Understanding Fixed Wireless Access

What Is Fixed Wireless Access?

Alex Marcham
NetworkArchitecture2020.com
1. Introduction

The spread of network technology across the globe has brought huge changes to every society it touches. With smartphones and broadband internet connectivity, networks have enabled billions to keep in touch with friends and relatives, get access to vital resources and limitless entertainment, whilst expanding their economic opportunities.

The network relies on the ability to add connections and bandwidth over time to support changing requirements. Otherwise, it’s easy to end up with a network built 5 years ago, for traditional traffic flows and demand, struggling to keep up with the rapidly changing landscape of applications seen today - a costly mistake for any network operator.

Inside a building, it’s not too hard; run more cable through the conduits, connect the new device to the network. However, things get more complicated when networks go outside, whether an inter-building connection by an enterprise, or a service provider expanding their coverage, particularly to rural areas.

No matter the size of the outdoor network, adding new connections and more bandwidth in a fast and flexible manner, whilst being economical, is not always easy. In many parts of the world, running your own cable above ground is prohibited or simply impractical.

For Network Architecture 2020, and network operators, this is a pressing problem; we need to be able to effectively expand our networks wherever needed, whether small enterprise or giant service provider, in an economical manner.

In some cases, copper or fibre cabling-based technologies are the right choice. In others, they are hamstrung by the need to lay physical cable through obstructions such as roads and rivers; in other cases, they are simply too expensive to install over long distances.

If networking technologies relying on cabling for outdoor connectivity aren’t always a viable option, what are our alternatives? And do any of them actually work?

Fixed Wireless Access (FWA) is a potential solution to these challenges for many use cases. It is a set of wireless networking technologies, using radio frequencies to send and receive data over long distances between two or more fixed network endpoints.

This eBook series will provide you with a solid understanding of FWA, and answer:

Is FWA part of Network Architecture 2020?
2. What Is Fixed Wireless Access?

Before delving into the how and why of FWA, it is important to define what FWA is, and how it is distinct from other technologies.

2.1 - Definition of Fixed Wireless Access

FWA is a set of technologies designed to provide fixed outdoor wireless networking, to allow long-distance data connectivity between one or more network endpoints, without the need for physical cable across the entire distance between them.

The diagram below shows a simplified example FWA deployment.

To better understand what the technology is attempting to do (and what it is not), consider each word individually:

2.1.1 - Fixed

Unlike cellular technologies, which are designed to accommodate devices which are physically moving relative to the base station such as cellular phones, FWA technologies are designed to connect two or more network nodes with physically fixed positions. This makes them much more comparable to a ‘wireless wire’, rather than a system like LTE.
2.1.2 - Outdoor

Unlike Wi-Fi networks, which are predominantly designed for indoor operation, FWA is designed for outdoor operation at considerably longer ranges than indoor wireless networks. FWA connections spanning 5 to 10 km are common, with much longer distances frequently seen.

The author has personally installed a FWA connection spanning 245 km, from the top of a mountain. Not something you do every day, and quite the view.

2.1.3 - Wireless

Although we usually assume any wireless network is using terrestrial radio technology to send and receive data, there are other approaches, such as Free Space Optical (FSO), satellite transmissions and many other types of wireless networks. FWA networks use terrestrial radio technology to send and receive data.

2.1.4 - Networking

At the end of the day, the point of an FWA network is to provide a network connection between two endpoints, to extend the reach or increase the bandwidth of the network. If the technology doesn’t achieve this in a useful and unique way, it’s unlikely to find widespread adoption.

This short definition provides the basis for understanding FWA. Let’s further narrow down what is considered FWA for the purposes of this book:

2.1.5 - Radio frequencies from 900 MHz to 6.4 GHz

FWA networks use radio technology to send and receive data, operating most frequently in the 2.4 GHz and 5 GHz bands. This has more to do with licensing than anything else; these frequency bands are unlicensed or lightly licensed in many parts of the world, including the United States.

