4
Understanding Wireless Networking

Looking around my bedroom right now, I can see several devices that can connect to wireless networks: mobile phone, laptop, tablet, fitness watch, games console, and television. It seems each month some hitherto non-smart device develops wireless connectivity. As we move toward the ubiquitous use of wireless technologies, the ability to understand how to implement and configure a wireless network is a skill that is in greater demand.

This chapter will introduce you to current technologies in use, covering the various standards that are in common use today. We'll discuss topologies in use in wireless networks, allowing you to identify which best suits your needs. Given the broadcast nature of wireless, we'll finish this chapter by highlighting the importance of security to maintain data protection.

The following topics will be covered in this chapter:

- Wireless standards
- Wireless topologies
- Wireless security

Technical requirements

To complete the exercises in this chapter, you will require a computing device with access to the internet.

Understanding wireless standards

As networked technology has developed, it appears to have thrown off the shackles of cables to a great extent. Most endpoint user devices now come shipped with some form of wireless connectivity already built in, offering us information at our fingertips as we connect to various wireless hotspots on our travels, uttering our mantra to the waiter in the coffee shop, *what's the Wi-Fi password?* As these devices are from different manufacturers, there was a requirement for a specification to be created that all network devices would adhere to.

Wireless standards are a set of standards that allows devices from different manufacturers to communicate with each other. My focus in this section will be on the IEEE 802.11 wireless standards (or Wi-Fi). Although there are other wireless standards, such as IEEE 802.15 (Bluetooth) and IEEE 802.16 (WiMAX), these are not covered in the exam objectives.

In July 1990, the **Institute of Electrical and Electronics Engineers** (**IEEE**), announced that their 802 project was forming a working group to investigate and develop wireless standards. This working group was named 802.11. Over the years, the working group has created several wireless standards that are in operation in various environments, but we will only look at five of these.

I would like to discuss some terminology common to all of these standards before going into their various characteristics.

CSMA/CA

Wi-Fi is classed as a contention-based technology. All devices on the network are vying for the attention of the access point. The access method used in Wi-Fi networks is called **Carrier Sense Multiple Access/Collision Avoidance** (**CSMA/CA**). Let's break that down a bit to understand it better:

- **Carrier sense** means it *listens* to what is happening on the carrier, in this case, the airwaves.
- **Multiple access** simply means that the carrier is available to multiple devices.
- **Collision avoidance** means that there is a mechanism in place to avoid collisions.

With a wired connection, you can detect a collision; in a wireless network, you cannot, so you need to avoid it.

As can be seen in *Figure 4.1*, CSMA/CA follows a simple process of **Ready To Send/Clear To Send** (**RTS/CTS**):

1. The sending device listens out for any transmissions (carrier sense).
2. If no transmissions are heard, it sends an RTS message to the access point advising it has data that it wants to transmit.
3. If the access point is free, it will send a CTS message to the device. All other devices hear it and do not attempt to transmit for a period of time.
4. The sending device transmits the data:

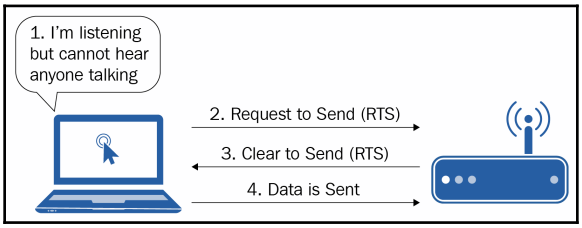

Figure 4.1: CSMA/CA process

You may be thinking, if the sender is listening to make sure the network is clear, why do we need to send an RTS message? I would like to draw your attention to *Figure 4.2*, which demonstrates what is known as the hidden station problem or hidden node problem:

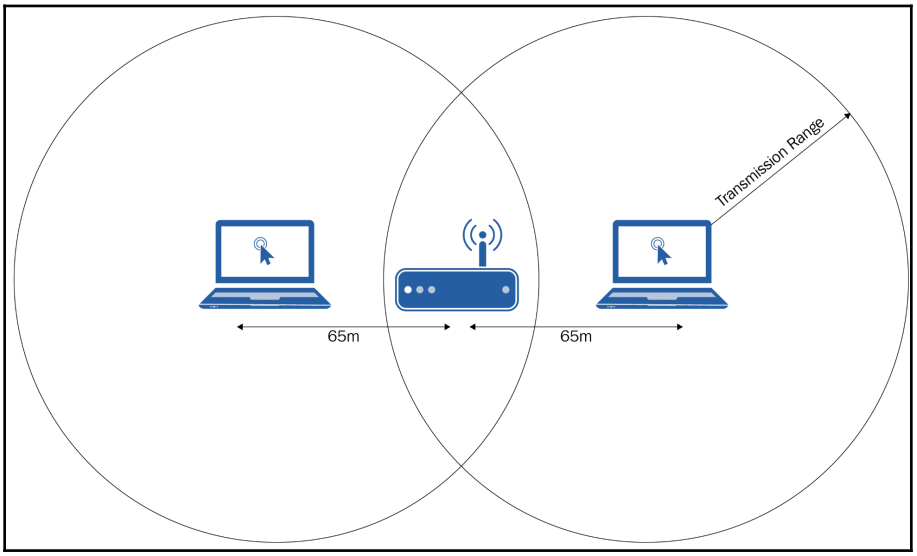

Figure 4.2: The hidden station problem

As you will read in the following sections, wireless networks can only transmit over a limited distance. In the preceding diagram, we can see that both laptops are 60 meters away from the wireless access point. Both devices are within range of the access point but are so far away from each other that they cannot hear when the other is talking to the access point. Because of this, when the device are listening to hear any device talking (*step 1* of CSMA/CA), they do not hear each other, and therefore send an RTS message. The access point will receive this but will not send a CTS message.

Radio waves

For this chapter, we will look at wireless communication through the use of radio waves, as opposed to light waves. Radio waves form part of the electromagnetic spectrum, and appear, as the name would suggest, in the radio frequency zone of the spectrum. These waves are generated by passing an alternating current through a conductor and transmitted out of an antenna as a waveform (*Figure 4.3*) or sine wave. Data is transmitted through these radio waves:

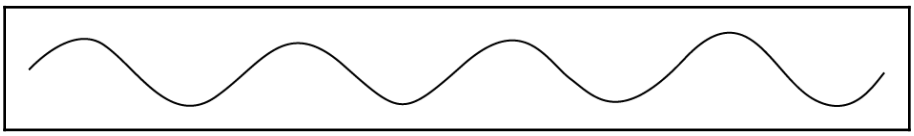

Figure 4.3: Waveform

How close each of the peaks of the waves are is dictated by the frequency, which is discussed in the following subsection.

Frequency

Frequency can be defined as the number of times a specific event occurs in a specified period of time. Looking at *Figure 4.4*, we can see that when the wave signal has returned to its starting point, it has completed a single RF signal cycle. Each cycle is measured in **hertz** (**Hz**):

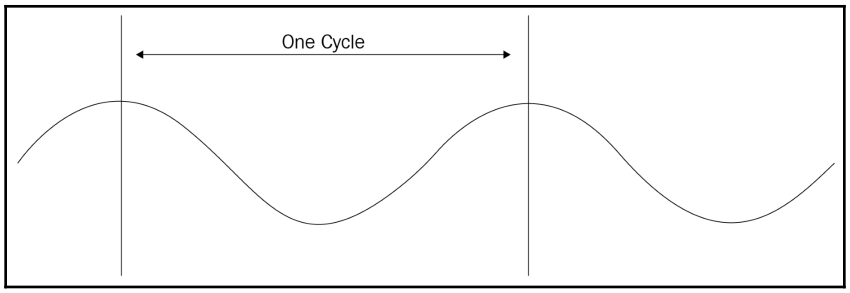

Figure 4.4: RF signal cycle

Frequency is defined by the number of cycles it completes in one second. One cycle per second is 1 Hz. *Figure 4.5* shows radio waves at two different frequencies. The top wave has a lower frequency (2 Hz) than the bottom wave, which is ~9 Hz. The higher the frequency, the more data can be transmitted per second. However, higher frequencies tend to have a shorter wavelength, which means that, over distance, the signal becomes too weak to be received:

