6

Wireless Lans I

Learning Objectives

By the end of this chapter, you should be able to:

* Explain basic Wi-Fi 802.11 terminology and access point connections.
* Explain basic radio signal propagation concepts, including frequencies, antennas, and wireless propagation problems. These are physical layer concepts.
* Explain the frequency spectrum, service bands, channels, bandwidth, licensed versus unlicensed service bands, and the type of spread spectrum transmission used in 802.11 Wi-Fi LANs. These are physical layer concepts.
* Describe 802.11 Wi-Fi WLAN operation with access points and a switched Ethernet distribution system to link the access points. Distinguish between BSSs, ESSs, and SSIDs. Discuss communication between access points. These are data link layer concepts.
* If you read the box, compare the CSMA/CA+ACK and RTS/CTS media access control disciplines. These are data link layer concepts.
* Compare and contrast the 802.11n, and 802.11ac transmission standards. Discuss emerging trends in 802.11 operation, including channels with much wider bandwidth, MIMO, beamforming, and multiuser MIMO. These are physical layer concepts.

# Introduction

## OSI Standards

In Chapter 5, we looked at wired switched Ethernet networks. Technologies for these wired switched Ethernet networks require both physical and data link layer standards. Consequently, they use OSI standards. In this chapter and in Chapter 7, we will look at wireless LANs. Like wired LANs, wireless LANs are also single networks, which require physical and DLL standards. They too use OSI standards.

Figure 6-1: 802.11 / Wi-Fi Wireless LAN (WLAN) Technology (Study Figure)

Wireless LANs

Require standards at the physical and data link layer

So OSI standards

Standards are actually created by the IEEE 802.11 working group

Wi-Fi

Certification system managed by the Wi-Fi Alliance

Wi-Fi is now synonymous for 802.11

Test Your Understanding

1. a) At what layers do wireless LANs operate? b) Do wireless LAN standards come from OSI or TCP/IP? Explain.

## 802.11 = Wi-Fi

Having discussed wireless transmission briefly, we will look at wireless networking’s widest application, wireless local area networks. Wireless LANs (WLANs) use radio for physical layer transmission on the customer premises.

Wireless LANs (WLANs) use radio for physical layer transmission on the customer premises.

In the last chapter, we saw that the 802.3 Working Group of the IEEE’s 802 LAN/MAN Standards Committee creates Ethernet standards. Other working groups create other standards. The dominant WLAN standards today are the 802.11 standards, which are created by the IEEE 802.11 Working Group.

It is common to call the 802.11 standards “Wi-Fi” standards. In fact, the terms have become almost interchangeable, and we will use them that way in this book. However, as an IT professional, you should understand the technical difference between 802.11 and Wi-Fi. The term Wi-Fi stems from the Wi-Fi Alliance, which is an industry consortium of 802.11 product vendors. When the 802.11 Working Group creates standards, it often creates many options. The Wi-Fi Alliance creates subsets of 802.11 standards with selected options. The Alliance conducts interoperability tests among products that claim to meet these “profiles.” Only products that pass interoperability tests may display the Wi-Fi Logo on their products. Products that do not pass are rarely sold, so when someone picks up a box containing an 802.11 product, they almost always see the Wi-Fi logo.

It is common to call the 802.11 standards “Wi-Fi” standards. In fact, the terms have become almost interchangeable, and we will use them that way in this book.

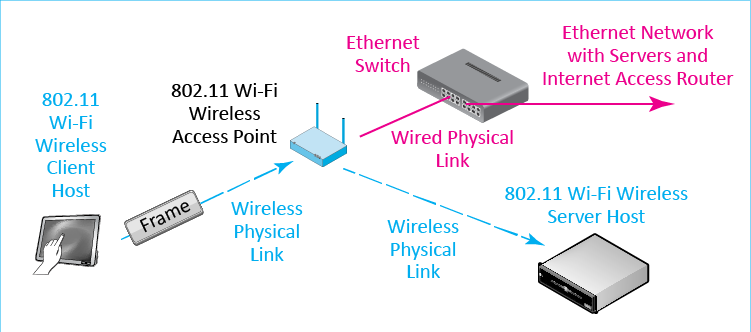
Test Your Understanding

2. a) Distinguish between 802.3 standards and 802.11 standards. b) Distinguish between 802.11 and Wi-Fi. c) How will this book use the two terms?

## Basic Access Point Operation

Figure 6-2 shows access point operation. The blue dashed arrows show what happens when a wireless host sends a frame to another wireless host that connects to the same access point. The source host transmits the frame to the access point. The access point then transmits the frame to the destination host. We show this interaction as pair of point-to-point transmissions.[[1]](#footnote-1),[[2]](#footnote-2)

Figure 6-2: Access Point Operation



In most situations, however, the client needs to connect to a server that is elsewhere, on the corporate Ethernet LAN or outside the organization on the Internet. To reach corporate servers and to reach the site’s Internet access router, the client needs to communicate over the corporate Ethernet LAN. As the solid arrows in the figure show, the access point connects via UTP to an Ethernet workgroup switch, which connects wireless client to the rest of the site network.

Test Your Understanding

3. a) In a wireless LAN, do two wireless hosts usually send frames directly to one another? Explain. b) Why does the access point connect to the Ethernet workgroup switch?

# Radio Signal Propagation

Chapter 5 discussed propagation effects in wired transmission media (UTP and optical fiber). Propagation effects in wired transmission can be well controlled by respecting cord distance limits and taking other installation precautions. This is possible because wired propagation is predictable. If you input a signal, you can estimate precisely what it will be at the other end of a cord. A wired network is like a faithful, obedient dog.

Propagation effects in wired transmission can be well controlled by respecting cord distance limits and taking other installation precautions.

In contrast, radio propagation is very unreliable. Radio signals bounce off obstacles, fail to pass through walls and filing cabinets, and have other problems we will look at in this section. Consequently, Wi-Fi networks, which use radio to deliver signals, are more complex to implement than wired networks. They do not have a few simple installation guidelines that can reduce propagation effects to nonissues. Therefore, we will spend more time on wireless propagation effects than we did on wired propagation effects.

Propagation effects in wireless networks are complex and difficult to implement.

Test Your Understanding

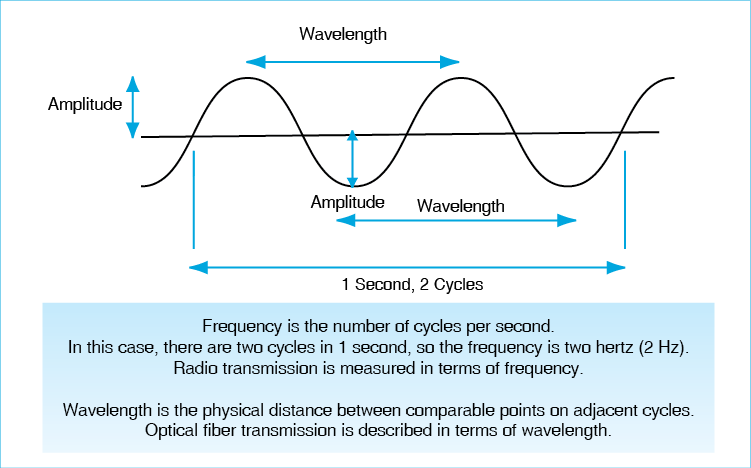
4. a) In 802.3 Ethernet networks, can simple installation rules usually reduce propagation effects to nonissues? b) In 802.11 Wi-Fi networks, can simple installation rules usually reduce propagation effects to nonissues?

## Frequencies

Radios for data transmission are called transceivers because they both transmit and receive. When transceivers send, their wireless signals propagate as waves, as we saw in Chapter 5. Figure 6-3 again notes that waves have amplitude and wavelength. While optical fiber waves are described in terms of wavelength, radio waves are described in terms of another wave characteristic, frequency.

Frequency is used to describe the radio waves used in WLANs.

Figure 6-3: Electromagnetic Wave



In waves, frequency is the number of complete cycles per second. One cycle per second is one hertz (Hz). Metric designations are used to describe frequencies. In the metric system, frequencies increase by a factor of 1,000 rather than 1,024. The most common radio frequencies for wireless transceivers range between about 500 megahertz (MHz) and 10 gigahertz (GHz).