However, FWA networks also commonly operate in a range of frequency bands from 900 MHz to 6.4 GHz, depending on use case and local government regulations across the world.

There are many other radio frequencies used for wireless networks, including those below 900 MHz up through millimetre-wave (mmWave) systems which cover 30 to
300 GHz. Although important for many use cases, these are typically used for different applications and won’t be the focus of this book.

**2.1.6 - Ethernet and IP based**

Modern FWA networks are designed to carry Ethernet and Internet Protocol (IP) – that is, frame or packet-based data, just as other modern networks such as Wi-Fi, LTE, our wired networks and the majority of the internet itself are.

Just like those networks, if circuit-based data needs to be transmitted, such as a legacy E1 or T1 circuit used by a telecoms operator, it is split into a stream of packets for transmission across the network and reassembled at the remote end.

**2.1.7 - Bandwidth up to 1 Gbps per connection**

As with all networking technology, there are enough ifs and conditions I could put next to that 1 Gbps figure to fill the rest of this book. Some products promise more, some promise less, and the ongoing march of technological development will surely render this figure outdated in the months and years ahead.

However, for the purposes of this book, consider the ability to provide a fixed wireless network connection between one or more endpoints in the network up to 1 Gbps as the capability of FWA as a technology, just as understanding 1 Gbps Ethernet stands you in good stead for 2.5 or 5 Gbps Ethernet.

I will elaborate on the many factors and conditions that take a claimed headline data rate and turn it into what you can reasonably expect in a real-world deployment throughout this book.

**2.1.8 - Deterministic MAC**

The Medium Access Control (MAC) functionality of a networking technology defines how it attempts to transmit and receive data on its medium of choice. For FWA networks, that medium is radio spectrum, and unless the network is operating in laboratory environment it is highly likely that the equipment used in the network will detect wireless transmissions from other networks or other devices using the same spectrum.

This is most common in the unlicensed spectrum bands of 2.4 and 5 GHz, where any transmitting device abiding by the rules from the local regulatory body (such as the FCC in the United States) in terms of power, channel bandwidth and other factors is allowed
to transmit freely. If another device transmits on the same channel as your network at the same time, it can cause your equipment to struggle or fail to correctly decode the wireless data transmissions it is intending to receive, losing transmitted data.

This is wireless interference, and is a fact of life for most FWA networks. This makes it important that a deterministic MAC is used, which will do its best to ignore competing wireless transmissions so that your network continues to function as expected regardless of what is happening in the spectrum around it.

This is worth emphasising as the most common technology for wireless networking in these unlicensed bands is Wi-Fi, which was designed for use inside the home where interference is assumed to be low or non-existent. On detecting interference, a Wi-Fi device will ‘back-off’, that is, delay its own transmission until the spectrum is clear. In an outdoor FWA network, the spectrum may never fully clear, rendering the network unusable without a deterministic MAC.

This and other issues will be elaborated on further in subsequent chapters.

2.2 - What Does It Look Like?

A FWA network typically conforms to either a hub and spoke, star, or point-to-point (PTP) topology.

In the case of a hub and spoke (also known as star) topology, these are often referred to as Point-to-Multipoint (PMP) networks. Two major components are present in these topologies:

2.2.1 - An access point

Similar to a base station used in cellular technologies or an access point used in a Wi-Fi network, an FWA access point is the ‘master and co-ordinator’ of its segment of the network. Subscribers all connect wirelessly back to an access point, which sends and receives data between its subscribers and the rest of the network.

2.2.2 - One or more subscriber modules

The number of access points and subscriber modules in a network or network segment is driven by many factors and varies wildly across deployments, from the number of nodes required in the network to technical constraints, including limitations in the system architecture of the radio equipment used and lack of available wireless spectrum.
In a PTP topology, two nodes (typically either two subscriber modules or two dedicated PTP nodes) are connected wirelessly, providing connectivity between two points of the network. These links often function as the backhaul or uplink connection for a PMP network segment, as they are capable of providing relatively high bandwidth and low latency. They are also often seen for building-to-building connections and other relatively high-bandwidth use cases between two network endpoints.