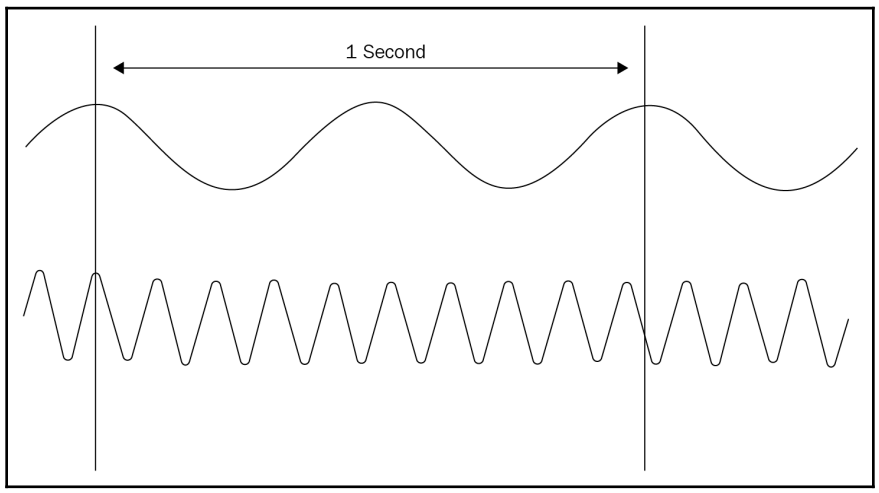

Figure 4.5: Two different frequencies

For ease of reference, as the number of hertz increases, we use a set of prefixes to identify the frequency:

- 1,000 Hz = 1 Kilohertz (1 KHz)
- 1,000 KHz = 1 Megahertz (1 MHz)
- 1,000 MHz = 1 Gigahertz (1 GHz)

The two most common frequencies used in Wi-Fi communication are the 2.4 GHz and 5 GHz ranges. Both of these are classed as unlicensed frequency ranges. Unlicensed means that anyone can use them without requiring a permit. The obvious advantage of this is avoiding every user of a wireless computing device seeking a license, but that advantage is a double-edged sword. Because anybody can use devices working within these ranges, there is an abundance of them out there, which can lead to unexpected **Radio Frequency Interference** (**RFI**). The 2.4 GHz range is particularly affected by this as baby monitors, microwave ovens, Bluetooth, radio-controlled toys, and so on all use this range.

The 2.4 GHz frequency band is broken down into up to 14 overlapping channels (*Figure 4.6*), each with a width of 22 MHz. In the US and Canada, there are 11 channels available; most of Europe has 13; and Japan has 14 channels available. These differences are due to regional legislation. Whenever you implement a wireless network, you ideally want to perform a site survey, in part, to see what channels are already in use by you or surrounding organizations.

You will look to see what channels are available to use and, where possible, spot an unused channel that does not overlap with any channels in use. Just looking at the channels available in *Figure 4.6*, you can see that channels **1**, **6**, and **11** do not overlap:

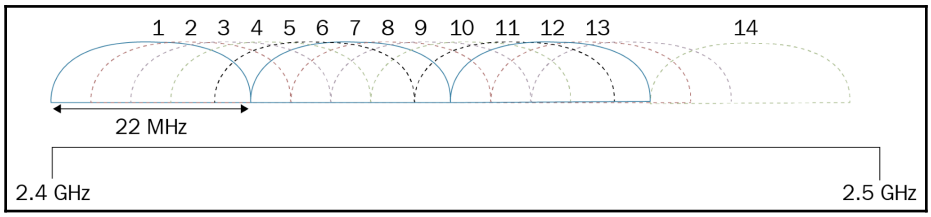

Figure 4.6: 2.4 GHz channels

However, if you look at the quick survey I have carried out on my laptop at home (*Figure 4.7*), you will see, in the bottom graph, that there is a lot of overlap going on. There are a couple of reasons for this.

First, I have no control over the wireless access points, so I am reliant on my neighbors being tech-savvy enough to check and configure the channels they are using. Second, most modern wireless access points will configure the channel used automatically, and select the channel least used:

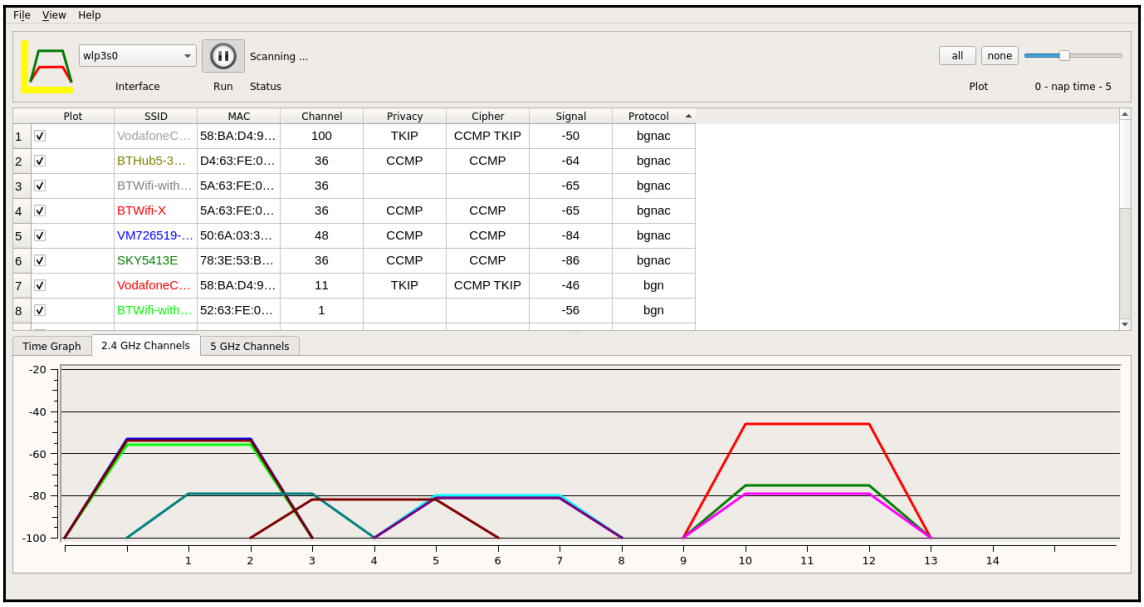

Figure 4.7: Overlapping 2.4 GHz channels

Although channels **2**, **7**, and **12** do not overlap either, it is unlikely you will need to think about these as channel **12** is not available in the US and Canada.

The 5 GHz frequency range, at one point, was less saturated with devices than its 2.4 GHz counterpart. However, as more devices embraced standards that supported this range, this is becoming less the case. Like the 2.4 Hz range, the 5 GHz range is split into channels, however, they are non-overlapping and there are 23 of them of 20 MHz each. Any devices that support both frequencies are referred to as dual-band.

The realms of frequencies can easily become quite complex, however, the exam does not go into any great detail. Remember that, for two devices to communicate, they need to be on the same frequency, and for better performance with 2.4 GHz devices, you utilize non-overlapping channels.

Modulation

The modulation of radio waves can be a very technical topic and goes well beyond the objectives of the exam. With that in mind, I would like to summarize its purpose here, and briefly mention it as we go through the various standards, as I feel it is relevant in the real world. Modulation can be simplified to mean a method of modifying the transmission of radio waves to increase efficiency. This modification can be applied to either the power (amplitude), frequency, or phase.

By modulating the power, you are increasing or decreasing the height of the sine wave; modulating the frequency involves changing the frequency in such a way that the peaks of the sine waves are nearer or further away from each other. The higher the frequency (the closer the waves are), the more data will be transmitted.

Phase modulation is one area that people struggle to get their heads around, usually because most materials discuss the signals being n^{o} out of phase of each other. In simpler terms, normally, signals are sent down at regular intervals; let's choose an arbitrary value here, and let's say that interval is every 4 seconds. If we are sending signals out of phase, we might send signal 1 at 0 seconds, signal 2 at 2 seconds, signal 3 at 4 seconds, and so on. If you have ever sung the song *row, row, row your boat*, where other people start the song when you are part of the way through it, those other singers are out of phase with you.

By modulating the signal, we are making more efficient use of the available bandwidth offered by the channel.

IEEE 802.11a

The 802.11a standard was released in September 1999 and supported devices using the 5 GHz range. In ideal conditions, this standard had a speed of 54 Mbps and had an indoor range of 35 m.

To make more efficient use of the available bandwidth, 802.11a utilized a modulation technology called **Orthogonal Frequency Distribution Multiplexing** (**OFDM**). This technique broke the 20 MHz channels used by this frequency range into 52 sub-carriers per channel. Each sub-carrier had a bandwidth of 312.5 KHz, and therefore had a lower data rate than a full channel. While this may seem counter-intuitive, it actually worked quite efficiently as the number of sub-carriers meant the overall data rate was better. An analogy may be beneficial here. Imagine you are driving a single car down a three-lane motorway, and no other cars are allowed to use it. The motorway itself is the channel. The single car is only using part of that channel. The other two lanes are sitting there unused and redundant. If, however, we split that motorway into lanes (the sub-carriers) and let other cars use the motorway, we can see that we are using it more efficiently. In essence, this is what OFDM facilitates.