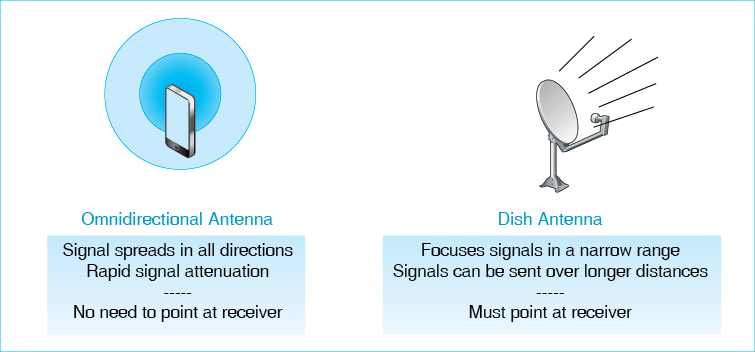
Test Your Understanding

5. a) What is a transceiver? b) Is wireless radio transmission usually expressed in terms of wavelength or frequency? c) What is a hertz? d) Convert 3.4 MHz to a number without a metric prefix. (The use of metric prefixes was discussed in a box in Chapter 1.) e) At what range of frequencies do most wireless systems operate?

## Antennas

A transceiver must have an antenna to transmit its signal. Figure 6-4 shows that there are two types of radio antennas: omnidirectional antennas and dish antennas.

Figure 6-4: Omnidirectional and Dish Antennas



• Omnidirectional antennas transmit signals equally strongly in all directions and receive incoming signals equally well from all directions. Consequently, the antenna does not need to point in the direction of the receiver. However, because the signal spreads in all three dimensions, only a small fraction of the energy transmitted by an omnidirectional antenna reaches the receiver. Omnidirectional antennas are best for short distances, such as those found in a wireless LAN or a cellular telephone network.

• Dish antennas, in contrast, point in a particular direction, which allows them to send stronger signals in that direction for the same power and to receive weaker incoming signals from that direction. (A dish antenna is like the reflector in a flashlight.) Dish antennas are good for longer distances because of their focusing ability, although users need to know the direction of the other radio. In addition, dish antennas are hard to use. (Imagine if you had to carry a dish with you whenever you carried your cellular phone. You would not even know where to point the dish!)

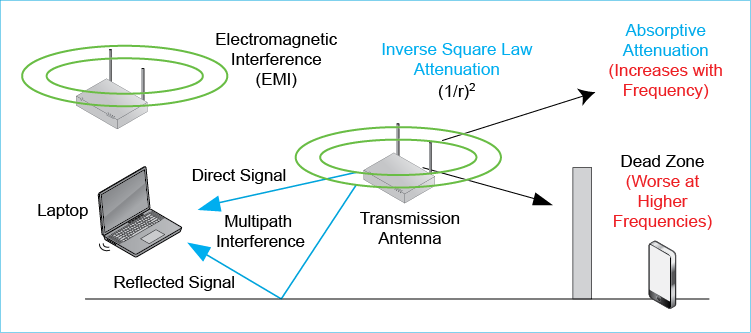
Test Your Understanding

6. a) Distinguish between omnidirectional and dish antennas in terms of operation. b) Under what circumstances would you use an omnidirectional antenna? c) Under what circumstances would you use a dish antenna? d) What type of antenna normally is used in WLANs? Why?

## Wireless Propagation Problems

We have already noted that, although wireless communication gives mobility, wireless transmission is not very predictable, and there often are serious propagation problems. Figure 6-5 illustrates five common wireless propagation problems.

Figure 6-5: Wireless Propagation Problems



Inverse Square Law Attenuation.  Compared to signals sent through wires and optical fiber, radio signals attenuate very rapidly. When a signal spreads out from any kind of antenna, its strength is spread over the area of a sphere. (In omnidirectional antennas, power is spread equally over the sphere, while in dish antennas, power is concentrated primarily in one direction on the sphere.)

The area of a sphere is proportional to the square of its radius, so signal strength in any direction weakens by an inverse square law rule. If distance is doubled, signal strength falls to a quarter of its original value. For example, if a signal is 100 watts at ten meters, it will only be 25 W at 20 meters. If the distance is increased ten-fold, then signal strength will be only 1/100 its original value or 1 Watt. This is very rapid attenuation and underscored why omnidirectional antennas are only used for short distances.

Figure 6-7: Inverse Square Law Attenuation (Study Figure)

|  |  |  |
| --- | --- | --- |
| Distance Ratio | Distance Ratio Squared | Signal Strength Ratio |
| 1 | 1 | 100.0% |
| 2 | 4 | 25.0% |
| 3 | 9 | 11.1% |
| 4 | 16 | 6.3% |
| 5 | 25 | 4.0% |
| 6 | 36 | 2.8% |
| 7 | 49 | 2.0% |
| 8 | 64 | 1.6% |
| 9 | 81 | 1.2% |
| 10 | 100 | 1.0% |

Note: if the original distance is 10 meters and the final distance is 30 meters, the distance ratio will be 3. The signal strength ratio will be 11.15%. If the original power at 10 meters is 100 watts, the signal at 30 meters will be 11.1 W.

Absorptive Attenuation.  As a radio signal travels, it is partially absorbed by the air molecules, plants, and other things it passes through. This absorptive attenuation is especially bad because water is an especially good absorber of radio signals. Rain and moisture in plants can reduce power substantially.

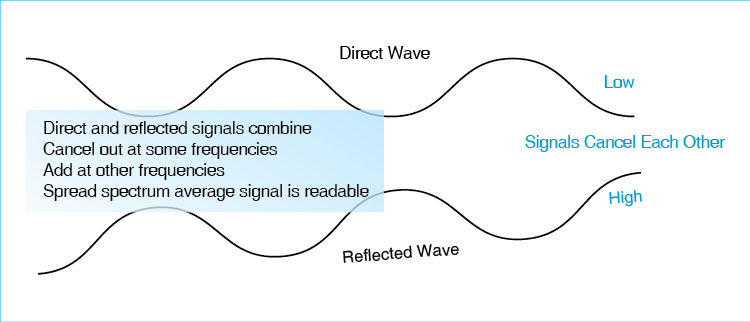
Absorptive attenuation can be confusing because we have already seen inverse square law attenuation. Yes, wireless propagation suffers from two forms of attenuation. Inverse square law attenuation is due to the signal spreading out as a sphere and so becoming weaker at each point on the sphere. Absorptive attenuation is signal loss through energy absorption.

Wireless transmission suffers from two forms of attenuation—inverse square law attenuation and absorptive attenuation.

Dead Zones.  To some extent, radio signals can go through and bend around objects. However, if there is a dense object (e.g., a thick wall) blocking the direct path between the sender and the receiver, the receiver may be in a dead zone, also called a shadow zone or dead spot. In these zones, the receiver cannot get the signal. If you have a mobile phone and often try to use it within buildings, you may be familiar with this problem.

Multipath Interference.  In addition, radio waves tend to bounce off walls, floors, ceilings, and other objects. As Figure 6-6 shows, this may mean that a receiver will receive two or more signals—a direct signal and one or more reflected signals. The direct and reflected signals will travel different distances and so may be out of phase when they reach the receiver. For example, one may be at its highest amplitude while the other is at its lowest, giving an average of zero. If their amplitudes are the same, they will completely cancel out. In real situation, multiple signals travelling different paths will interfere, so we call this type of interference multipath interference.

Figure 6-6: Multipath Interference



Multipath interference may cause the signal to range from strong to nonexistent within a few centimeters. If the difference in time between the direct and reflected signal is large, some reflected signals may even interfere with the next direct signal. Multipath interference is the most serious propagation problem at WLAN frequencies. We will see later that it is controlled by spread spectrum transmission.

Multipath interference is the most serious propagation problem at WLAN frequencies.

Electromagnetic Interference (EMI).  A final common propagation problem in wireless communication is electromagnetic interference (EMI). Many devices produce EMI at frequencies used in wireless data communications. Among these devices are cordless telephones, microwaves, and nearby access points. Consequently, placing access points so that they give good coverage without creating excessive mutual interference is difficult.

Frequency-Dependent Propagation Problems.  To complicate matters, two wireless propagation problems get worse as frequency increases.

• First, higher-frequency waves suffer more rapidly from absorptive attenuation than lower-frequency waves because they are absorbed more rapidly by moisture in the air. Consequently, as we will see in this chapter, WLAN signals around 5 GHz attenuate more rapidly than signals around 2.4 GHz.

• Second, dead zone problems grow worse with frequency. As frequency increases, radio waves become less able to go through and bend around objects.

Test Your Understanding

7. a) If you quadruple propagation distance, how much will signal intensity change at the receiver? b) If you increase propagation distance by a factor of 100, how much will signal intensity change at the receiver? c) If the signal strength from an omnidirectional radio source is 8 mW at 30 meters, how strong will it be at 150 meters, ignoring absorptive attenuation? Show your work. d) What will it be at 200 meters?