The diagram below shows both PMP and PTP topologies together in a network.

2.3 - How Is It Used?

FWA can be deployed as a replacement for wired technologies using copper or fibre, as well as a compliment to them providing extra bandwidth or redundant connectivity for an existing wired network connection, deployed outdoors.

Some common use cases for the technology today are:
2.3.1 - Residential internet access

A Wireless Internet Service Provider (WISP) is an organisation providing internet service to customers by using FWA technology, with a subscriber module mounted on each customer’s house. Although more prevalent in rural areas where wired connectivity is insufficient or unavailable, deployments are also seen in some urban areas.

Typically, the requirement is for asymmetric uplink and downlink ratio packages, such as 5 Mbps up 25 Mbps down, with reasonable assurances of service and support, comparable to those from a wired internet service provider.

2.3.2 - Business internet access

Although similar to residential internet access in many ways, business internet access is distinct from that use case by the bandwidth and service assurances typically required by business customers. Symmetrical uplink and downlink ratios are expected for business internet connectivity, with strict service level agreements (SLAs) on the part of the service provider in terms of bandwidth, latency and availability.

The areas where business internet access is typically required also vary, with business parks being a common area of deployment for the technology with this use case.

2.3.3 - Video surveillance and remote monitoring

Video surveillance cameras, remote sensors and other devices typically located outside or in remote locations which are generating data that needs to be returned back to a central location such as a video surveillance monitoring station or sensor aggregation point are prime use cases for FWA.

2.3.4 - Enterprise connectivity

Inter-building connectivity for the enterprise can be enabled and improved by FWA, connecting either multiple buildings or equipment to a central building using a PMP network topology, or providing high-bandwidth connections between individual buildings using PTP connections.

Think of a business with multiple buildings on a business park; unable to bury cable themselves under the tarmac or run it overhead, a service provider must be called to lay the cable and then charge a monthly fee to the enterprise to use it – if the service provider even decides to offer this, due to costs.
2.4 - Why Is It Used?

Before delving into a comparison between FWA and specific competing technologies, here are a few key reasons why FWA is used during network rollout and expansion by a variety of users for many use cases.

2.4.1 - Speed of deployment

Whether installed for permanent or temporary use, the speed of deploying an FWA network for outdoor connectivity is considerably faster than a comparable deployment with wired technologies.

The main differentiator is the time required to bury or lay physical cable to each network endpoint with wired technologies, which can increase exponentially when it comes to crossing road or other property not owned by the organization deploying the network.

2.4.2 - Cost

The typical cost to deploy a FWA network is substantially lower than that of a wired network covering an outdoor area, often by an order of magnitude. The costs of laying cable to each endpoint – including obtaining the right to do so from property owners, workers required to lay the cable, safety and other regulations plus ongoing maintenance once the cables are installed – are significantly higher than using FWA.

This cost difference may determine whether or not the network gets deployed at all, making FWA an enabler of connectivity, not just a cost saving.

2.4.3 - Flexibility

Not all bandwidth requirements in the network are permanent; consider a temporary event such as a concert requiring high-bandwidth data connectivity, emergency response teams deploying a communications network at a disaster scene for a few weeks, or a building that the wired service provider has not yet connected with wired technologies but which requires internet access now. All of these use cases can be achieved with flexible FWA deployments.

2.5 - Why Isn’t It Used?

No technology is perfect, and no technology fits all use cases to the best possible extent.
Here are a few key reasons why FWA isn't used in some deployments and for some use cases:

### 2.5.1 - Capacity

Some applications, such as permanent data centre interconnections, require multiple gigabits of throughput. Although it may be possible to use multiple FWA connections side-by-side to achieve this level of capacity, often limitations in available wireless spectrum will prevent this from being possible.

High-capacity data centre interconnects are typically best left to fibre connections, although FWA may be valuable as a temporary bandwidth increase or redundant connection.

