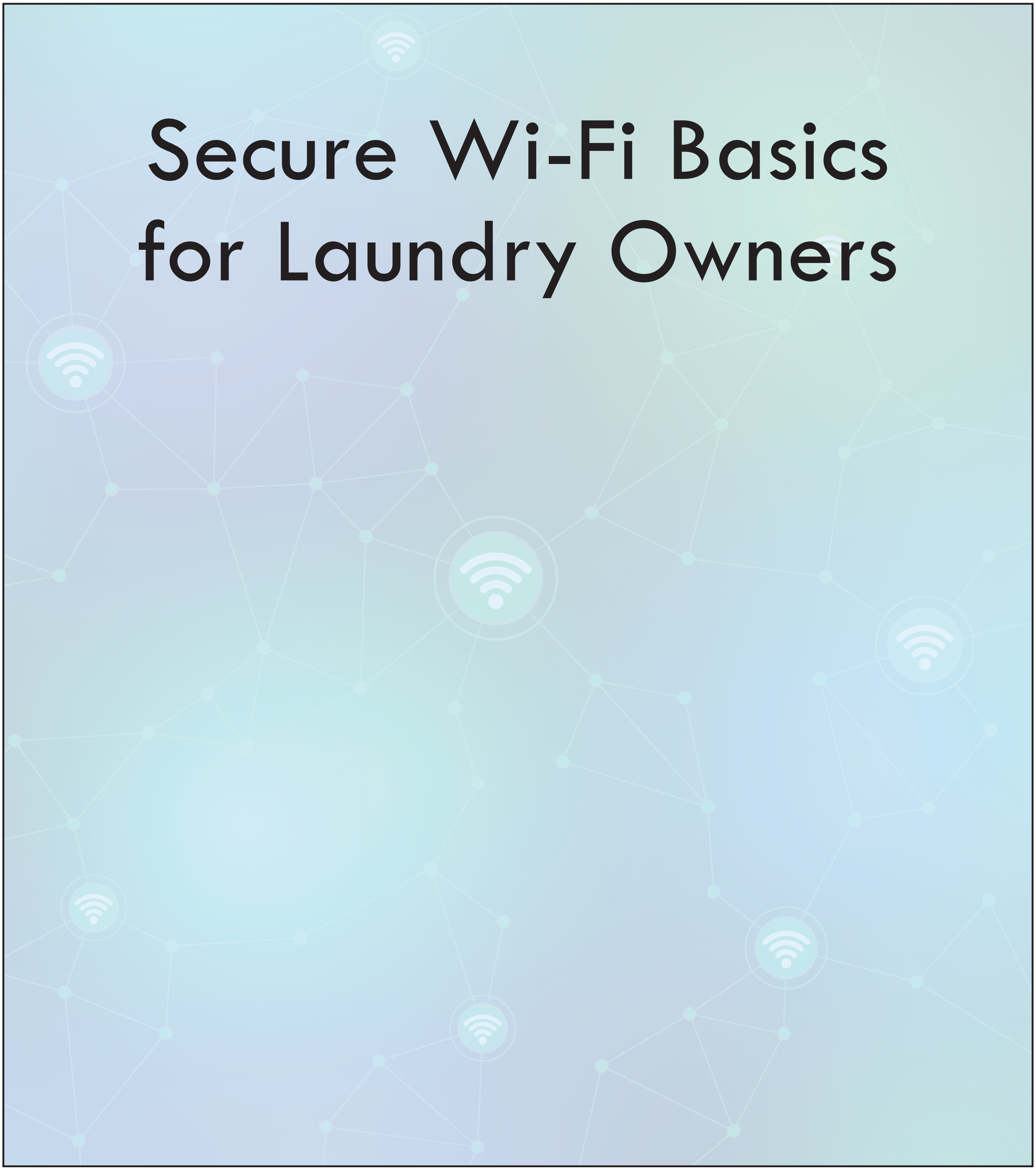
Secure Wi-Fi Basics for Laundry Owners



Volume 4 No. 9

A white paper by the Coin Laundry Association
www.coinlaundry.org

Gold Book
Research Series
Your Guide to Laundry Excellence

Coin Laundry®
ASSOCIATION

1s660 Midwest Road, Suite 205
Oakbrook Terrace, Illinois 60181
800-570-5629
coinlaundry.org

Secure Wi-Fi Basics for Laundry Owners

As a business owner, you're always trying to give your customers the best experience possible. Your success depends on your ability to innovate. If you're unable to keep up with customer demands and the trends that your competition follow, you're doomed to fall behind in your marketplace. One trend that more and more businesses are adopting is offering free Wi-Fi access to their in-store customers. Today, there are billions of Wi-Fi-enabled devices out there – many of them in the hands of potential laundry customers.