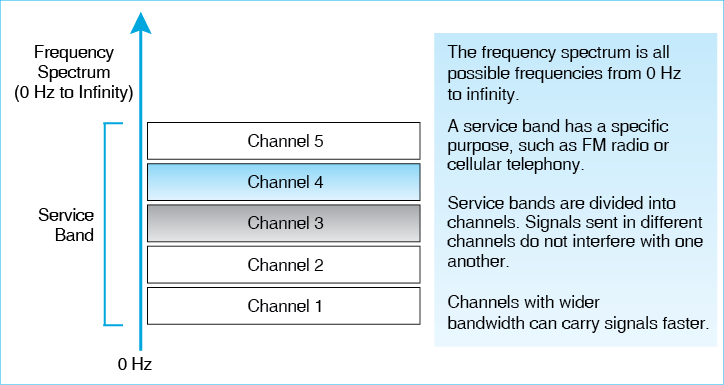
8. a) Contrast inverse square law attenuation and absorptive attenuation. b) How are dead zones created? c) What is the most serious propagation problem in WLANs? d) How is it controlled? e) List some sources of EMI. f) What two propagation problems become worse as frequency increases?

# Radio Bands, Bandwidth, and Spread Spectrum Transmission

## Service Bands

The Frequency Spectrum.  The frequency spectrum is the range of all possible frequencies from zero hertz to infinity, as Figure 6-7 shows.

Figure 6-7: The Frequency Spectrum, Service Bands, and Channels



Service Bands.  Regulators divide the frequency spectrum into contiguous spectrum ranges called service bands, which are dedicated to specific services. For instance, in the United States, the AM radio service band lies between 535 kHz and 1,705 kHz. The FM radio service band, in turn, lies between 87.5 MHz and 108.0 MHz. The 2.4 GHz service band that we will see later in this chapter extends from 2.4 GHz to 2.4835 GHz. There are also service bands for police and fire departments, amateur radio operators, communication satellites, and many other purposes.

Channels.  Service bands are subdivided further into smaller frequency ranges called channels. A different signal can be sent in each channel because signals in different channels do not interfere with one another. This is why you can receive different television channels successfully. In FM radio, channels are 200 kHz wide. So the first channel extends from 87.5 MHz to 88.5 MHz.

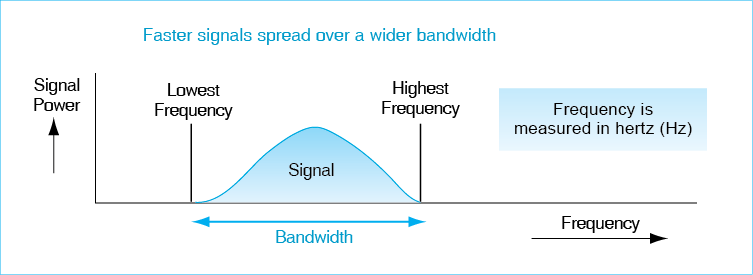
Test Your Understanding

9. a) Distinguish among the frequency spectrum, service bands, and channels. b) In radio, how can you send multiple signals without the signals interfering with one another? c) How many channels are there in the FM band?

## Signal and Channel Bandwidth

Figure 6-3 showed a wave operating at a single frequency. In contrast, Figure 6-8 shows that real signals do not operate at a single frequency. Rather, real signals spread over a range of frequencies. This range is called the signal’s bandwidth. Signal bandwidth is measured by subtracting the lowest frequency from the highest frequency.

Figure 6-8: Signal Bandwidth



A channel also has a bandwidth. For instance, if the lowest frequency of an FM channel is 89.0 MHz and the highest frequency is 89.2 MHz, then the channel bandwidth is 0.2 MHz (200 kHz). AM radio channels are 10 kHz wide, FM channels are 200 kHz wide, and television channels are 6 MHz wide. How wide must the channel bandwidth be? The channel bandwidth must be wide enough for a signal’s bandwidth.

Claude Shannon discovered a remarkable thing about signal transmission. A signal carrying X bits per second only needs half the bandwidth of a signal carrying 2X bits per second.[[3]](#footnote-3) Looked at the other way, if you want to transmit twice as many bits per second, you need to double your bandwidth. More generally, if you want to be able to transmit N times as fast, you need N times as much channel bandwidth. High bandwidth brings high radio transmission speed.

To transmit N times as fast, you need N times as much channel bandwidth.

Figure 6-9: Channel Bandwidth and Transmission Speed (Study Figure)

Signal Bandwidth

Figure 6-3 shows a wave operating at a single frequency

However, most signals are spread over a range of frequencies

The range between the highest and lowest frequencies is the signal’s bandwidth

The maximum possible transmission speed increases with bandwidth

Channel Bandwidth

Channel bandwidth is the highest frequency in a channel minus the lowest frequency

An 87.5 MHz to 88.1 MHz channel has a bandwidth of 0.2 MHz (200 kHz)

Channel bandwidth must be sufficient for the signal’s bandwidth

Channel Bandwidth and Propagation Speeds

Doubling the bandwidth doubles the maximum possible transmission speed

Multiplying the bandwidth by X multiplies the maximum possible speed by X

Higher-speed signals need wider channel bandwidths

Broadband Channels

Broadband means wide channel bandwidth and therefore high speed

Today, “broadband” has come to mean “fast,” whether or not radio transmission in channels is used.

Radio channels with large bandwidths are called broadband channels. They can carry data very quickly. Although the term broadband technically refers only to the width of a channel in radio, broadband has come to mean “fast,” whether or not radio is used.

Transmission systems that are very fast are usually called broadband systems even when they do not use radio channels.

Test Your Understanding

10. a) Does a signal usually travel at a single frequency, or does it spread over a range of frequencies? b) If the lowest frequency in a channel is 1.22 MHz and the highest frequency is 1.25 MHz, what is the channel bandwidth? (Use proper metric notation.) c) If you want to transmit seven times as fast, how much wider must the channel be? d) Why is large channel bandwidth desirable? e) What do we call a system whose channels are wide? f) What other types of system do we call broadband?

## Licensed and Unlicensed Service Bands

If two nearby transceivers send at the same frequency, their signals will interfere with each other. To prevent chaos, governments regulate how radio transmission is used. The International Telecommunications Union, which is a branch of the United Nations, creates worldwide rules that define service bands and specify how individual radio service bands are to be used. Individual countries enforce these rules but are given discretion over how to implement controls.

Figure 6-: Licensed and Unlicensed Radio Service Bands (Study Figure)

Licensed Radio Service Bands

If two nearby radio hosts transmit in the same channel, their signals will interfere

Most service bands are licensed bands, in which hosts need a license to transmit

The government limits licenses to reduce interference

Television bands, AM radio bands, etc. are licensed

In cellular telephone bands, which are licensed, only the central transceivers are licensed, not the mobile phones

Unlicensed Radio Service Bands

Some bands are set aside as unlicensed bands

Hosts do not need to be licensed to be turned on or moved

802.11 operates in unlicensed radio bands

This allows access points and hosts to be moved freely

However, there is no way to stop interference from other nearby users

Your only recourse is to negotiate with others

Licensed Service Bands.  In licensed service bands, transceivers must have a government license to operate. They also need a license change if they move. Commercial television bands are licensed bands, as are AM and FM radio bands. Government agencies control who may have licenses in these bands. By doing so, the government limits interference to an acceptable level. In some licensed service bands, the rules allow mobile hosts to move about while only central transceivers are regulated. This is the case for mobile telephones.

Unlicensed Service Bands.  However, for companies that have wireless access points and mobile computers, even the requirement to license central antennas (in this situation, access points) is an impossible burden. Consequently, the International Telecommunications Union has created a few unlicensed service bands. In these bands, a company can add or drop access points any time it chooses. It can also have as many wireless hosts as it wishes. All 802.11 Wi-Fi networks operate in these unlicensed radio bands.

The downside of unlicensed service bands is that companies must tolerate interference from others. If your neighbor sets up a wireless LAN next door to yours, you have no recourse but to negotiate with him or her over such matters as which channels each of you will use. At the same time, the law prohibits unreasonable interference by using illegally high transmission power.

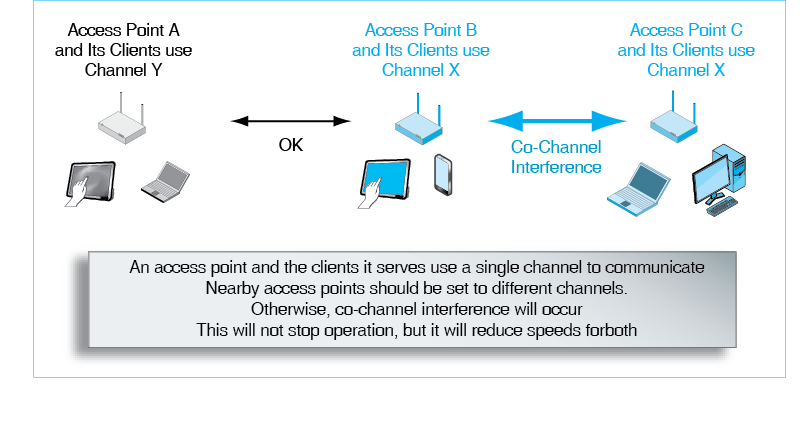
Test Your Understanding

11. a) Do WLANs today use licensed or unlicensed service bands? b) What is the advantage of using unlicensed service bands? c) What is the downside?