### 2.5.2 - Cost

Although the typical cost of deploying FWA is lower than that of a wired technology when copper or fibre cable is not already installed, in cases where it has already been deployed the cheaper option is often to use that existing infrastructure rather than deploying an FWA network.

### 2.5.3 - Obstructions and interference

Wireless networking technology has advanced significantly in terms of achievable range, handling of obstructions and resiliency to wireless interference. Many networks operate in areas and conditions that were thought impossible in the past, such as over stretches of water, over very long (tens or hundreds of kilometres) distances, or through conditions which do not allow for a completely clear Line of Sight (LoS) between network endpoints.

However, situations do exist where adequate network connectivity is not achievable using FWA, through a combination of physical obstructions, required range and wireless interference.

### 2.6 - Competing Technologies

To understand how FWA compares with other technologies for long-distance outdoor connectivity, let's first take a look at the wired alternatives and how they compare, both copper and fibre-based.
2.6.1 - Wired Technologies

2.6.1.1 - Comparison with fibre

When it comes to the highest bandwidth and lowest latency, fibre optic networking technology is the king. There’s a reason it’s used in the submarine-laid cabling connecting the Earth’s continents together to form the internet – techniques like Dense Wavelength Division Multiplexing (DWDM) and the unique capabilities of laser transmission inside fibre optic cabling provide unparalleled bandwidth.

However, there’s a problem – with this very high bandwidth comes the high cost of deployment.

Fibre optic cabling, termination equipment and optical interfaces can range from inexpensive to a considerable investment depending on the bandwidth and range required. But the bigger problem is the cost of laying the cable. Outside of densely populated urban areas, it is often not economically viable for a service provider to dig a trench to every home, business or outdoor space they want to provide internet connectivity to, lay the cable, bury it, and come back to fix it in a few months when someone has cut through it with a backhoe (which happens more often than you’d hope).

This constraint leads to hybrid network architectures, such as Fibre to The Cabinet (FTTC), where the fibre connection is brought to a Point of Presence (PoP) in an area, which then connects to the homes and businesses using existing copper cabling. Although this can be a significant improvement over copper-only architectures, the ‘last mile’ of copper cabling is frequently the cause of much frustration for service providers and end users as it introduces reliability and performance issues.

For applications requiring bandwidths that are sometimes multiple hundreds of Gbps, there is no substitute for fibre connectivity. But, for many other applications, its cost of deployment and lack of flexibility is prohibitive compared to deploying FWA technologies.

The diagram below shows a simplified example Fibre to The Home (FTTH) deployment.
2.6.1.2 - Comparison with cable

Coaxial cable – the type used to carry both Internet connectivity (using Data Over Cable Service Interface Specification, or DOCSIS) and cable TV – is similar in a lot of ways to fibre. Cable offers high potential bandwidth and reasonable latency, though neither of these matches up to the performance possible with pure fibre optics. It is widely deployed in urban centres in the United States and in some other countries.

Where it does share a lot in common with fibre, is the cost of deployment and maintenance. Similar cost barriers exist for deployment, with similar investment required by the service provider in terms of digging a trench to everywhere in need of internet connectivity, burying and maintaining the cable.

Most operators capable of the investment to deploy a wired technology today are looking towards fibre, leaving existing cable infrastructure relegated in many areas to legacy status. Although it is still possible to increase the life of existing cable infrastructure, such as through Hybrid Fibre-Coaxial (HFC) infrastructure and new revisions of the DOCSIS standard which add features and performance, the future for new greenfield cable deployment looks to be shifting to fibre.
In areas where customers are already connected to the cable infrastructure, this provides a solid argument against FWA deployment as the cost of using existing infrastructure is often lower than installing new infrastructure. Where cable is unavailable or insufficient however, deployment of an FWA network by a wireless internet service provider is often a very viable option.

The diagram below shows a simplified example cable deployment.