In fact, many people filter businesses – coffee shops, bookstores and, yes, laundromats – based on which ones offer fast, secure, free Wi-Fi. Those that do have a clear advantage over those that don't. Free Wi-Fi access can make your customers' lives easier and improve the perception of your business.

The reality is that customers have come to expect free Wi-Fi at most of the places they frequent. According to Coin Laundry Association statistics, nearly half of today's self-service laundry owners offer Wi-Fi access to their customers. And, not surprisingly, that number is growing every day.

However, the fact of the matter is that – along with all of the positives of a "connected world" – we are now subject to a wide variety of challenges and security risks. There was a time not long ago when business owners had to work hard to secure just the physical assets of their locations. Today, operators must consider both the physical and non-physical, which includes the data on the backend that helps you manage your operation and the customers that you serve.

You must protect yourself and your business from the cyber world. Whether intentional or not, those risks are real. Unintentional risks may include something as simple as an infected laptop. If you are offering free Wi-Fi access and you haven't taken the proper steps to secure your private network from the public network, that little device can wreak havoc on your data.

You may have heard the term "The Internet of Things" being bandied about lately – it refers to all of the devices that are now Wi-Fi/network-enabled. From security cameras to biometric devices, consider the need to protect the information that these devices are capturing.

Since the end goal ultimately is to have an internet-connected network – an Internet Service Provider (ISP) must be chosen. Your choices (or lack thereof) may directly relate to the area in which you're located. The speed at which you can access the internet also will depend on your location. Connection types and speed offerings often will coincide with where your laundry business resides within a given area. For example, rural areas typically don't offer the same choices as a bustling city or growing suburb. Speed can make or break the experience that you and your customers receive, and unfortunately some cities and towns don't provide much of an offering.

The most popular options and considerations are listed below; "popular" meaning well-established, but not necessarily robust or preferred. Dependability/uptime can vary widely by geographically area as well. You also may have the option to use two different technology types for redundancy. In other words, if one connection goes down, the other will take over. Here are your choices:

- Cable
- Fiber
- DSL
- Satellite
- Cellular

Cable-based internet has been the most popular connection type, generally reliable and offering high speeds at a low cost. If you have cable TV, you already know what the cable looks like. The majority of small businesses run off of internet provided by cable companies.

Fiber can provide the greatest speeds but also comes at the highest cost. Aside from larger businesses and multi-site location-to-location networks, fiber is not very popular due to the cost. Although there are exceptions, the price of fiber overall is generally high. Some will argue that services like AT&T U-verse are fiber-based and low-cost, which is true. However, the provided bandwidth doesn't come close to cable, and you may not receive fiber to your store. For instance, there may be fiber to the pole outside, but not necessarily to your building.

DSL is another popular selection. For small businesses, many IT companies install only DSL (or AT&T U-verse) as a primary connection, when cable is not available. This is due to the often poor wiring in many buildings, or the lack of speed/service it provides.

Satellite and Cellular are frequently considered last-resort connection types. If all else fails and nothing else is available that works at your business, you often will get one of these two options. Both work – albeit slowly and weather permitting. However, Cellular is not impacted as strongly by weather as Satellite. If your only option is one of these two services, Cellular (area and service depending) typically is the better choice.

During the planning stage of your network and selection of a service provider, consider any business plan offerings.

In general, business plans are given more priority and have better stability than consumer services. Also, consumer services often don't offer static IP addresses, which will be necessary for certain options.

When you contact the companies, be sure to ask such questions as:

- What are my download and upload speed options?
- What has been your typical uptime in my neighborhood?
- Do you have an SLA, or Service Level Agreement, which guarantees a certain percentage of uptime?
- Are your services month-to-month or contracts? If a contract, how long?
- Do I have the option of upgrading my speed at a later time? If so, how do I go about that? Would my services go down during the upgrade; if so, for how long?
- I have multiple laundries. Do you offer a discount if I sign up for multiple locations?
- Do you offer Static IP Addresses?

