendors, the configuration interface might look different but the settings are the same. And the great thing about this Linksys wireless router is if we want it can work right out of the box. Let's take a closer look. If we take a look at the back of our wireless router we've got a yellow port that gets us out to the internet and we've got these four blue ports. This is a four port ethernet switch. It's into these ports that we could connect our ethernet devices or we could even connect another switch into these ports, to give us an even higher port density. And we mentioned that this device would work out of the box. If we don't want to do any configuration at all we could look on the bottom and it gives us a default SSID and the wifi password. But let's do this, let's go out to a browser, connect to the administrative interface of this wireless router and let's set up a non default configuration. Our Linksys router is booted up and the internet connection is going out to the internet. My computer is plugged into one of those switch ports on the back. And without doing anything else I'm connected to the internet**. But what we want to do is set up some non default settings**. To do that we're going to point our browser to the default wireless router IP address of 192.168.1.1. And I've already done that and this is the initial setup page. By the way, if you're using a wireless router from another vendor it still may be 192.168.1.1 that you point to, that's very common. However some vendors might use 192.168.0.1. Just check your wireless router's documentation. But here I'm pointing to 192.168.1.1 and I'm going to say that, yes, I have read the license terms, and I'm going to opt out of sending information back to Linksys reporting router errors. And we'll click on Next. And again, the interface that we're going through here is going to look at bit different if you're using a wireless router from a different vendor, but when we get into the settings like setting up channels, setting up security, those basic settings are going to be the same across all of our vendors. I'll leave the check box checked that says hey, I want to get an update for my router if another update becomes available. And we'll click on next. Now we see the wifi names that we have by default. Notice that there's one for the 2.4 gigahertz band and there's another one for the 5 gigahertz band. Now this might be desirable. **A lot of times when you're working with IOT, internet of things, devices they often want to work on the 2.4 gigahertz band**. **So there can be an advantage of having your bands have a separate name**. In my example though **I'm going to say that I've got a lot of smart phones, I've got a lot of wireless laptops and they're going to be roaming around an area. And I want to connect to either the 2.4 or the 5 gigahertz band using the same wireless name**. And I could hard code that, I could type in the same name twice but I have a shortcut here. It says give all of my wifi bands the same name. I'm going to select that and I'm going to call the name, which is our SSID, I'm just going to call it DEMO. And I'm going to use the non secure password, please done use this but just for the demo purposes I'm going to call it demopass. And we'll click on Next. And in the future I may want to point to 192.168.1.1 and get in and do some additional configuration on this router. To do that I need to set up a password to get in. And I'm going to use a very basic password of admin just for demo purposes. And I'm going to add a hint of default. Typically Linksys wireless routers have a default username and password of admin. And we'll say Next. Now we see a summary of our set up. We see that both bands, the 2.4 and the 5 gigahertz band, we see that they both have the same SSID of DEMO, and they both have the same wifi password. And I'll say Next. And I'm going to opt out of using a smart wifi account which would let me manage remotely. We'll just skip that because that does vary quite a bit between vendors. And we're presented with this dashboard where we can do some additional configuration. For example, by going through the wizard it turned on a guest network. And it's called DEMO-guest and the password it just dynamically assigned to us, cherry19. We could leave that if we wanted to, or we could turn it off. I'm going to opt to turn off the guest wireless network. By the way, when somebody is connecting to your guest wireless network they'll see that it's not protected with a password. There will not be a lock next to it when they look through the available SSIDs. But once they attach to it they'll be prompted to enter the password. So the password is entered after connecting to the network. So we've turned off guest access and now we want to see if we can connect to this wireless access point. So I'm going to go up and select DEMO and on another screen I'm being prompted to enter the password, and I'm going to say demopass. And we'll say join. And let's see if we connect. Great news, we're connected to the DEMO SSID and that's a look at how to set up a basic configuration on a Linksys wireless router.