![Cable connection diagram](image)

### 2.6.1.3 - Comparison with DSL

Digital Subscriber Line (DSL) technology uses the copper cabling utilized by home or business telephone lines to deliver internet connectivity. In many areas, it is the only option, where cable and fibre connections do not reach. Typically, connections to the home will use Asynchronous DSL (ADSL) to provide higher downlink than uplink speeds. Businesses will often use Synchronous DSL (SDSL), which splits the connection speed evenly between downlink and uplink. Speeds are typically below cable.

The issues with DSL aren’t so much due to DSL itself as a technology; the problem is that in areas where DSL is an attractive option due to the lack of competing technologies, which are most often rural areas, the copper cabling carrying the DSL signals is often outdated and poorly maintained. This results in the speeds achieved by the end user often being far less than the advertised peak speeds.
Much like cable, in areas where service providers are capable of justifying the investment in new cabled infrastructure, the attention is now turned towards fibre. Similar hybrid architectures to HFC are possible combining DSL and fibre, such as FTTC, but the troublesome ‘last mile’ of copper cabling, which in the case of DSL is often far older than that used for cable, remains an issue.

In these rural areas where DSL is attractive, or even the only option, FWA provides a solid alternative to DSL for internet connectivity, assuming that the physical characteristics of the rural area allow for long-range outdoor wireless connectivity.

By replacing the wired phone in the home or business with a VoIP phone, the copper telephone line can be removed from use entirely, which can also result in a significant saving for the end user (British Telecom for instance charges separately for the ‘line rental’, as well as the services provided over it).

The diagram below shows a simplified example DSL deployment.

Although the deployment examples of wired technologies are heavily simplified, conceptually they are similar and the examples serve to show the distinction between wired and wireless deployment models.
2.6.2 - Wireless Technologies

FWA networks of course compete not just against wired copper or fibre technologies for outdoor connectivity, but against many wireless options as well.

2.6.2.1 - Comparison with Free Space Optics

Free Space Optics (FSO) technology uses lasers, outside of the visible light spectrum, to transmit data from one network node to another. These systems are capable of offering speeds above 1 Gbps, coupled with low latency over short distances, and are deployed typically between rooftops of buildings across a street from one another in dense urban centres.

A constraint of FSO systems, and others relying on light to transmit data, is that a clear line of sight is required at all times between receiver and transmitter. Bad weather, dirt on the transceiver lenses, wildlife passing by (such as birds in flight) or light foliage can quickly render the system unusable by increasing the error rate dramatically.

This can be partly addressed by using a backup radio link, typically in the 30 to 300 GHz mmWave range. However, deploying an FSO system with a high level of service assurance – such as the favoured ‘five nines’ of uptime (99.999%), required by many organisations, working out to 5 minutes of downtime per year, remains challenging.

Alignment can also be an issue, with small misalignments capable of introducing large drops in link performance. Although the short range of FSO links helps with alignment, weather or wildlife may cause a misalignment knocking the link out of action for a period of time until it is manually realigned. This can be addressed by proper installation; however, FSO systems are more prone to suffer from misalignment than those based on radio technology.

Due to their range limitations, FSO systems are unable to compete in many use cases with FWA networks, although in use cases where they excel, such as some enterprise connectivity deployments, they are capable of greater data capacity measured in Gbps. However, even in these use cases, radio or mmWave systems are often equally as capable and more robust.

The diagram below shows a simplified example FSO deployment.
What Is Fixed Wireless Access?

2.6.2.2 - Comparison with satellite

Satellite networking technology relies on a base station on the ground with a clear view of the sky, sending and receiving data to and from a satellite orbiting above the Earth. Although there are very few places on the surface of the planet that can’t be reached by satellite communications, providing a connection almost anywhere, there are some disadvantages in equal measure.

The maximum claimed downlink data capacity is 50 Mbps, with high latency due to the extreme distances involved in communicating with the satellite and its supporting network of ground stations. Even on newer-generation satellites, round-trip latencies an order of magnitude above those achievable with terrestrial technologies, wired or wireless, are common, making interactive applications frustrating, impractical or simply impossible.