Renting the Internet Service Provider (ISP) equipment is suggested, as they are far more helpful during support calls if you rent rather than own. In fact, if you don't use their equipment, some companies will only assist you to where the wiring comes into your space. Using the ISP's hardware also will allow (and force) them to manage and work on the modem, which is the device that your network relies on for internet access.

Next, it's important to consider security and the need to protect your business and the data within. How exactly is this done?

In a word… firewalls. A firewall isn't just some fancy device that only large corporations and banks use in the movies so that our favorite actors can breach Fort Knox. A firewall is a hardware device (and software) designed to inspect, filter, and block access from one network to another. In this case, the public network – such as the internet or your public Wi-Fi – from gaining access to your private network, like your POS systems, security devices and so on. A firewall can be integrated into other devices such as certain wireless access points, or a physical dedicated device. The type of firewall you use will be determined by the network option your business chooses to implement.

Wireless access points (AP) come in many flavors – some square and some round; some with six antennas, some with two, some showing only one and some that appear to have none. However, all access points have multiple antennas, whether you see them or not. ISPs offer modems with built-in Wi-Fi and public hot spots, too. Although the decision is being made on the access point type, pay attention to how they are powered. Not all devices plug into a wall outlet – certain models are "PoE," which stands for Power Over Ethernet. They are simply powered by another device such as a power injector, which looks similar to your laptop brick, or from a PoE switch over a network cable. Many business class wireless APs are PoE.

Every network relies on wires, and wireless networks are no exception. The backbone of your network relies on low-voltage wiring, which carries the data back and forth between devices. The cables connecting your devices are known as patch cables, and the cables running from your equipment to end points (such as your computers and POS system) are known as data runs. The importance of quality cables and the quality of their installation cannot be stressed enough. The stability and experience of your network directly relates to the time and effort you put into it.

Simply put: poor cables = a poor experience. You can spend a lot of money on high-quality equipment, but always keep in mind that, if your cabling is poor, your experience also will be poor. And a bad experience for you directly relates to a bad experience for your customers.

The location of your data runs also impact how well your network will work. If you install high-quality cabling but place them poorly, you can end up with a great deal of stress on your hands.

For example, there was a drycleaner that had an excellent site. It was state-of-the-art, from the machines to the network devices. They even did a great job of running their cables throughout the building. Sadly, their computers and network devices suffered from horrible send and receive times. In fact, some information going from computer to computer would never even arrive.

So, if they appeared to do everything correctly, why were they having so many computer problems? The simple answer: EMF, which stands for electromagnetic interference. Electricity can negatively affect wired and wireless networks more than most people realize. All of the network cables at this drycleaning business were neatly following electrical conduit pipes, going around electric boxes and hovering over fluorescent lighting. After all, this is a great way to hide unsightly cables.

In this case, an EMF detector showed levels that were off the charts. The business owner eventually re-ran the wires in more suitable locations, and all of the issues disappeared.

This story is relevant, as there likely are many forms of interference in your space. What you see and don't see around your devices and access points must be considered during the planning stage. You will find putting the extra effort in at the start of your project will allow you to enjoy yourself at the end of it.

Working our way back to the topic of wireless access points, we're going to focus on two ways they can be configured and controlled. One is controller-less and the second is controller-based.

Controller-less access points are often familiar to those who have installed consumer-grade wireless devices at home. You plug them in, follow a few directions, and you're set to go. There wasn't too much to do. You didn't need to go through too much trouble setting it up. In fact, all that was needed was logging into an IP address (the address of the device itself), entering a username and password, and following a wizard to get you going.

Because this type of device is controller-less, it doesn't use any other equipment or page to control it. You log directly into the device and that's it. The AP knows only about itself and is usually not concerned about connecting any other wireless access points. There are many business APs that are configured in the same manner, and they work fine – often wonderfully, with a decent number of logs or information to observe (such as who is connected). Although with the business-class devices, there are a lot more configurations for security that take place.

Controller-based wireless access points are different and offer far more control and insight into your wireless world. These APs are business/enterprise devices that are often more robust than their controller-less counterparts. Not only are you given a great deal of control over one single access point, but you are given control over two, three, four or even more.