## Channel Use and Co-Channel Interference

Figure 6-11 illustrates two important points about how Wi-Fi uses its channels. The first is that an access point and all of the clients it serves communicate using a single channel, taking turns sending. In the figure, Access Point A is using “Channel Y,” while both Access Point B and Access Point C are using “Channel X.” (These are really numbers rather than letters, but letters are used to illustrate the principle.) The total number of channels in the service band is irrelevant to this communication because only one is used

Figure 6-: Channels and Co-Channel Interference in Wi-Fi



Adjacent Access Points B and C operate on the same channel, so their signals will interfere with each other. This is called co-channel interference because it only exists if nearby access points and clients are using the same channel. When co-channel interference occurs, it does not stop transmissions, but it does slow them down. One hotel decided to be “consistent” and put all access points on the same channel. Service was terrible.

The solution to reducing co-channel interference is placing nearby access points on different channels. However, there are a limited number of channels in the service bands that Wi-Fi uses, so if there are many nearby access points, some of them will inevitably suffer co-channel interference. In addition, channel bandwidths in newer standards are greater than those in earlier standards, so there will be fewer channels in each service band in the future. This will increase the co-channel interference problems unless service bands become much larger in the future. Reducing co-channel interference is an important goal in design.

## The 2.4 GHz and 5 GHz Unlicensed Service Bands

802.11 Wi-Fi WLANs today use two unlicensed service bands. One is the 2.4 GHz unlicensed band. The other is the 5 GHz unlicensed band.

Figure 6-12: The 2.4 GHz and 5 GHz Unlicensed Service Bands (Study Figure)

The 2.4 GHz Unlicensed Service Band

2.400 GHz to 2.485 GHz for the entire unlicensed service band

This is small total bandwidth

Difficult to put nearby access points on different channels

If not, there will be co-channel interference

802.11n will drop from 40 MHz channels to 20 MHz channels if there is interference

802.11ac channels are so big that they cannot fit in the 2.4 GHz unlicensed service band

The 5 GHz Unlicensed Service Band

Slightly shorter propagation distance because of higher frequencies

Deader dead zones because of higher frequencies

More bandwidth, although spread across multiple contiguous frequency ranges

Usually allows nearby access points to operate on non-overlapping channels

With increasingly wider channels, this ease of channel selection is declining.

The 2.4 GHZ Unlicensed Service Band.  The 2.4 GHz unlicensed service band is the same in most countries in the world, stretching from 2.4 GHz to 2.4835 GHz. Unfortunately, this is only 83.5 MHz of total service band bandwidth. Traditionally, each 802.11 channel was 20 MHz wide, although 40 MHz bandwidth channels were introduced in 802.11n. Furthermore, due to the way channels are allocated, there are only three possible non-overlapping 20 MHz 802.11 channels, which are centered at Channels 1, 6, and 11.[[4]](#footnote-4) In addition, if an 802.11n station finds itself in a crowded area, it will drop back from 40 MHz channels to 20 MHz channels to reduce interference. This will further reduce transmission speed.

The 5 GHZ Service Band.  Wi-Fi also operates in the 5 GHz unlicensed service band. The big advantage of the 5 GHz band is that it is far wider than the 2.4 GHz band. In contrast to the 2.4 GHz band’s mere three 20 MHz channels, the 5 GHz band provides between 11 and 24 non-overlapping 20 MHz channels today, depending on the country. This number of channels is going down as channels become wider, but it is still much greater than the number of channels in the 2.4 GHz service band.

Adding to the attractiveness of the 5 GHz unlicensed band, regulators in several countries have been expanding it to add more total bandwidth and therefore more channels. The United States added more bandwidth in 2003. In 2013, the Federal Communications Commission announced that it would add 35% more. In contrast, the 2.4 GHz band has no expansion potential because it is bordered by services that cannot be moved.

Test Your Understanding

12. a) In what two service bands does 802.11 operate? b) How many 20 MHz non-overlapping channels does the 2.4 GHz band support? c) Why is this a problem? d) Why are companies moving rapidly into the 5 GHz band? e) Why is it important that governments add more bandwidth to the 5 GHz band? f) If you triple channel bandwidth, what happens to the number of channels in the service band?

# Spread Spectrum Transmission

At the frequencies used by WLANs, there are numerous and severe propagation problems. In these service bands, regulators mandate the use of a form of transmission called spread spectrum transmission. Spread spectrum uses far wider channel bandwidth than the transmission speed requires.

Spread spectrum transmission uses far wider channel bandwidth than the transmission speed requires.

Figure 6-: Spread Spectrum Transmission (Study Figure)

Normal Radio Transmission

Uses only the channel bandwidth required to transmit a signal of a certain speed

This is conserves bandwidth to allow more channels

Spread Spectrum Wireless Transmission

Uses *much more* channel bandwidth than required by the transmission Speed

This is wasteful but necessary

Spread spectrum transmission transmits signals redundantly across the channel bandwidth, so that if there are some transmission problems at some frequencies, the signal will still get through

Why?

Reduces transmission problems, especially multipath interference

NOT used for security in commercial WLANs

NOT used to increase transmission speed

## Normal versus Spread Spectrum Transmission

Regulators mandate the use of spread spectrum transmission to minimize propagation problems—especially multipath interference. (If the direct and reflected signals cancel out at some frequencies within the band, they will be double at other frequencies and will average out over a wide enough frequency range.) Spread spectrum transmission transmits signals redundantly across the channel bandwidth, so that if there are some transmission problems at some frequencies, the signal will still get through.

In wireless LANs, spread spectrum transmission is used to reduce propagation problems, not to provide security or higher transmission speed.

In commercial spread spectrum transmission, security is not a benefit. The military uses spread spectrum transmission for security, but it does so by keeping certain parameters of its spread spectrum transmission secret. Commercial spread spectrum transmission must make these parameters publicly known to allow parties to communicate easily.

Spread spectrum channels are much wider than normal channels. One might expect them to offer faster speeds as well. They do not.

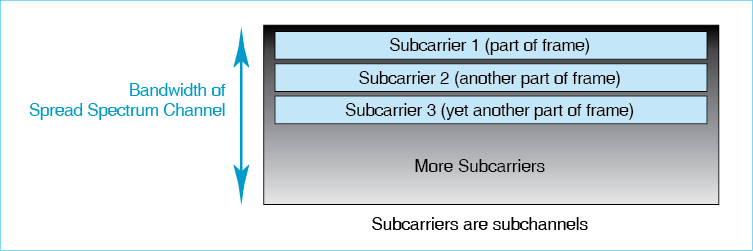
Test Your Understanding

13. a) In the 2.4 GHz and 5 GHz service bands, what type of transmission method is required by regulators? b) What is the benefit of spread spectrum transmission for business communication? c) Is spread spectrum transmission done for security reasons in commercial WLANs? d) Does spread spectrum transmission increase transmission speed.

## Orthogonal Frequency Division Multiplexing

There are several spread spectrum transmission methods. The 802.11 Working Group’s current standards all use orthogonal frequency division multiplexing (OFDM), which Figure 6-14 illustrates.

Figure 6-14: Orthogonal Frequency Division Multiplexing (OFDM)



In OFDM, each broadband channel is divided into many smaller subchannels called subcarriers. OFDM transmits part of a frame in each subcarrier. OFDM sends data redundantly across the subcarriers, so if there is impairment in one or even a few subcarriers, all of the frame will usually still get through.

Why use subcarriers instead of simply spreading the signal over the entire channel? The problem is that sending data over a very wide channel reliably is very difficult. It is much easier to send many slow signals in many small subcarriers.