In addition, the cost of satellite internet connectivity compared with the speeds it offers is highly prohibitive, with the highest cost per Mbps of bandwidth of any mainstream Internet connectivity technology. Satellite connectivity is not typically considered a competitor to fibre, cable or DSL; it is most often the technology of last resort, when no other connectivity is available due to geography.

In some areas, such as those requiring extreme mobility (the most frequent example of satellite data transmission technology in use being reporters in danger zones reporting live from the scene, or military applications) or those that are very remote such as the extremes of the planet, satellite looks to remain the only viable option.
That said, there are many users – typically residential or very rural businesses such as farms using satellite internet connectivity today – who would be possible to connect using FWA in a more economical manner. Whether this occurs is down to the service provider weighing their investment against the likely return, although a higher-performing service to those users should also be possible.

The diagram below shows a simplified example satellite deployment.

![Satellite connection diagram](image)

2.6.2.3 - Comparison with LTE

Long Term Evolution (LTE) is considered the dominant cellular connectivity technology today, at the forefront of investment by almost all major carriers worldwide. It has supplanted previous and competing technologies such as 2G and 3G, and is capable of offering both traditional voice calls and high-capacity internet access.

A comparison between FWA and LTE is not always clear. Whereas both are wireless technologies designed for long-distance outdoor operation, there are many differences between them, ranging from technical, economical and design intent. LTE is a complex system, designed to incorporate and build on all of the features and functionality of the 2G and 3G cellular systems.
This includes mobility, handoff of mobile subscribers between base stations whilst retaining active data transmissions, interaction with legacy circuit-switched systems, and a comprehensive Evolved Packet Core (EPC) backend system, interfacing with a myriad of functionality crucial to the operation of a modern cellular network, such as a subscriber location register, subscriber management, blocking of stolen devices, and many other functions.

For the operator looking to deploy connectivity wirelessly between two or more fixed network endpoints separated by long-distance outdoors, the range of features and functionality in LTE is very likely to be significant overkill, raising the cost, time and knowledge required to deploy an LTE solution considerably – the cost of an LTE base station can be considered an order of magnitude higher than an access point used for FWA, often more.

When device mobility is required, such as a service provider looking to provide cellular connectivity to mobile phones, there is no contest; LTE provides mobility and subscriber management for mobile devices, where FWA does not.

For a real comparison with LTE and other cellular technologies, think of FWA as a ‘wireless wire’, a fixed connection between two network nodes outdoors. Where that is what is needed, FWA is worth considering and typically wins over cellular technologies in terms of cost, required knowledge and achievable bandwidth. Where mobility is needed, cellular is the best (and often only) option.

The diagram below shows a simplified example LTE deployment.
2.6.2.4 - Comparison with Wi-Fi

As discussed above in the section on deterministic MAC, Wi-Fi itself is not suited for the same applications as FWA as it uses a Carrier Sense Multiple Access with Collision Avoidance (CSMA/CD) mechanism; Wi-Fi devices will not transmit whilst another device is transmitting, instead waiting a variable length of time after the transmission has finished before attempting to transmit.

Although this allows Wi-Fi to operate well inside the home (as well as being simple and cheap to implement), for the long-range outdoor applications of FWA networks it results in poor performance. This is due to other devices transmitting on the same or neighbouring channels as the Wi-Fi system, causing the Wi-Fi system to wait for them to finish transmitting, which they may never do.

The problem is that these other devices are often not Wi-Fi devices themselves; they may be wireless security cameras, non-Wi-Fi wireless networking systems, baby monitors, microwaves, or anything else using the 2.4GHz and 5 GHz unlicensed bands. These devices may transmit continuously, resulting in a Wi-Fi system waiting to transmit indefinitely until it gives up and drops the data it was trying to send.

Wi-Fi devices are designed to operate inside the home or in a defined area where the amount of interference is low. This assumption can't be made in long-range outdoor conditions, so FWA systems are designed to operate in co-existence with interference on the same or close channels.

With this in mind, Wi-Fi systems cannot be considered a comparable alternative to FWA networks, due to their unsuitability for long-distance outdoor operation.