Consider how your laundry business is situated. You may have a space in which multiple wireless devices are needed on the same floor, or have devices on multiple floors. Controller-based APs allow you to control multiple devices from one place, which includes keeping them updated simultaneously. This all allows you to gain a deeper view of usage – ranging from how many people are using your Wi-Fi to how long they've been on to how much bandwidth/data they've used. You also have the option of blocking devices, throttling (lowering or raising) speed, and presenting customers with messages and legal information. Keep in mind that you have some of these options with a controller-less AP as well. However, controller-based APs are far easier to manage depending on your situation and how your business is situated.

From a high-level standpoint, we have covered a number of topics, including the following:

- Service providers
- Service types
- Equipment
- Wireless access points (APs)
- Importance of good cabling
- Controller-based/Controller-less APs

Thus far, you've taken in a good amount of basic knowledge, which will help immensely in designing or redesigning your wireless network. With this base of knowledge under your belt, we can move into the "meat and potatoes" of technical requirements, options, environment concerns, proper placement of your wireless APs, social/data capture and management methods. Now that you're familiar with many of the network and Wi-Fi considerations, let's dive into a higher level of detail.

Although you may have a network in place – and perhaps even a wireless network – I'm assuming that you're just getting started. My hope is that, if you do already have a network up and running, you may learn some valuable new information. OK, let's get started…

Design is extremely important, as are the materials you use in that design. You most certainly put a lot of thought into your vended laundry – where your washers and dryers will go; where the outlets will be placed; how much voltage each outlet should handle; and where the walls, doors and plumbing should be located. Undoubtedly, this all started on paper – perhaps hand-drawn, marked up and then professionally placed into drawings. The machines and materials you chose surely were of top quality to ensure the greatest dependability.

The same attention to detail and quality should be put into your network – quality in, quality out. At this point, you may be thinking, "That sounds great, but I don't know how to draw out a network, or what that even means!"

Don't worry. This is easier than it sounds. Having a floor plan of your laundromat allows you to draw out locations where equipment should be placed. If you don't have a floor plan, simply sketch one out. If you are planning on having a private secured network, as well as your guest network, mark them down accordingly.

A guest network is the public network that your patrons will use. The public network will be separate from your private network. Working our way backward (with the wireless access points) – mark the areas in which you want guest wireless connectivity. Don't be shy – even if you want wireless in the restroom – mark it down. Once you have decided where you want wireless access, you must decide on the type or speed of wireless you will provide. Wireless involves radio frequencies, and your choices (and advantages/disadvantages of each) are as follows:

2.4 GHz

- Most compatibility
- Longer range
- Greater dependability as you move around
- Passes through certain materials better
- More congested
- Greater interference (from nearby noise/devices)
- Slower speed
- Less channels (equates to fewer communicating connections)

5 GHz

- Faster
- More channels (more communicating connections)
- Less congested
- Degrades more as it passes through materials
- Shorter range
- Less dependability as you move around

2.4 GHz is the most common and most widely used frequency band for wireless devices. A great number of devices – including mice, cameras, printers, walkie-talkies, watches, remote control lightbulbs and even microwave ovens – use 2.4 ghz. While highly convenient and readily available, this also is a reason you may choose not to use it. Think of 2.4 GHz as a multi-lane highway with a 55-mph speed limit that merges down to one lane. The more cars, the more congestion. If the road drops down to one lane, everyone must halt to allow other vehicles into the single lane. Wireless is the same way – especially 2.4 GHz. Less channels (lanes) mean less traffic can pass. More traffic (devices) means more congestion, which in turn causes more collisions, slowdowns or falling off the road altogether (drops). If you place your wireless access point next to a microwave oven, chances are that someone's frozen dinner will cause issues with your wireless connectivity.

On the other hand, 5 GHz has more channels (lanes), is faster (think 85-mph speed limit) and can handle more capacity (big trucks vs. cars). Given this, why would you ever want to use 2.4 GHz, if 5 GHz is so much better? Simply put, 5 GHz drops off (slows down) rather quickly as you move around. Also, this frequency doesn't pass through objects very well, which lessens the signal/speed. Your customers want a good experience to go along with the convenience – and signal and speed definitely make a difference.