Test Your Understanding

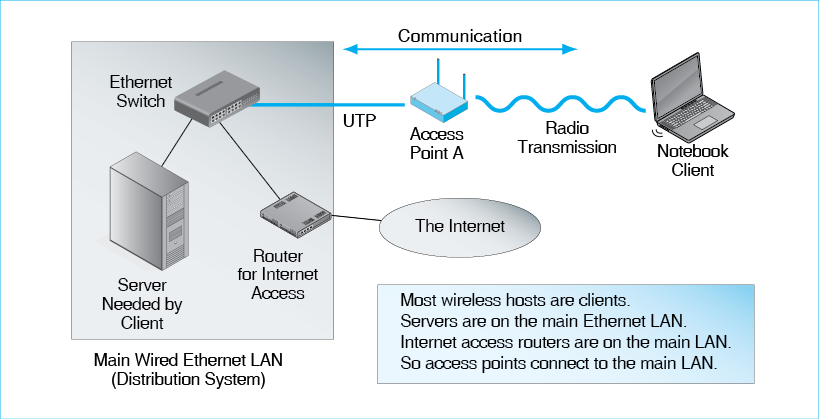
14. a) In normal radio operation, how does channel bandwidth relate to the bandwidth required to transmit a data stream of a given speed? b) How does this change in spread spectrum transmission? c) What spread spectrum transmission method dominates today? d) Why does it use subcarriers instead of simply spreading the data over the entire channel?

# 802.11 WLAN Operation

As Figure 6-15 shows, an 802.11 Wi-Fi LAN typically connects a mobile devices to a large wired Ethernet LAN rather than directly to each other. This is because most wireless devices are client hosts, and the servers and Internet access routers that mobile hosts need to use usually are on the wired LAN.[[5]](#footnote-5) In 802.11 terminology, the wired Ethernet LAN to which access points connect is a distribution system (DS).

The wired LAN to which access points connect is a distribution system (DS).

Figure 6-15: Typical 802.11 Wi-Fi Operation



Test Your Understanding

15. a) Why do most access points need to connect to Ethernet networks? b) In Figure 6-15, what is the distribution system?

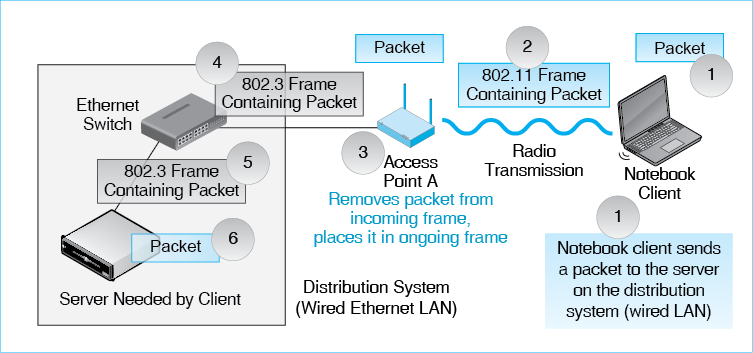
## Wireless Access Points

When a wireless host wishes to send a frame to a server, it transmits the frame to a wireless access point.

* As Figure 11-16 shows, when a wireless host transmits, it puts the packet in an 802.11 frame.[[6]](#footnote-6)
* Of course an 802.11 frame cannot travel over the 802.3 LAN. Wi-Fi has an entirely different frame organization, and Ethernet switches have no idea how to handle 802.11 frames.
* To address this problem, the access point removes the packet from the 802.11 frame and places the packet in an 802.3 Ethernet frame.
* The access point sends this 802.3 frame to Ethernet network, which delivers the frame to the server.
* Later, when the server replies, the wireless access point receives the 802.3 frame, removes the packet from the Ethernet frame, and forwards the packet to the wireless host in a Wi-Fi frame.[[7]](#footnote-7)

The packet goes all the way from the wireless host to a server. The 802.11 frame travels only between the wireless host and the wireless access point. The 802.3 frame travels only between the wireless access point and the server.

Figure 11-: Packet and Frame Transmission



Test Your Understanding

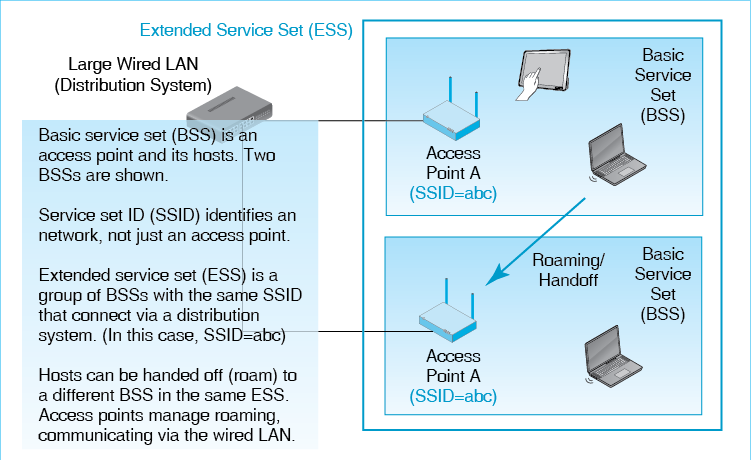
16. Why must an access point remove an arriving packet from the frame in which the packet arrives and place the packet in a different frame when it sends the packet back out?

## Basic Service Sets (BSSs)

We need to introduce a bit of jargon at this point. First, a basic service set (BSS) consists of an access point and the wireless hosts it serves. In Figure 6-17, there are two BSSs. The basic service set of Access Point A has two wireless hosts, while the BSS of Access Point B has one. Of course, most BSSs serve many more wireless hosts.

A basic service set (BSS) consists of an access point and the wireless hosts it serves

Figure 6-17: Basic Service Sets, Extended Service Set, Handoff, and Roaming



The access point in a BSS has an identifier called the service set identifier (SSID). (Note that the term basic is not in the name.) Wireless hosts must know the SSID to associate with the access point. Fortunately, this information is very easy to learn.[[8]](#footnote-8)

Test Your Understanding

17. a) What is a BSS? (Do not just spell out the acronym.) b) What is an SSID? (Do not just spell out the acronym.) c) Does the access point have an SSID? d) Why must wireless devices know the access point’s SSID?

## Extended Service Sets (ESSs), Handoffs, and Roaming

If a mobile host travels too far from a wireless access point, its signal will become too weak to reach the access point. However, if there is a closer access point, the host can be handed off to that access point for service. In WLANs, the ability to use handoffs is also called roaming.[[9]](#footnote-9)

Roaming requires that both access points belong to the same extended service set. An extended service set (ESS) is a group of BSSs 1) that are connected to the same distribution system and 2) in which all access points have the same SSID. In roaming, the two access points involved have to coordinate the handoff. They do this by communicating over the distribution system.

An extended service set (ESS) is a group of BSSs 1) that are connected to the same distribution system and 2) in which all access points have the same SSID.

Access points also need to contact one another via the distribution system.

Test Your Understanding

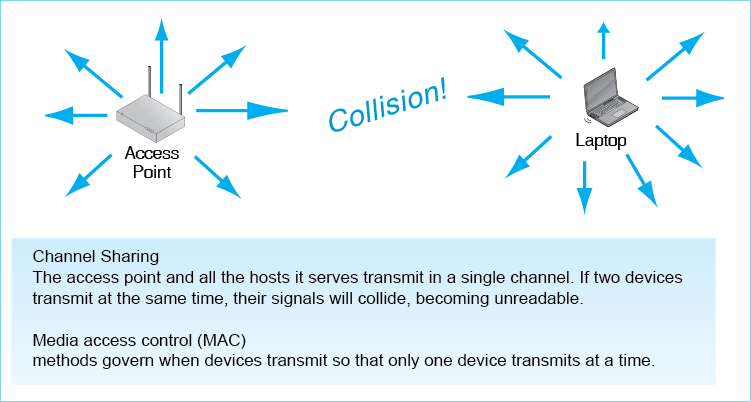
18. a) What is a handoff in 802.11? b) What is an ESS? (Do not just spell out the abbreviation.) c) What characteristics do all access points in an ESS share? d) How can access points communicate with each other to accomplish roaming?

## Media Access Control

The access point and all of the wireless hosts it serves transmit and receive in a single channel. Figure 6-18 shows that if two devices transmit in the same channel at the same time, their signals will interfere with each other. This is called a collision. It makes both signals unreadable. When a wireless host or the access point transmits, all other devices must wait. As the number of hosts served by an access point increases, individual throughput falls because of this waiting. The box “Media Access Control” discusses how media access control (MAC) methods govern when hosts and access points may transmit so that collisions are avoided.[[10]](#footnote-10)

Media access control (MAC) methods govern when hosts and access points may transmit so that collisions can be avoided.

Figure 6-18: Hosts and Access Points Transmit on a Single Channel



The access point and all of the wireless hosts it serves transmit and receive in a single channel. When a wireless host or the access point transmits, all other devices must wait.

Test Your Understanding

19. All wireless hosts and the access point that serves them transmit on the same channel. a) What problem does this cause? b) How does media access control address this problem? c) Does media access control apply to wireless hosts, access points, or both?