IEEE 802.11b

Like IEEE 802.11a, the 802.11b standard was released in September 1999. However, this standard utilized the 2.4 GHz frequency range and therefore is not compatible with 802.11a. This disparity in frequency between the two standards meant that there was no compatibility between the devices in each of the standards. 802.11b has a maximum indoor range of 35 m.

For modulation, 802.11 uses a technique called **Direct Sequence Spread Spectrum** (**DSSS**). If a radio signal is corrupted in transit between devices for any reason, such as interference or a weak signal, then it would likely be discarded and the original transmission would have to be re-sent. This becomes more of an issue over distance or in areas of higher RFI. To overcome this obstacle, additional data would be transmitted that would allow for errors occurring in the transmission. On any network, data is transferred at a base level in bits. Each bit can be one of two values, `0` or `1`. When DSSS is used, rather than sending the data over as a single bit, a representative set of bit values is sent (known as **chips**). An example of this is as follows:

- `1` = `10101101`
- `0` = `01010010`

So, every time a device wants to send a bit with a value of `1`, it actually sends over a stream of bits: `10101101`. Again, this may seem counter-intuitive, however, if one of the bits in the stream is corrupted, then we can still calculate the original value of the bit being transmitted, hence avoiding having to re-transmit and use up bandwidth.

IEEE 802.11g

IEEE 802.11g was released in 2003 and was designed to enhance the technical capabilities of 802.11b and provide a speed of up to 54 Mbps. Like 802.11b, a frequency of 2.4 GHz was used, which meant that devices from both standards were able to communicate on the same network. This meant in the early days of 802.11g implementation, organizations did not necessarily have to replace all of their hardware at the same time. However, the downfall of mixing standards on a network was that the network could only go as fast as the slowest device. Therefore, a mixed network would likely reach 11 Mbps, which really defeated the object of having a faster standard. IEEE 802.11g had a maximum indoor range of 38 m.

For modulation, this standard uses a derivative of OFDM.

IEEE 802.11n

While previous iterations of the Wi-Fi standards marginally improved with each release, IEEE 802.11n really leaped forward. To begin with, it supported both 2.4 GHz and 5 GHz, therefore, devices supporting it were usually dual-band. It also introduced the concept of **Multiple-Input Multiple-Output** (**MIMO**) antennas. Simply put, 802.11n devices usually had multiple antennas. Of those, all of them could send or all of them could receive, or most likely you would have some antennas transmitting or some receiving. All of these antennas could be used for communication with one or other or multiple devices, and you could even have some antennas working on one frequency, while the remainder worked on the other frequency.

In addition to MIMO, 802.11n had a couple of other tricks up its sleeve. Firstly, it could combine two adjacent 20 MHz channels into one 40 MHz channel, in a process called **channel bonding**, effectively more than doubling the bandwidth (more than double due to less management overhead). Secondly, it could use a technique called **beamforming**. When an antenna transmits, the signal goes out equally in all directions (technically, it's more of a doughnut shape than a ball). However, with beamforming, the signal is more focused in a particular direction and therefore provides a stronger signal, reaching up to 70 m. By combining all of these techniques, 802.11n provides speeds of up to 600 Mbps (in total).

For modulation, this standard uses a derivative of OFDM.

IEEE 802.11ac

The final Wi-Fi standard I will cover is IEEE 802.11ac. This more recent standard returned to using a single frequency, namely, 5 GHz, but improved on the MIMO beamforming and channel bonding that we first saw in 802.11n. In fact, it utilized 40 MHz channels that could be bonded to make 80 MHz and 160 MHz channels. It also used a very efficient modulation technique called **Quadrature Amplitude Modulation** (**QAM**). These improvements allowed 802.11ac to have a staggering overall speed of 1.3 Gbps. However, the indoor range dropped back down to 35 m.

Summarizing the standards

I've given you a lot of facts and figures in the preceding sections, so I feel it would be beneficial to summarize them in a table. You will notice in the table I have not put the standards in alphabetical order. This is deliberate, as I find people remember them better this way as you generally start low (frequency, speed, and so on) and work up. And it spells B(e)GAN AC. I have to admit before AC came along, it was a little tidier:

Category	Speed	Frequency	Indoor distance	Modulation
B	11 Mbps	2.4 GHz	35 m	DSSS
G	54 Mbps	2.4 GHz	38 m	OFDM
A	54 Mbps	5 GHz	35 m	OFDM
N	Up to 600 Mbps	2.4 GHz & 5 GHz	70 m	OFDM
AC	1.3 Gbps	5 GHz	35 m	QAM

Now we have talked about the standards, we will look at the topologies we can implement to take advantage of them.