Configuring channels

Here we're sitting at the dashboard of our Linksys wireless router that we set up in the previous video. In this video, let's see how we can manipulate channel selection. To do that, I want to go under Wi-Fi Settings. And notice that we have both the 2.4 and the 5 gigahertz band with the same SSID. Again, **you may want to have the 2.4 gigahertz band have a different SSID if you have some devices that can only communicate using the 2.4 gigahertz band. That happens sometimes with internet of things devices**. **In fact, if you're setting a wireless router up for that purpose, we could entirely turn off the 5 gigahertz band**. Or if we're going to have clients that we know are compatible with the 5 gigahertz band and we don't want to cause interference for the 2.4 gigahertz band, we could turn off the 2.4 gigahertz band. But let's take a look at channel selection. **Typically, we just let the wireless device itself dynamically listen to the radio waves in the air and set its own channel to minimize interference.** However, from a design perspective, **maybe we've laid it out where we're going to be using channels 1, 6, and 11 at very strategic points in the building and we want to control what channels get used**. **If we wanted to do that, we could set the channel for 1, 6, or 11 for the 2.4 gigahertz band, or we could just leave it at auto**. If I didn't want to announce this wireless network, **I didn't want to broadcast out my SSID, which could add a minimal layer of security, I could say, "No, don't even advertise this**. **"Somebody would have to know the name "in order to connect to this network**." **For the channel width, I'll just leave this at auto.** And for **the 5 gigahertz band, we could set a specific channel**. **And we have more channels to select from using the 5 gigahertz band. And I'll leave that at auto**. **And if I wanted to, I could adjust the channel width to 20 megahertz, 40 megahertz, or 80 megahertz is available if I select a Wi-Fi mode of 802.11ac only**. **If I did that, we would want to make sure that our wireless clients could speak 802.11ac.** Otherwise, they wouldn't be able to connect. And we also have different Wi-Fi modes we could select for the 2.4 gigahertz band. And that's a look at how we could do some channel manipulation on our Linksys wireless router.

Configuring security

We're back at the dashboard of our linksys wireless router. And we've seen this in the prior two videos. This time though, we want to take a look at setting up our wireless security. We had an earlier video in this course that talked about wireless security. Let's go take a look at some of the settings. We go under Wi-Fi Settings, and we have our security mode. The options- and this is for both the 2.4 and the 5 gigahertz bands. The options are **None, where no one is required to enter any sort of authentication credentials.** **They just get to attach to the network. That might be good for a coffee shop or something, where you want to make it open to guests**. **The default is WPA2 Personal, and we do have the option for WPA2 Enterprise.** If we select **Enterprise, we're going to have to set up user accounts for each of our users.** They're **going to authenticate with the wireless network by providing not just a pre-shared key on their device**. **They're going to have to provide a username and a password**. And that's great for a large enterprise. **That way if somebody leaves the company we don't have to change everybody's Wi-Fi password**. **We simply delete their account**. **But typically in a small or home office environment, we set this to WPA2 Personal**. And **we'll leave it set at that default**. And by doing that, remember we have a pre-shared key configuration where this password has to be entered on the wireless client. And they're going to match. The downside to doing this, if somebody were in your company and they knew this wireless password, if they were to leave your company they would still know the wireless password that you're currently using. That's the advantage of using Enterprise mode for a larger environment. But if you can control the devices that have access to this network, you may just want to go with WPA2 Personal.