# Box: Media Access Control (MAC)

The 802.11 standard has two mechanisms for media access control. The first, CSMA/CA+ACK, is mandatory. Access points and wireless hosts must support it. The second, RTS/CTS, is optional.[[11]](#footnote-11)

## CSMA/CA+ACK Media Access Control

The mandatory method is Carrier Sense Multiple Access with Collision Avoidance and Acknowledgement, which is mercifully shortened to CSMA/CA+ACK.

Figure 6-19: CSMA/CA+ACK Media Access Control

CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)

Sender listens for traffic

Carrier is the signal; sensing is listening

1. If there is traffic, waits

2. If there is no traffic:

2a. If there has been no traffic for less than the critical time value, waits a random amount of time, then returns to Step 1.

2b, If there has been no traffic for more than the critical value for time, sends without waiting

This avoids collision that would result if hosts could transmit as soon as one host finishes transmitting.

ACK (Acknowledgement)

Receiver immediately sends back an acknowledgement

If sender does not receive the acknowledgement, retransmits using CSMA

CSMA/CA plus ACK is a reliable protocol

Carrier sense (CS) means to listen to (sense) traffic (the carrier, in radio parlance). Multiple access (MA) means that this method uses listening to control how multiple hosts can access the network to transmit. Quite simply, if another device is transmitting, the wireless host or access point does not transmit.

Collision avoidance (CA) means that the method attempts to avoid two devices transmitting at the same time. Most obviously, if one device has been sending for some time, two or more others may be waiting to send. If they both send as soon as the current sender stops, they will both transmit at the same time. This will cause a collision. Collision avoidance adds a random delay time to decide which device may transmit first. This works, but it is inefficient because it adds dead time when no one is transmitting.

ACK means that if the receiver receives a message correctly, it immediately sends an acknowledgment to the sender, not waiting at all. This is another reason to require stations to delay before sending when a sender stops transmitting.

If the sender does not receive an ACK, it retransmits the frame. Sending acknowledgments and retransmissions makes 802.11 Wi-Fi transmission reliable because it provides both error detection and error correction. CSMA/CA+ACK is the only reliable transmission method we will see in this book other than TCP. Most early DLL protocols were reliable because transmission then was unreliable, even in wired networks. Under these circumstances, error correction at the data link layer made sense. This is no longer true today generally. Wired transmission protocols such as Ethernet are unreliable. Doing error correction is simply not worth the effort when transmission errors are rare. We have seen that wireless transmission, however, is encumbered with propagation problems, and lost or damaged frames are far too common. It makes sense under these conditions to make 802.11 (and many other wireless protocols) reliable.

Thanks to CSMA/CA+ACK, 802.11 is a reliable protocol.

CSMA/CA+ACK works well, but it is inefficient. Waiting before transmission wastes valuable time. Sending ACKs also is time consuming. Overall, an 802.11 LAN can only deliver throughput (actual speed) of about half the rated speed of its standard—that is, the speed published in the standard.

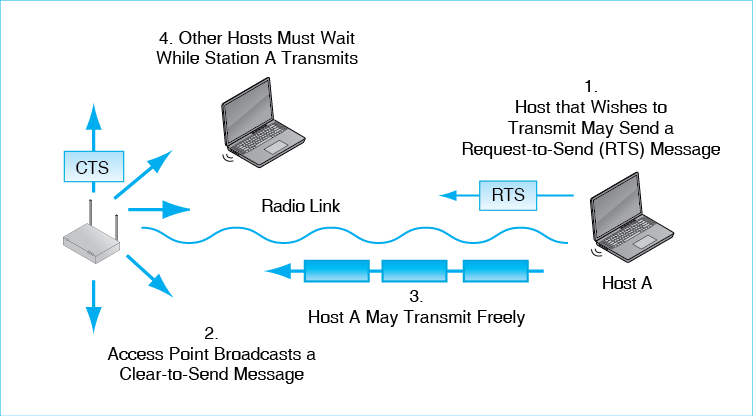
Test Your Understanding

20. a) What does CS mean? (Do not just spell out the abbreviation.) b) How is carrier sensing used in multiple access? c) Why is CA desirable? d) Does a frame’s receiver transmit an ACK immediately or after a random delay? e) Is CSMA/CA+ACK reliable or unreliable? f) Why was 802.11 made reliable? g) Is CSMA/CA+ACK efficient?

## Request to Send/Clear to Send (RTS /CTS)

Although CSMA/CA+ACK is mandatory, there is another control mechanism called request to send/clear to send (RTS/CTS). Figure 6-20 illustrates RTS/CTS. As noted earlier, the RTS/CTS protocol is optional. Avoiding RTS/CTS whenever possible is wise because RTS/CTS is much less efficient, and therefore slower, than CSMA/CA+ACK.

Figure 6-20: Request to Send/Clear to Send Media Access Control



* When a host wishes to send, the host may send a request-to-send (RTS) message to the wireless access point. This message asks the access point for permission to send messages.
* If the access point responds by broadcasting a clear-to-send (CTS) message, then other hosts must wait. The host sending the RTS may then transmit, ignoring CSMA/CA.

Although RTS/CTS is widely used, keep in mind that it is only an option, while CSMA/CA is mandatory. Also, tests have shown that RTS/CTS reduces throughput when it is used even compared to CSMA/CA.

RTS/CTS makes sense primarily when two wireless clients can both hear the access point but cannot hear each other. With CSMA/CA+ACK, the two stations may transmit at the same time. RTS/CTS eliminates this.

Test Your Understanding

21. a) Describe RTS/CTS. b) Is CSMA/CA+ACK required or optional? c) Is RTS/CTS required or optional? d) Which is more efficient, RTS/CTS or CSMA/CA+ACK? e) When does it make sense to use RTS/CTS?

# 802.11 Transmission Standards

The 802.11 Working Group has created several WLAN transmission standards since 1997. We will look at the two most important of these standards today, 802.11n and 802.11ac. Sometimes, access points also have to deal with stations communicating with the older 802.11g standard in the 2.4 GHz band and the even older 802.11a standard in the 5 GHz band.

## Speed and Market Status

Figure 6-21 compares the 802.11n and 802.11ac standards. 802.11n products deliver speeds of 100 to 600 Mbps. The newer 802.11ac standard delivers far higher rated speeds of 433 Mbps to 6.9 Gbps. 802.11n dominates the installed base today, while 802.11ac dominates sales and will supplant 802.11n as the dominant Wi-Fi technology in the near future

Figure 6-21: Characteristics of Major 802.11 Wi-Fi Standards

|  |  |  |
| --- | --- | --- |
| **Characteristic** | **802.11n Dual Band** | **802.11ac** |
| Rated Speed | 100 Mbps to 600 Mbps. | 433 Mbps to 6.9 Gbps. |
| Status | Dominates the Installed Base | Dominates Sales |
| Unlicensed Band(s) | 2.4 GHz and 5 GHz | 5 GHz |
| Channel bandwidth | 40 MHz, but will drop back to 20 MHz if there is interference with older 20 MHz standards | 80 MHz or 160 MHz |
| Number of Non-overlapping Channels (varies by country) | 3 in 2.4 GHz band; 12 in the United States in 5 GHz band | 6 at 80 MHz channel bandwidth and 3 at 160 MHz bandwidth in the United States in the 5 MHz band. |
| Maximum MIMO spatial streams | 4 | 8 |
| Multi-User MIMO / Beamforming? | No. | Yes. |

Test Your Understanding

22. a) Compare the rated speed of 802.11n and 802.11ac. b) Compare the market statuses of 802.11n and 802.11ac.

## Channel Bandwidths and Numbers of Channels

802.11n Channel Bandwidth.  The 802.11n standard can operate in both the 2.4 GHz band and the less-crowded and wider 5 GHz band. It also doubles 802.11g bandwidth, raising it to 40 MHz. This alone roughly doubles speed. However, to be a good neighbor, when there are stations operating on the three possible 20 MHz channels, 802.11n products will drop back to a 20 MHz channel bandwidth, losing their channel bandwidth advantage.

802.11n also operates in the 5 GHz band, in which 40 MHz channels are widely available. However, that 802.11n can only use eight to twelve 40 MHz channels in the 5 GHz band in the United States.