We've already discussed antennas and the fact that all access points have them, whether you see them or not. This may have seemed like obvious and perhaps useless information, since I didn't follow with any immediate information on the topic. However, now it's time to understand the importance of the quantity and type of antennas that your wireless access points may have. Picture yourself tossing a stone into a pond – envision the circular ripples proceeding out from the center and growing larger as they move farther away from the entry point? This is how omni-directional antennas work; the RF signals transmit in a similar fashion. Omni-directional antennas work differently than the other popular antenna type, which is directional. The best way to visualize a directional antenna is to imagine yourself standing at home plate on a baseball field. Home plate would be the wireless access point, and the pie-shaped field would be the transmitted signal. If you stand facing forward and place each arm diagonal to the left and right, you would be mimicking how a directional antenna works.

As you take the time to draw out and mark the spots where you want to have wireless access, the visualization technique you just learned will help you immensely. Picturing the pond ripples or the baseball diamond will enable you to choose what type of access points to use and where you should place them.

Since height is might (but not always), omni-directional devices are best suited to be ceiling-mounted, and often the best place to install them is center to where you want your mobile devices to be used. The center of the room is generally a great place to mount them. Of course, this is not always possible and certainly not always ideal. Depending on your store, your centrally located access point may offer much more access to your parking lot then it would other areas of your laundromat. In other words, depending on the size and shape of your location, "ideal" isn't always best. Many devices come with both wall- and ceiling-mounting brackets, so you often have a choice of both. There is nothing wrong with a wall mounting, and you may have noticed that many access points are indeed mounted to walls. Quality devices will work well for you and your customers, whether on the ceiling or the wall.

Now that you know where you want access and you've thought of places to install the hardware, look around the space and consider the materials and machines that are nearby. Not all materials can pass your signal – and some will even bounce, absorb, scatter or block them altogether. Also, never place your Wireless Access Point or any other network hardware near or on something that gives off a lot of electromagnetic fields/interference (EMI). This includes:

- Electrical boxes
- Electrical conduit
- Microwave ovens
- Fluorescent lights
- Washers and dryers
- Electric wires
- Essentially, anything electrical that is not computer-network-related

What's more, keep in mind the materials, walls, etc. that will surround your device. Aside from the above list, the following will help you further identify what is good or bad:

Type of Barrier (Interference Potential)

- Wood (Low)
- Synthetic material (Low)
- Glass (Low)
- Water, which includes people (Medium)
- Bricks (Medium)
- Marble (Medium)
- Plaster (High)
- Concrete (High)
- Bulletproof glass (High)
- Metal/mirrors (Very high; no signals can pass through mirrors – they just bounce off)

You may need to use additional access points for the sake of the surrounding materials. Where you place a WAP may work great for a section of your desired signal; however, the material nearby may block or hinder further access. This is another area where visualization is helpful. You can picture where the RF signals will stop or have trouble passing through by using the above barrier/interference list.

Once you've finalized the placement of your devices, you must move onto the backbone of the network, which is the low-voltage cabling. You must use quality materials and have your cables installed properly. Quality Category 6 cabling should be used from your network equipment to each WAP. Category 6 is less susceptible to EMI, can pass traffic faster and is a better choice than Category 5e cable.

When purchasing access points, pay attention to how they are powered. Many business devices are PoE, which stands for "Power Over Ethernet." Traditionally, these devices don't have power supplies. They are powered over the cable themselves. Some WAPs come with power injectors, which require two cables per device. One connects to your LAN (network) and the other connects to the access point. Others don't come with power injectors and require you to plug into a PoE capable network switch. Access points, such as the Ubiquiti Unifi, come with power injectors. And these power injectors are the preferred method, as they guarantee the AP will receive the power it needs; as a result, you won't have to worry whether or not your switch is PoE, or if that switch has enough wattage to power your 2.4 GHz or 5 GHz wireless device.

Our next step is to dive directly into the world of network types and configuration options, including such topics as:

- RF noise discovery
- Wireless signal/ channel testing
- Securing your network
- Technical requirements/options

By now, you likely have already drawn out the desired placement of your Wireless Access Points. Perhaps you already have Wireless Access Points in place and wish to increase their signal or dependability. Think about who your wireless is for. In other words, are you installing just to support your business, or are you installing to support your customers?