**Ubiquiti UniFi Controller installation**

Here we have the basic components that we're going to use to set up our UniFi wireless network. First we a have a **USG, this is the UniFi Security Gateway**. **It's going to act as a router and a firewall,** so we're going to connect it into the internet connection, **there's a WAN 1 port we'll connect into, and it's got to get into the rest of the network.** So let's plug in a second connection into the LAN 1 port and we'll connect that into our ethernet switch. This is a 24-port Power over Ethernet switch, and it's actually going to be powering all of our wireless access points. We'll connect this into the network. There is a main connector that I'll use. And we'll plug that into the switch. And finally we have our controller. This is a UniFi Could Key Gen2 Plus Controller, and this is going to be talking to all the devices of the network. All the devices, the UniFi devices, they're going to be adopted by this controller and we're going to configure everything from this single interface. Now let's connect it into the network. Interestingly, it's going to be powered by the switch because it can use Power over Ethernet. Now that we've got everything plugged in, and also we have our laptop, we can do our configuration there, now that we've got everything plugged in, let's go out to a live interface and configure our UniFi wireless network. Let's begin the configuration of our UniFi wireless network by going to the USG. It has a default IP address of 192.168.1.1, and the USG, remember, that's going to be our router and our firewall, so this is the default gateway that's going to be assigned to our endpoints. By the way, when you go to the USG for the first time, your browser might prompt you as to whether or not you really want to go there, because it's going to have a self-signed certificate and it might warn you that it's an unsafe website. But I've already told my browser to trust it, and here we are. It says congratulations, we're connected to the internet. And the way this USG got an IP address was via DHCP from my service provider, and that might not be your situation. Perhaps you want to go under configuration and say I don't want to get my IP address via DHCP, I want to get it via Point-to-Point Protocol over ethernet, that's how you might do it with a DSL connection. Or maybe you have a static IP address assigned. You might want to assign a different LAN, range of IP addresses for your endpoints. By default it's 192.168.1.0/24. Maybe that's not going to give you enough usable endpoints. You might want to give a different network address based with a different subnet mask. Maybe you've got a different device that's acting as your DHCP server. You could say that you don't want to use the USG as the DHCP server. In my case, I do, so I'll just leave this at the default settings, and let's go over to our controller, take a look there, let's go to... And by the way, you can learn the controller's IP address simply by looking on the front of the controller. Mine has an IP address of 192.168.1.9. And we'll go there, and because this is a Gen2 Plus Controller, the Plus indicates that in addition to managing the UniFi wireless network, we can also manage UniFi Protect. That's a video surveillance system where we attach cameras to our switch as well, and it's managed by this controller through a different interface. Now, we're not going to be doing that in our setup, we're just going to be setting up the Wi-Fi network. But first, before we do the Wi-Fi network, let's go to our Cloud Key, that's our controller, and the default credentials are UBNT. UBNT, let's log in. And it's going to prompt us for a different password for future access, so let me put in a different password. I'm going to paste it in so I don't mistype it. We'll say Accept. And here we can see an overview of our controller. For troubleshooting, you might want to go under the Performance tab and see if we're maxing out any resources. Again, we see that we can control a Wi-Fi network or the video surveillance UniFi Protect network. Now let's go over to Settings. Really, the only thing I typically change at the beginning is under Settings. I'm going to set the time zone. I'm in U.S. Eastern Time, so we'll set that and we'll say Apply Changes. By the way, you might want to change the firmware if there's a firmware update available. You can click on Firmware. And right now it says I'm up to date. If I were not up to date, there would be a button here that would let me do an update, but I'm already up to date so I'm good to go. Now let's go back to our Cloud Key tab and say we want to set up our UniFi network. And it begins by saying what is the controller name? Now, this is going to be installed in a residence. The family's name is Ray, so I'll say this is the Ray controller, we'll say Next. For the username and password, this is your Ubiquiti account. You may or may not have a Ubiquiti account already set up. If you don't you can go to their website and set one up for free. That allows you to log into a browser wherever you are in the world, and as long as you have cloud access enabled, you're able to manage networks even though you're not physically there. I definitely want to do that, so I'll log in with my Ubiquiti credentials. And we'll say Next. And under the option of automatically optimize my network, personal opinion, I like to turn this off. I've had some issues with Internet of Things devices like televisions and appliances. They sometimes want to attach just to the 2.4 gigahertz range, and this might prevent that from happening. So I just like to turn this off, personal opinion. I do want to the leave the enable auto backup enabled. And we'll click on Next, and what is our wireless name? In other words, what is the SSID that's going to be advertised? Well, this is going to be for a residence, and the family name is Ray, again, so I'll say it is the Ray House. And for the password, I'm going to copy-paste that in to make sure I get it correct. And instead of having different networks for the 2.4 gigahertz range or the 5 gigahertz range. I'll just say let's both use the same SSID name, and we'll just pick one of those two frequency ranges. Let's click on Next, and you can see these three devices that we have ready to adopt into our controller. We've got the access point, we've got the UniFi Security Gateway and we've got our 24-port Power over Ethernet switch. Now I'm going to check this box to select all of them and we'll say Next, we'll say we want to adopt everything. I'll just verify that everything looks good there. I do have remote access enabled. I'm logged in with my Ubiquiti account. There's the SSID, the time zone is correct, the controller name is correct, looks great. Let's click on Finish, and it's going to take a few minutes for the controller to update and get everything reset, and when it's done we should have a nice blue light on the USG, on our switch, and also on our access point. I don't want you to have to wait through that inthe video, so I'm going to pause the video right here, and after everything has been reset and rebooted and we're ready to go, we'll resume the video. The controller has now reset, everything's been rebooted or reset, and things are looking great. In fact, it tells us that. Now let's take a look at the devices that we have in our network right now. If we go over to this little icon on the left labeled Devices, it looks a bit like an access point, if we click on Devices we can see the three devices that have been adopted by this controller. However, they're known by their MAC addresses. I prefer to use names instead of MAC addresses. I'm going to go in and quickly relabel these. Let's click on the MAC address of our USG, and under the Config gear icon we can say alias, and I'll give it an alias of simply USG. We'll save that and I'll give the switch an alias as well. Let's go under the gear Config icon, and the alias is going to be simply Switch. And finally for our access point. We're going to have a total of five access points in this installation. This one's going to be located in the kitchen so we'll say the alias is Kitchen, and we'll save that. And at this point we should have a fully-functioning wireless network. Just to prove it, let's go out to my iPhone and let's see if we can connect the Ray House network and give our credentials. I did need to wait for the access point to finish provisioning after the alias name change, but that's done now and we're ready to get on the new network that we've created. Again, the network name, the SSID, was Ray House. And I'm going to go under Wi-Fi, let's see if we can find Ray House, there it is. And I'll give the password, we'll say Join. And we're successfully connected to the internet via our new wireless network.