802.11ac Channel Bandwidth.  The 802.11ac standard operates only in the 5 GHz band and has even wider channels than 802.11n. Support for 80 MHz channels is mandatory, and 160 MHz channels are optional. Doubling and quadrupling channel bandwidth compared to 802.11n means roughly a doubling and quadrupling of transmission speeds, other things being equal. Of course, having wider channels means having fewer channels, and the filling of available ranges with 80 MHz and 160 MHz channels is even harder than with 40 MHz channels. There are only 4–6 channels at 80 MHz and 1–2 channels at 160 MHz.[[12]](#footnote-12)

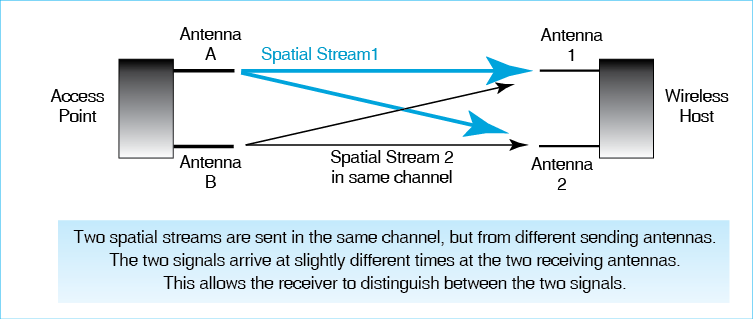
Test Your Understanding

23. a) Why is wider channel bandwidth good? b) What is the downside of wider channel bandwidth? c) What frequency band or bands do 802.11n and 802.11ac use? d) For each, compare channel bandwidth and the number of possible channels.

## MIMO

Increasing bandwidth is the easiest way to boost transmission speed, but there is also a more elegant way to increase speed without increasing bandwidth. Figure 6-22 notes that standards beyond 802.11g use a technique called multiple input/multiple output (MIMO) to double, triple, or quadruple transmission speed (or even increase it more) without increasing channel bandwidth.

Figure 6-22: Multiple Input/Multiple Output (MIMO) Operation



The key to higher throughput in MIMO is that the host or access point sends two or more spatial streams (radio signals) in the same channel between two or more different antennas on access points and wireless hosts. Earlier, we said that that was impossible. That was a bit of a lie, actually. It used to be impossible, but newer technology has made this possible.

In the figure, there are two spatial streams. As we saw earlier in this chapter, two signals in the same channel should interfere with each other. However, the two spatial streams sent by different antennas will arrive at the two receiving antennas at slightly different times. Using detection and separation methods based on differences in arrival times for the two spatial streams, the receiver can separate the two spatial streams in the same channel and so can read them individually.

Even with only two spatial streams using two antennas each on the sender and receiver, MIMO can roughly double throughput. Using more antennas and therefore more spatial streams can increase throughput even more. MIMO is not limited to two spatial streams.

The 802.11n standard introduced MIMO to Wi-Fi. With two spatial streams, the rated speed in 802.11n with 40 MHz channels is 300 Mbps. Three spatial streams raise the rated speed to 450 Mbps, and four raise it to 600 Mbps. The 802.11n standard requires access points to support four spatial streams, although wireless hosts are only required to support two spatial streams. Typical speeds in 802.11n products today have rated speeds of 150 Mbps to 300 Mbps.

The 802.11ac standard, in addition to doubling or quadrupling channel bandwidth compared to 802.11n, doubles the number of possible spatial streams to eight. The standard offers 16 possible combinations of bandwidth (80 MHz or 160 MHz) and number of spatial streams (1 to 8). This creates a large number of possible rated speeds: 433 Mbps to 6.9 Mbps. Products today typically provide rated speeds of 433 Mbps to 1.3 Gbps, but speed is increasing rapidly.

Another benefit of MIMO, beyond greater transmission speed, is greater transmission range. Greater propagation distances may permit fewer access points to be installed, and this will lower equipment and installation cost.[[13]](#footnote-13)

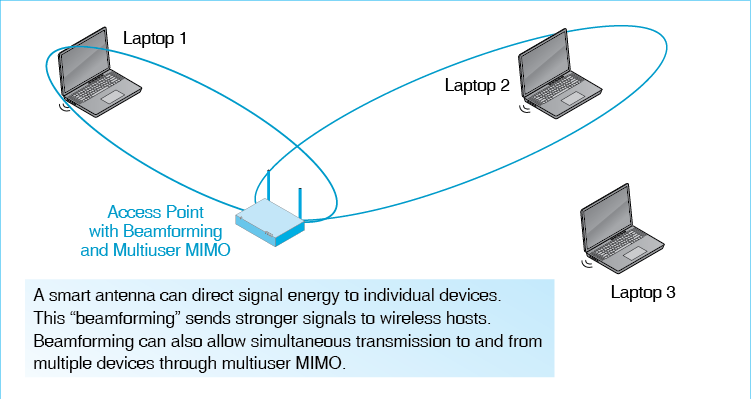
Test Your Understanding

24. a) How does MIMO use spatial streams to increase transmission speed? b) What is the main benefit of MIMO? c) What is its other benefit? d) Compare the range of rated speeds possible with 802.11n and 802.11ac.

## Beamforming and Multiuser MIMO

Today, jet fighters use phased array radar systems that are flat dishes with many tiny antennas spread over the surface. Controlling the relative phases of the signals from these antennas can focus the radar beam in a particular direction very rapidly. The antennas on advanced MIMO systems can do the same, focusing the radio power instead of broadcasting it isotropically (in all directions equally). Figure 6-23 illustrates this focusing, which is called beamforming.

Figure 6-23: Beamforming and Multiuser MIMO



Obviously, beamforming means that when the access points transmits to (or receives from) a wireless device the signal will be stronger. The radio can operate at lower power or send the signal farther.

Beamforming also allows multiuser MIMO (MU-MIMO), in which the access point focuses on two wireless devices at the same time. With focused transmissions, it can communicate with two or more devices simultaneously. This eliminates the time a device may have to wait before transmitting in order to avoid collisions.

Test Your Understanding

25. a) What is beamforming? b) What benefits can it bring? c) Distinguish between MIMO and multiuser MIMO.

# Conclusion

## Synopsis

Chapter 5 looked at Ethernet switched local area networks. This chapter and Chapter 7 look at wireless LANs (WLANs). All single networks, whether point-to-point, switched, or wireless, operate at Layers 1 and 2. OSI standards dominate at those layers, so we can expect wireless network standards to be OSI standards. The most widely used WLAN standard, 802.11 is widely called Wi-Fi.

This chapter focuses extensively on physical layer propagation. This detail is needed because wireless propagation effects are complex. We can predict what will happen as a signal travels down a copper wire or an optical fiber, but predicting how strong a radio signal will be at a user’s location is far more difficult. We looked at five wireless propagation problems: absorptive attenuation, inverse square law attenuation (yes, there are two types of attenuation), interference, dead zones, and multipath interference. Multipath interference is the biggest propagation problem in wireless LANs. Absorptive attenuation and dead zones become worse at higher frequencies.

Wireless LANs use omnidirectional antennas because users would not know where to point a dish antenna and certainly do not want to carry a dish around. Fixed users may use dishes pointing at a distant radio source to have stronger transmission and reception.

The frequency spectrum consists of all frequencies from 0 Hz to infinity. (Radio propagation is described by frequency, which is measured in hertz.) Service bands are (usually) contiguous ranges of the frequency spectrum that are reserved for particular purposes, such as FM radio, television, or police communication. Service bands are divided into channels. Signals are sent in a single channel, and signals in different channels do not interfere with each other. Most commercial wireless services and corporate WLANs operate between 500 MHz and 10 GHz.

Radio signals do not propagate at a single frequency. They spread over a range of frequencies, and the spread increases as signal speed increases. Consequently, to carry fast signals, channels must have wide bandwidths. Doubling bandwidth should double possible signal speed.

Wireless LANs operate in unlicensed bands, in which you can set up your network the way you wish. However, you must tolerate interference from nearby WLANs built by others.

Initially, almost all WLAN technology operated in the 2.4 GHz band, in which radio prices were low. However, there are only three non-overlapping 20 MHz channels in this band, so nearby access points often interfere with one another. Increasingly, new WLAN equipment operates in the 5 GHz unlicensed band, in which there are more channels for a given channel bandwidth. The gap between 2.4 GHz prices and 5 GHz prices is narrowing. Consequently, the use of the 5 GHz band is growing rapidly.

In the 2.4 GHz and 5 GHz bands, the government requires the use of spread spectrum transmission, in which the signal is spread far more than it needs to be for its speed. Current 802.11 Wi-Fi standards use orthogonal frequency division multiplexing (OFDM), in which the channel is broken into much smaller subchannels called subcarriers. The frame is transmitted redundantly within the subcarriers. WLAN spread spectrum techniques, unlike military spread spectrum techniques, provide no security.