Perhaps you wish to have a wireless network for you (Private) and a wireless network for your customers (Public). We will go over all of those scenarios soon. The first step was to draw out your AP locations; the second step was to be mindful of the objects and materials surrounding those locations; and the third step is to survey the desired locations. Using a quality smartphone or tablet, download the following applications:

- A wireless analyzer
- An EMF/EMI detector

A popular (free) choice on Android is WiFi Analyzer, created by Kevin Yuan. A wireless analyzer finds and analyzes wireless signals, channels and neighboring Wireless Access Points. WiFi Analyzer offers a window into how many devices surround your laundry, the channels they are using and how congested those channels are. You will be amazed at how many signals pass through our brains every second of the day. Using this information will help you configure and place (or replace) your Wireless Access Points.

Open WiFi Analyzer and swipe back and forth on the screen to see the various views. Don't feel overwhelmed – the presentations may look intimidating, but they are fairly straight forward. If you have used or seen a stereo equalizer before, you already have an understanding of what some of the screens depict. The needle to the right indicates a strong signal; the needle to the left means weak signal. Graph near the top means the strongest Access Points, while the graph near the bottom signals the weakest. Many stars – less congested channels; few stars – more congested.

However, strong signal strength doesn't always equal capacity. Just because the signal is strong doesn't mean you will have the best quality. Essentially, you can have a strong signal, but the noise around your device may interfere with the data to and from your device. Since all wireless devices contend for their time to "speak," paying attention to the channel congestion (the stars) is important. Think back to our example earlier in this series, with cars passing through a tunnel – the more cars on the road (the channel), the more cars that need to wait to get through that tunnel. If you've got a one-lane road, that means one car at a time. We'll come back to using the WiFi Analyzer later.

On the other hand, an EMF/EMI (Electromagnetic Field and Electromagnetic Interference) detector doesn't search or analyze wireless signals per se, but it allows you to "see" the electrical fields around you. The importance of this traces back to the example of the drycleaning business and its extremely poor network experience. All of the slowness, drops and overall issues were related to EMI. An EMF/EMI detector allows you to visually see the electromagnetic fields/electromagnetic interference (by way of onscreen numbers and graphs) that may cause troubles. High EMF/EMI is bad for your cable runs, as well as your wireless signals.

Once you've downloaded and opened an EMF detector, you can move your phone or tablet around the area in question. Taking note of how high interference is adjacent to where you want your wireless devices and access is important. Expecting a quality signal around heavy noise devices is like expecting your car's clean, newly changed oil to flow perfectly through a dirty oil filter. Use both apps to better install or rearrange your WAPs.

The Wi-Fi analyzer detector also will come in handy to test your signal as you move around a space. The analyzer, along with an EMF/EMI detector, can be used prior to actually mounting your hardware. Taking the time to walk your space and validate your ideas will save you from accidentally mounting hardware in the wrong places.

OK, you've got the internet. You've run your cabling. You've mounted your WAPs. You're excited and ready to go. Let's do this!

Not so fast.

You've only done the front-end work. What was your decision on why you wanted wireless? Are you installing everything to support your business itself, or was your end game to support the public? Perhaps you wanted both.

Securing Your Network: Technical Requirements and Options

When it comes to IT, just like medical advice, always seek the assistance of a professional to ensure you are properly installing, configuring and securing your network. All of these options are provided for informational purposes and to help guide you toward your goals. Using this information will assist in enhancing your knowledge and providing your IT firm a good roadmap as to what you're looking to achieve. Many devices come with easy-to-install wizard-based installations; however, it's always a good idea to have an IT professional install or validate the installations to ensure security, protection and confidence.

We will stick to the four most common scenarios/options. Which option resonates with you will depend on what type of wireless network you desire – private, public or both. If you plan on having both a private (secure) and public (guest/unsecure) network, always have a firewall in place to protect your assets. Options One and Two include a firewall and are the more advanced options of the four. Redundancy here is intentional. If you plan on having a secure private network, a firewall is a must. A business firewall, such as Sonicwall, is suggested.

Sonicwall has a line of security appliances designed for small businesses, which include the Sonicwall SOHO and TZ series. They are excellent devices and help secure your network even further when coupled with the Comprehensive Gateway Security Suite.