**Adding APs**

- In this video, we want to see how to add some access points to our existing network. Our existing network currently has a single access point, but the final network that we're setting up is going to have five access points. We're going to have these access points scattered throughout a fairly large home, upstairs and downstairs and we want to add now four additional access points. The goal is we want our end stations like a smartphone or a laptop. We want those in stations to roam seamlessly around the home and associate with an appropriate access point based on their location in the house. And to do that we're going to add some access points and we'll scatter them physically around the house and we'll take a look in an upcoming video, at how to make sure we are using different channels to minimize interference between the access points. But right now we just need to add these four access points to our controller and as we hover over an access point, you'll see that it says adopt. That tells us it's not yet adopted and it looks like we've got these four that need to be adopted. so I'm just going to click on adopt for each one of these and it's going to take just a bit of time for all of those to be adopted by the controller. So what we're going to do right now is pause the video and after the adoption is complete, we'll resume the video and we'll change the names. We don't want these to have the default names of the Mac addresses. We'll come back and we'll set the names for these four brand new access points. Our four new access points have now been adopted by our controller. Let's change the name. I don't want to have to look at a Mac address. I want to know where this is located. Again, as we did in our prior video, I'll go into the gear icon for config and I'll set the alias. We're going to have one access point located in the upstairs hallway. So we'll give that as the alias and we'll say save. For another access point, we're going to have that in the game room and we'll save that. For another access point, we're going to have that in bedroom number one. And the other access point you probably guessed is going to be in bedroom number two. So we'll save that. We now have five total access points for this wireless network, and if these newly added access points needed to be updated, we could hover over them and it would tell us that an update was available. We're not seeing that. We're seeing restart and locate. This one's being reprovision right now. Actually, it looks like it's now done. The other one should pop up in a moment, but we just have the options of locate and restart and that one's ready to go now. So we've got these five wireless access points and we have a fully functioning and scalable network at this point.

**Configuring channels**

- Now that we have our unified wireless networks set up and we have five access points total, we want to make sure that those access points are not interfering with one another's radio signals and the great news is UniFi is going to try to do that on its own. They can automatically select some radio frequencies to use to make sure we minimize interference. Well, let me show you how we could go in and manually set that up. If we wanted to. Am going to just do one access point. Let's go into your kitchen and under kitchen we could set the channel width to 20 megahertz or 40 megahertz. Remember when we discussed the different channel widths. **If we want to really have three non-overlapping channels using the 2.4 gigahertz range, we probably need to keep the channel width to the default of 20 megahertz. Otherwise, we're not going to have those three non-overlapping channels of one, six and 11.** And what I've done in my home personally, I've gone in and just based on my knowledge of where XS sports are located, I've manually set the channels to either one, six or 11. We could do that here or we could just let the channels be auto selected because the UniFi wireless network does a great job of listening to signal strengths on these different channels and it's going to try to pick an appropriate channel based on what it hears. I'm also not going to mess with the transmit power, we could, but I typically leave that at auto. I'll let the controller take care of that and one thing I might want to change here is the five gigahertz channel width. Here we've got a default channel width of 40 megahertz and remember width five gigahertz, we have a very wide spectrum of frequencies that we could select from and we could get a wider channel width and still have non-overlapping channels by using an 80 megahertz channel width in many cases. And I won't bother to set the channels automatically. Notice we have a lot to select from. I'll just leave it at auto. Again, I'll not miss with the transmit power and we'll say queue changes and apply changes. Now I won't make you spend the time watching it on the video, but just to make sure everything matches up, I'm going to go through our four remaining controllers and also set the channel width to 80 megahertz for the five gigahertz range, and that's a look at how we can go in and manipulate channel settings to minimize interference between our access points.