In 802.11 WLAN operation, access points normally attach to the firm’s main wired Ethernet LAN so that wireless clients can access servers and Internet access routers on the wired LAN. When a wireless host transmits, it sends its packet in an 802.11 frame. The access point removes the packet from the 802.11 frame, puts it in an 802.3 frame, and sends the frame to the server or Internet access router. The packet travels all the way; the 802.11 frame does not. A basic service set (BSS) consists of an access point and the wireless hosts it serves. The SSID is the name of a radio on an access point. In an extended service set (ESS), all access points have the same SSID. Among other things, this permits roaming, which is also called being handed off.

The access point and the stations it serves all transmit in a single channel. Media access control (MAC) ensures that they take turns transmitting so that their signals do not interfere. In a box, we looked at 802.11 Wi-Fi’s two MAC protocols. CSMA/CA+ACK is mandatory. Request to send/clear to send is optional but sometimes useful. Both create inefficiency by creating dead time in which there is no transmission.

WLAN products on the market follow different 802.11 standards. Figure 6-21 compares the two main 802.11 transmission standards in use and for sale today. One consistent theme for newer standards is the use of wider channel bandwidths, which brings higher speeds. Earlier standards used 20 MHz channels. The 802.11n standard doubles this (except when there is interference from older devices). The 802.11ac standard, in turn, uses 80 MHz and 160 MHz channels. Both 802.11n and 802.11ac can take advantage of the wider 5 GHz band’s far greater total bandwidth.

Another way to boost speed is MIMO, which uses multiple antennas on the sender and receiver. The signals sent by different antennas are called spatial streams. The sender can transmit multiple spatial streams in the same channel, and the receiver will be able to read them. Roughly speaking, transmission speed increases in proportion to the number of spatial streams. The 802.11g and 802.11a standards do not use MIMO. The 802.11n standard uses MIMO and can support up to four spatial streams. The 802.11ac standard can support up to eight.

The 802.11ac standard can also use beamforming, which directs signals to individual devices instead of broadcasting signals omnidirectionally. Beamforming increases distance by focusing more of the sender’s power on the receiver without using a dish antenna. A particularly sophisticated type of beamforming is multiuser MIMO, which allows multiple stations to communicate simultaneously with a single access point in a single channel. The access point can use their different spatial streams to separate their signals. If one station is sending, other stations do not have to wait to send.

In Chapter 7, we will continue to look at 802.11 wireless LANs, focusing on security and management. We will then look at other local wireless technologies, including Bluetooth.

## End-of-Chapter Questions

Thought Questions

6-1. A building is cube-shaped. It uses 16 access points, which are, on average, 10 meters apart from one another. The company wishes to reduce this to 8 meters. About how many 5 GHz access points would the company need for the building?

6-2. For the following subquestions, give your answer and explain your reasoning. a) Is multipath interference a Layer 1 or Layer 2 concern? b) Is media access control a Layer 1 or Layer 2 concern? c) Is MIMO a Layer 1 or Layer 2 concern? d) Are wireless propagation problems Layer 1 or Layer 2 concerns? e) Is 802.11ac a Layer 1 or Layer 2 standard?

Perspective Questions

6-3. What was the most surprising thing you learned in this chapter?

6-4. What was the most difficult part of this chapter for you?

[Figure 6-1: 802.11 / Wi-Fi Wireless LAN (WLAN) Technology (Study Figure) 2](#_Toc444272903)

[Figure 6-2: Access Point Operation 3](#_Toc444272904)

[Figure 6-3: Electromagnetic Wave 5](#_Toc444272905)

[Figure 6-4: Omnidirectional and Dish Antennas 6](#_Toc444272906)

[Figure 6-5: Wireless Propagation Problems 7](#_Toc444272907)

[Figure 6-6: Multipath Interference 9](#_Toc444272908)

[Figure 6-7: The Frequency Spectrum, Service Bands, and Channels 10](#_Toc444272909)

[Figure 6-8: Signal Bandwidth 11](#_Toc444272910)

[Figure 6-9: Channel Bandwidth and Transmission Speed (Study Figure) 12](#_Toc444272911)

[Figure 6-10: Licensed and Unlicensed Radio Bands (Study Figure) 13](#_Toc444272912)

[Figure 6-11: Channels and Co-Channel Interference in Wi-Fi 14](#_Toc444272913)

[Figure 6-12: The 2.4 GHz and 5 GHz Unlicensed Service Bands (Study Figure) 15](#_Toc444272914)

[Figure 6-13: Spread Spectrum Transmission (Study Figure) 16](#_Toc444272915)

[Figure 6-14: Orthogonal Frequency Division Multiplexing (OFDM) 17](#_Toc444272916)

[Figure 6-15: Typical 802.11 Wi-Fi Operation 18](#_Toc444272917)

[Figure 11-16: Packet and Frame Transmission 19](#_Toc444272918)

[Figure 6-17: Basic Service Sets, Extended Service Set, Handoff, and Roaming 20](#_Toc444272919)

[Figure 6-18: Hosts and Access Points Transmit on a Single Channel 22](#_Toc444272920)

[Figure 6-19: CSMA/CA+ACK Media Access Control 23](#_Toc444272921)

[Figure 6-20: Request to Send/Clear to Send Media Access Control 24](#_Toc444272922)

[Figure 6-21: Characteristics of Major 802.11 Wi-Fi Standards 25](#_Toc444272923)

[Figure 6-22: Multiple Input/Multiple Output (MIMO) Operation 27](#_Toc444272924)

[Figure 6-23: Beamforming and Multiuser MIMO 28](#_Toc444272925)

1. Actually, each broadcasts its signal, so the signal spreads in all directions from the transmitter. The arrows indicate that only the receiver, to which the frame is addresses. Pays attention to the frame. (Or at least should.) [↑](#footnote-ref-1)
2. This is what normally happens. However, it is possible for two hosts to transmit to each other directly. This is called Miracast. It is used for such applications as displaying your mobile phone’s screen on a nearby television set or printing to a wireless printer. [↑](#footnote-ref-2)
3. Speaking more precisely, Shannon also found that the signal-to-noise ratio (the ratio of single power to noise) also affects propagation speed. However, engineers find it far easier to increase speed by increasing bandwidth than by increasing the signal-to-noise ratio. [↑](#footnote-ref-3)
4. Channel numbers were defined for the 2.4 GHz band when channels were narrower. A 20 MHz 802.11 channel overlaps several initially defined channels. Channels 1, 6, and 11 operate in the 2.402 GHz to 2.422 GHz, 2.427 GHz to 2. 447 GHz, and 2.452 GHz to 2.472 GHz frequency ranges, respectively. Note that there are unused 5 MHz “guard bands” between the channels to prevent inter-channel interference. [↑](#footnote-ref-4)
5. There is a rarely used 802.11 *ad hoc mode*, in which no wireless access point is used. In ad hoc mode, computers communicate directly with other computers without using an access point. (In contrast, when an access point is used, this is called 802.11 infrastructure mode.) In addition, 802.11 can create point-to-point transmission over longer distances than 802.11 normally supports. This approach, which normally is used to connect nearby buildings, uses dish antennas. [↑](#footnote-ref-5)
6. 802.11 frames are much more complex than 802.3 Ethernet frames. Much of this complexity is needed to counter wireless propagation problems. [↑](#footnote-ref-6)
7. This sounds like what a router does. However, a router can connect any two single networks. Access points are limited to connecting 802.3 and 802.11 networks. [↑](#footnote-ref-7)
8. The access point also has an EUI-48 address. This is called the Basic Service Set ID (BSSID). This identifies a particular access point. In contrast, as the text notes, all access points in an ESS have the same SSID. [↑](#footnote-ref-8)
9. In cellular telephony, which we will see in Chapter 10, the terms *handoff* and *roaming* mean different things. [↑](#footnote-ref-9)
10. Yes, this is where the term MAC address comes from. Conceptually, Media Access Control is a sublayer of the data link layer. It applies to Ethernet, Wi-Fi, and other 802.11 standards. Addresses are defined at this layer so that all 802.11 standards use EUI-48 addresses. [↑](#footnote-ref-10)
11. Actually, if you have even a single host with older 802.11b equipment connected to an access point, RTS/CTS becomes mandatory. However, 802.11b wireless hosts are almost never encountered anymore. [↑](#footnote-ref-11)
12. The United States is currently in the process of adding about 35% more capacity to the 5 GHz band. Some of this will fill spaces between available ranges to give larger available ranges. This will add one or two 160 MHz channels, again depending on conditions. [↑](#footnote-ref-12)
13. When a station transmits, it modulates the signal for physical layer transmission. (Modulation is covered in Module B). The 802.11n standard’s best modulation method is 64 QAM. 802.11ac raises this to 256 QAM. This allows 802.11ac to send a third more bits per clock cycle as 802.1n (8 versus 6 bits per clock cycle). [↑](#footnote-ref-13)