When installing any piece of hardware or having hardware installed, always ensure that the default password is changed. Default passwords are readily available and should absolutely be changed on every device. Difficult passwords are your best choice, and the longer the better. The same holds true for wireless network passwords.

The more you care about your data – the more you should protect it. Easy passwords are almost as bad as default passwords. Never use personal information in any of your passwords, as personal information is easy to come by. This includes – but is not limited to – your company name, family member names, family birthdays, family pets, etc.

Also, be certain that the latest firmware is installed on your hardware devices. Firmware is the software that not only tells your device how to do what it does but also keeps the devices secure with the latest security patches. Hardware is only as secure as the security patches/upgrades that you keep up with. Again, an IT group is recommended to make sure you're up to date and continue to stay up to date.

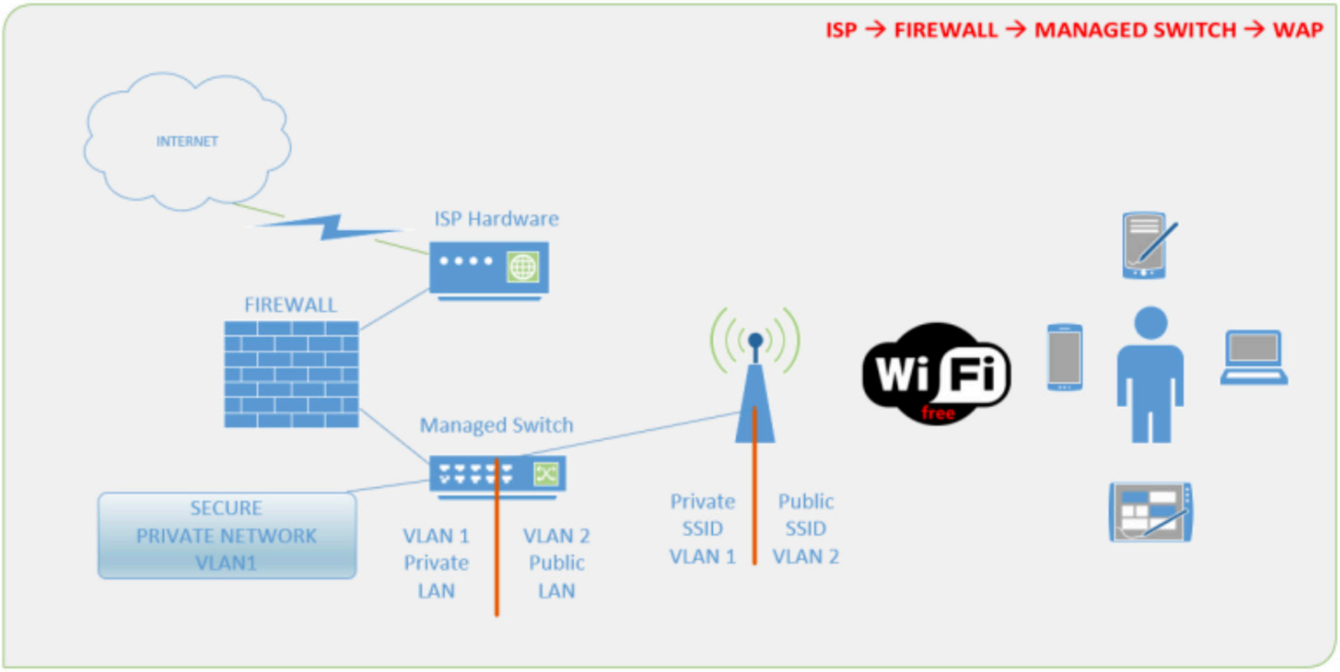
The headings of each option are meant to give you a quick outline of how each device ultimately connects to the next. The options show one single access point for each network type, but it can depict multiple access points with the same network names (SSID). In Option One, you see "ISP → FIREWALL → MANAGED SWITCH → WAP." On a very basic level, think of the old song "The toe bone's connected to the foot bone, the foot bone's connected to the heel bone…"

NOTE:

Options One and Two should be the first choices for laundry operations that have their business entities attached to their laundromat, drycleaning facility, etc. In other words, if you run your business from a single location (accounting, etc.), the first two options are a must; hence, the more advanced configurations. These entities typically will have multiple PCs, documents and spreadsheets, as well as management and accounting software to run your business. You may only have one single computer that handles all of this – but even that one computer may be your business' lifeblood. (As a side note, backing up your data is a completely separate topic, but it must be mentioned – back up your data and then back it up again! Securing your business, including the digital assets, is of utmost importance.)