AI :   
  
To configure three 5GHz-based devices with a Wi-Fi 6 router on non-overlapping channels, here's what you need to do:

1. **Understand Channel Widths**: In the 5GHz band, you have more channels available compared to the 2.4GHz band. You can use wider channel widths (40MHz, 80MHz) while still having non-overlapping channels.
2. **Select Appropriate Channels**: Unlike the 2.4GHz band where channels 1, 6, and 11 are non-overlapping, the 5GHz band offers more flexibility. For 80MHz channel width, you can use channels like 36, 52, and 100, which are non-overlapping.
3. **Manual Configuration**:  
     
   * Access your Wi-Fi 6 router's configuration settings.
   * Navigate to the 5GHz channel settings.
   * Set the channel width to 80MHz (or 40MHz if you prefer narrower channels).
   * Manually assign channels to each device. For example, set one device to channel 36, another to channel 52, and the third to channel 100.
4. **Automatic Configuration**: If you prefer, you can let the router automatically select the best channels. Many modern routers, like the UniFi system mentioned in the video, can automatically choose channels to minimize interference.

**Configuring security**

- Let's take a look in this video on how to add a guest wireless LAN. Again, the wireless network that we have set up right now is for residential use and when a guest comes over to this family's home, they can be told to get on the guest VLAN along with the password. By default, a guest VLAN that we set up is going to be open and not require a password, however this home is located in close proximity with lots of neighbors. We probably don't want those neighbors to, without a password, be getting on their network. So we're going to set up some security as well. To begin with, we're going to go under settings, that's on the lower left hand corner of the screen, and we're going to go to Networks and we're going to add a new network for the guest. We'll say create a new network, and the name, we'll just call it GUEST. And the purpose, it doesn't really matter what we set here, I'll just say corporate. And we are going to set a different VLAN. That's going to be a different broadcast domain. I'll say we're going to be in VLAN 2, and the gateway subnet, that's going to be the default gateway that users in that VLAN are going to be pointing to, and it's going to be different than our default gateway for everybody in the home right now, which was 192.168.1.1. This is going to be 192.168.2.1 with a 24-bit subnet mask. So we do a /24, and we do want to use DHCP. And I'll set the address range, I'll give away 100 IP addresses. I'll make the range that we give out to clients as 192.168.2.100 all the way through 192.168.2.199. That's really all I need to do here. I've created a new network called GUEST, I've put it in its own VLAN with its own range of IP addresses and I set up DHCP for clients in that VLAN. Let's say save. Now we want to create a user group. And this user group is going to have a limitation on the bandwidth that's going to be available to them. Let's create a new user group and we'll call this user group GUEST. And I want to limit the download and upload bandwidth. And I'll change the unit of measure to megabits per second, and this particular network connection has fiber and they get a gig download and they get only 30 meg upload, and we don't want the guest to have full access to that. So I'm going to limit the guest access to only 100 meg download and only 15 meg upload, and we'll save that. Now, here's the connective tissue that ties all this together. Let's create a new wireless network for a guest user. They'll have a different SSID, and when they join that SSID, they're going to be part of that guest user group and they're going to be part of VLAN 2. Let's create a new wireless network. And this wireless network will be called RAYGUEST and notice that we're open by default when it comes to our authentication. That's probably not what we want. We want to have some password required. And we already talked about how WEP is very not secure and we probably want to use something like WPA, WP2 specifically. We're not going to use the enterprise option because that implies we're using a radius server. Personal is what we're going to do. That's going to be a pre-shared key. And I'll give the pre-shared key. And I'll say advanced options, and I'll say that I want to use VLAN number two and we want to use user group GUEST and we will save that. That has given us a separate wireless network that's going to show up our mobile devices and we can instruct our guests to get on the RAYGUEST network and give them the password, and they're going to have limited access to bandwidth and they're going to be in their own broadcast domain. So in this video, we've talked about how to set up a guest network and how to add wireless network security

**Review and next steps :**

- Now that you've completed the Wireless Networking Essentials course, which gave you a very focused look at one aspect of networking, a great next step for you would be to take my upcoming Networking Basics course. In fact, that course may already be out by time you watch this. And in that Networking Basics course, you're going to get more of a sampler platter of different networking technologies. But in the mean time, I invite you to follow me on my YouTube channel at YouTube.com/kwallaceccie to see new free videos as I come out with those. You could also listen to my podcast. It's called the Broadcast Storm. You can search for that on Spotify, or for Apple devices you can go to kwtrain.com/podcast. And for now, I want to give you a huge congratulations on completing this course, and a sincere thank you for entrusting me with your time. I hope to see you in another training course very soon.