Implementing wireless topologies

Wireless networks can fall into general topographic groups, ad hoc and infrastructure. We will discuss both of these in this section, as well as some peripheral information pertinent to wireless networks, such as planning a network.

In `Chapter 2`, *Understanding Local Area Networks*, we discussed various areas that we needed to consider when planning our LAN. All of these are still valid in a wireless network, but I would like to specifically highlight some that have a major impact on the performance of a wireless network:

- **Hardware**: Recall that in the preceding section, we discussed the different wireless standards, and how they needed to support the same frequency to be compatible.
- **Environment**: One of the reasons we would implement a wireless network is to support devices in locations where we do not have the capacity to lay cables. This may cause us some issues in a large warehouse-like environment where the distance from the device to WAP may hit the limits, or the equipment within the warehouse may interfere with the signal. In those instances, we may want to locate a WAP in the center of the warehouse. But what if there is no power there? In that case, we would use a network cable to provide power to the device. This is referred to as **Power over Ethernet** (**PoE**) and has to be supported on the device.
- **The number of users**: The number of users efficiently supported by a WAP varies depending on whether it is a consumer-grade or business-grade device. Remember that Wi-Fi is a contention-based technology. The more users, the less efficient the network will be for an individual user.
- **Site surveys**: Planning a wireless network should include conducting a site survey. A survey will help you to identify the best positioning for your WAPs and identify any wireless black spots or dead zones where there is no signal. Ideally, you will want the coverage area of the WAPs to overlap to a degree to allow users to roam the building and have a continuous signal.

A Wi-Fi network is identified by its **Service Set Identifier** (**SSID**). This is a human-readable name usually created by the network administrator and broadcast out by the WAPs.

Ad hoc mode

An ad hoc mode network (or peer-to-peer) is geared toward connecting devices together without the need for any intermediary devices such as WAPs. The devices quite simply talk to each other, in what is referred to as an **Independent Basic Service Set** (**IBSS**). The IBSSID is a pseudorandom identifier similar to a MAC address generated by the device creating the ad hoc network.

Infrastructure mode

In an infrastructure mode wireless network, wireless clients must connect to an intermediary wireless network device, such as a WAP or wireless router, to be able to communicate to other devices on the network. This network may involve just one WAP or multiple WAPs and usually connects to a wired backbone network. Regardless of which method you implement, the SSID will be the same for all WAPs. A single WAP and its associated devices are referred to as a **Basic Service Set** (**BSS**) and are identified by a **Basic Service Set Identifier** (**BSSID**), which is the MAC address of the WAP. A collection of BSSes using the same SSID form an **Extended Service Set** (**ESS**) and are identified by an **Extended Service Set Identifier** (**ESSID**), which is usually the SSID of the network.

The implementation of a wireless network using an extended service set allows users to roam around the building and maintain connectivity as they do so. We can see, in *Figure 4.8*, that this network is made up of three separate BSSes that share the same SSID, hence forming an ESS:

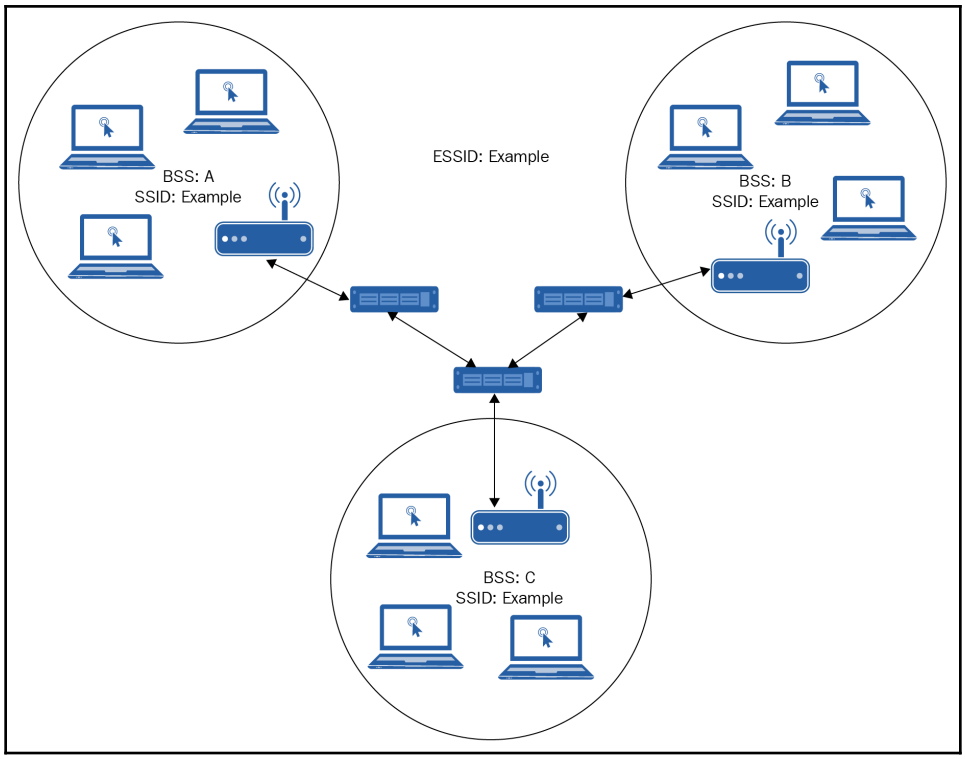

Figure 4.8: Service sets in operation

An infrastructure mode wireless network will be the main type of wireless network implemented within an organization and at home. I will now discuss a few variations of the infrastructure mode network.

Point-to-point wireless including wireless bridge

Traditionally, a wireless bridge allows you to connect a wired network to a wireless network, and that still holds true. However, we can also think of a wireless bridge as connecting two wireless networks together, such as when you want to connect one building to another building but cannot lay cables (*Figure 4.9*):

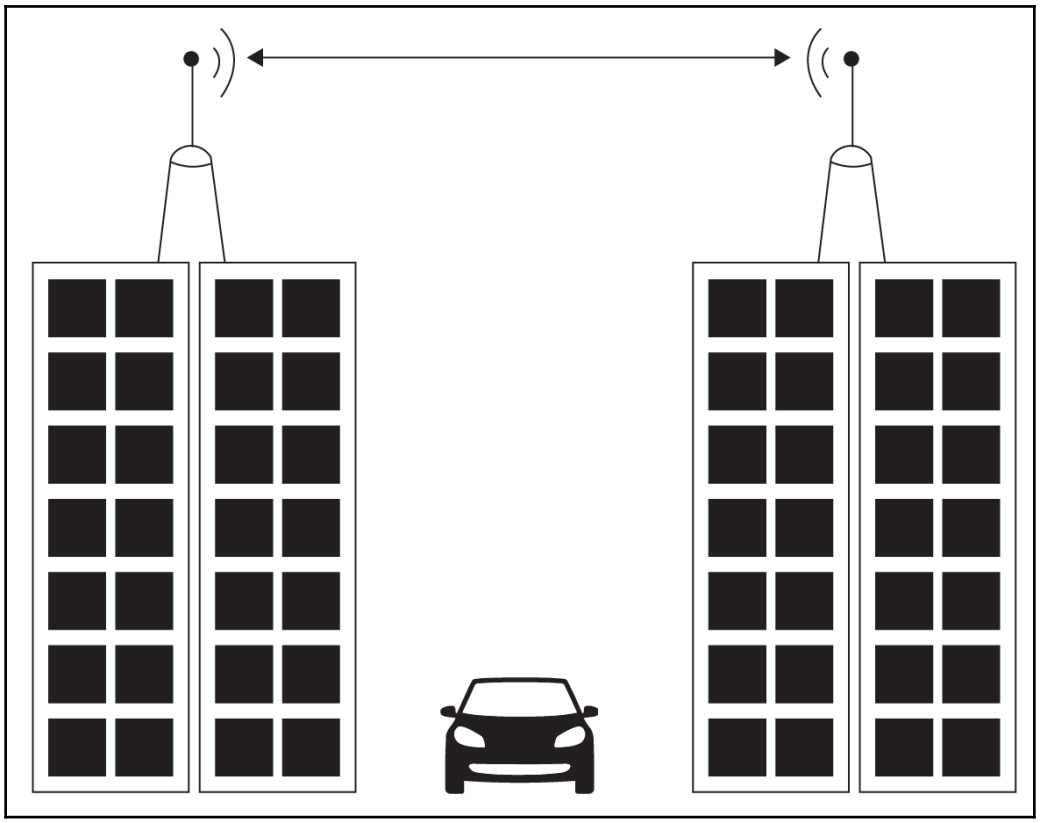

Figure 4.9: Wireless bridge connecting between two buildings

In this sort of implementation, you will most likely use a unidirectional antenna, such as a Yagi. I would also like to mention that, although the preceding diagram shows a straight line connecting the two antennae, this is for simplicity, and the transmission is, in reality, more of a flattened oval shape, known as a Fresnel zone.