2.7 - Frequently Asked Questions

Plenty of questions arise when discussing any technology in detail. Here are a few of the most common questions encountered for FWA.

2.7.1 - “Does this stuff actually work?”

As ever, if you ask an engineer, the answer is ‘it depends’.

There are many use cases and deployments where FWA technology functions as expected, providing the required bandwidth and latency in a way that is economical for the service provider and the end user. However, there are cases where deployments of
the technology haven't worked as expected, due to equipment issues, network planning, unforeseen wireless interference or a host of other issues, much like those that can dog any network technology rollout.

This will be covered more in later sections, but the most crucial part of ensuring that a FWA network deployment works, is planning. The wireless spectrum, physical locations of equipment and actual equipment to use must all be planned and selected with enough care. No technology, wired or wireless, can make up for poor or negligent planning, and FWA is no different.

Yes, there are scenarios where two people can simply go out and install a FWA network, particularly using a PTP topology, and have no discernible issues. But, as with any network deployment, it is useful to ensure that precautions are taken with installation, configuration and planning to ensure solid future operation and limit the need to return to the sites for troubleshooting later on.

2.7.2 - “Is FWA a recent technology?”

In short, no. Commercial FWA systems as we think of them today have existed and been widely deployed for over a decade, with precursor systems existing long before that. Due to this, the deployment model and core functionality of the technology are proven, with new systems building on this foundation at a rapid rate to improve performance, features and value.

One important note is the geographical spread of deployments of FWA to date. Across the world, on all continents, FWA networks provide internet connectivity for hundreds of thousands of users every day. It can be considered a mature technology, though one that is still evolving as technology progresses and is applied rapidly to FWA.

2.7.3 - “How much does it cost?”

Some FWA systems are based on open standards, whilst others are based on proprietary technologies, and across the industry widely-varying degrees of performance, features and pricing are seen.

The issue with answering this question is it requires knowledge of what the needs and requirements are for a particular deployment, and so a sweeping statement is difficult to make. That said, the starting cost of an entry-level system can be below $100 US dollars per node, with costs increasing in-step with features, performance and reliability.
Rather than look at a given vendor, as I will not do in this book, an approach more likely to yield a system fitting the business need that is being addressed is to understand the issues and trade-offs detailed throughout this book, then use that knowledge to select a system which best meets the need.

2.7.4 - “What are access and backhaul?”

In terms of FWA networks, a PTP topology connection is typically, though not exclusively, considered a backhaul connection; it is ‘backhauling’ a segment of the access network to the rest of the network, very much the branch of the network tree.

An access network is typically a PMP topology segment of the network, which connects as closely as possible to the end users by use of a subscriber module for each user; the leaves of the tree.

In terms of this book, in general the term ‘FWA’ is used to encompass both topologies as there are many similarities between them. When it is appropriate, distinctions between access and backhaul will be made, such as in network design and any unique requirements for these topologies.

2.7.5 - “Is it secure?”

FWA networks typically employ Advanced Encryption Standard (AES) encryption for all data transmitted wirelessly, ensuring that it meets the data encryption standard as defined by the United States government. This provides protection against traffic interception, the primary concern when transmitting data over long distances using wireless communications.

Other aspects of system security such as user account protection, Denial of Service (DOS) mitigation and other security factors are addressed by a combination of standard operational security measures and product-specific features. Not all equipment may implement the range of features required for a certain application or user, and so take care to evaluate equipment to ensure it meets security needs, as should be done for all network equipment as well as the end devices attached to the network.
2.8 - Conclusion

FWA is a technology with as many similarities to other networking technologies as differences. To fully understand its unique capabilities, it is important to grasp what it is and is not trying to achieve as well as how it compares to fibre, Wi-Fi and other technologies for a set of use cases.

Throughout this chapter, we have seen a description of the core characteristics of the technology, use cases, reasons why and why not to deploy it, and comparisons with other outdoor connectivity technologies.

This forms a foundation for the following chapters, exploring the how and why of FWA networks.