A wireless bridge is a form of point-to-point network. When we use a wireless access point, this is point-to-multipoint communication. That is, the one device (point) connects to multiple clients (multipoint). As you saw earlier with the wireless bridge, one antenna (point) is talking to only one other antenna (point). Wireless point-to-point communication can reach up to around 15 km at the time of writing, and therefore avoids the costs associated with laying cable in most cases. An important consideration is that the two devices have *line-of-sight* of each other so the signal be transmitted clearly. In some instances, this may require elevating the antenna so it avoids any obstacles.

We have already discussed the attrition suffered by wireless communication, and point-to-point is no exception. Of course, over these greater distances, this can be more of an issue, and the signal can be affected by things such as solids (for example, buildings and trees), dust, and water. You may think water is an odd thing to affect a wireless signal, but it is worth bearing in mind that there is moisture in the atmosphere, and of course, these connections are outside, and there is the potential for rain.

Wireless Distribution System

A **Wireless Distribution System** (**WDS**) is a wireless network where the majority of the networks do not connect to a wired network but connect to each other. Any WAP that connects to the wired network is referred to as a main base station. A remote base station is one that receives data from wireless clients and forwards them to a main base station or relay base station. A relay base station receives data from main and remote base stations and forwards it to another base station.

By creating a wireless mesh network (*Figure 4.10*), we allow for redundancy in our network. If a base station fails, there are mechanisms in place to route the data to another relay base station for onward transmission:

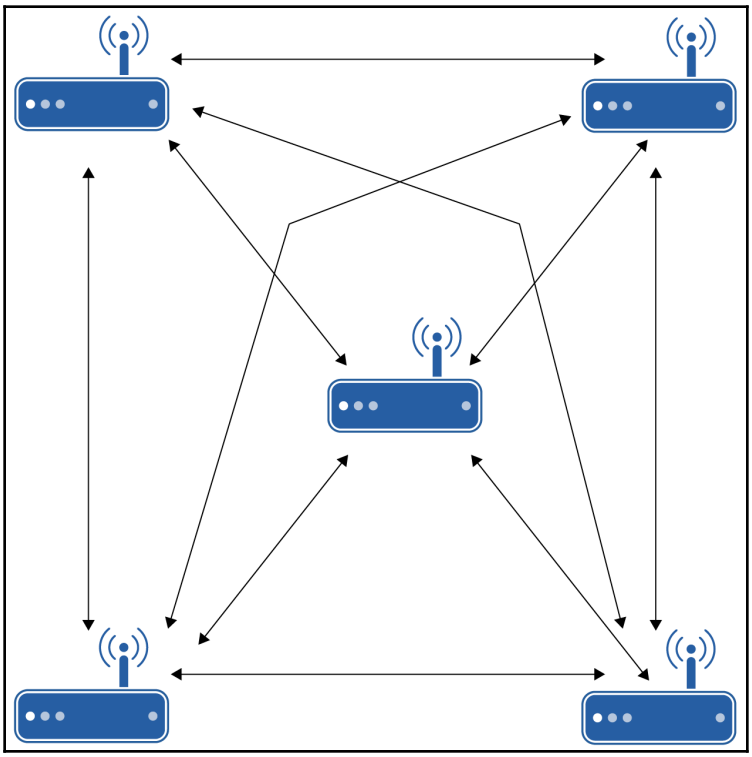

Figure 4.10: Wireless mesh topology

With all of this data flowing across the airwaves, we need to think about how we are going to protect it. In the next section, we will discuss the security methods available to do just that.

Understanding wireless security

Wireless communication could be described as a broadcast technology. Anything that is transmitted is available for all to hear or eavesdrop on. Can you spot what issues this may bring? If you said this leaves the data unsecure, you would be correct. Therefore any wireless deployment needs to ensure that appropriate measures are taken to protect the data.