Options One and Two are also highly suggested if you are taking digital payments, as firewalls help to further secure those devices.

OPTION ONE



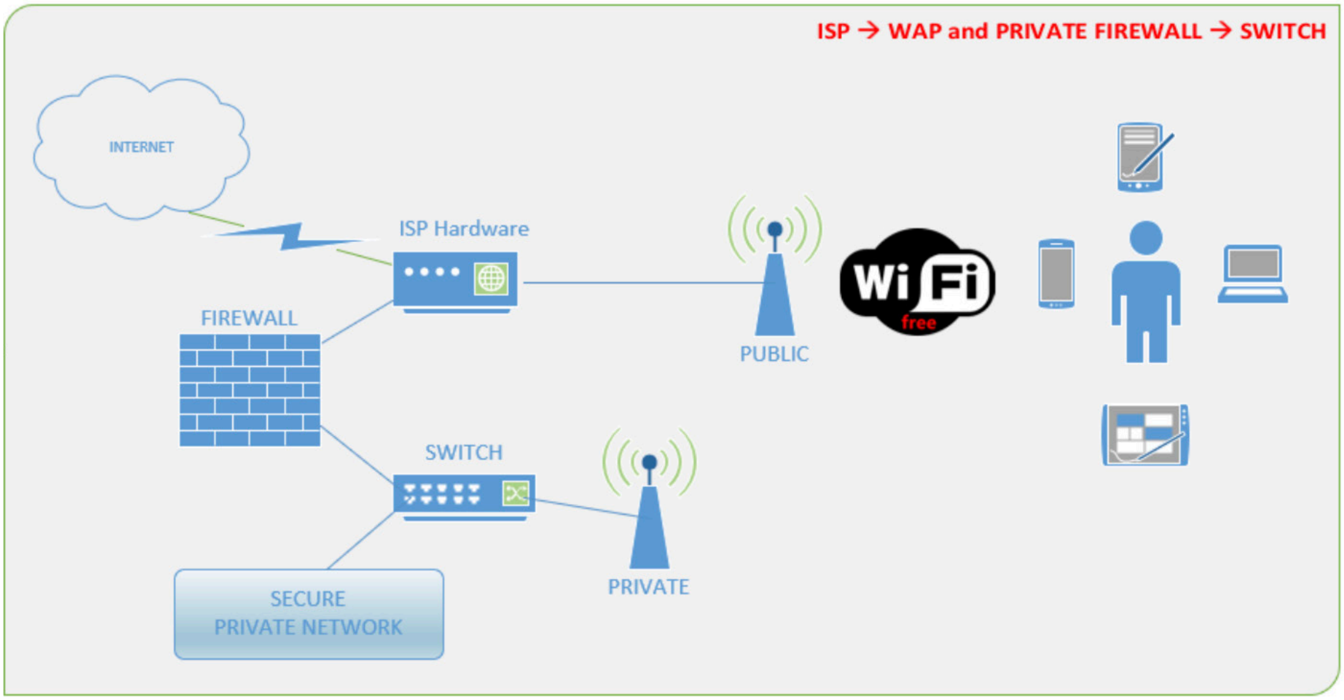
Option One Highlights

- Private and public networks
- Firewall
- Managed switch
- VLANs
- Access Point with both private and public SSIDs

With Option One, your ISPs hardware is connected directly to a firewall, and the modem is used strictly as a gateway to access the public internet. The firewall manages connections to and from your network and secures it as such. The firewall connects to a managed switch, which has two VLANs. VLANs (Virtual LANs) allow you to have multiple networks (subnets). In this case, one network is your private secured network and the other is the guest network. Each VLAN will be connected to its own port on the firewall, which would be configured to communicate with each network (private and public) completely independent of each other. When configured properly, traffic (data) from the guest network will not be able to access any part of your private network. The same is true for your private network – when configured properly, your private data on VLAN 1 should not pass over to the guest network on VLAN 2.

With this option, we are taking advantage of a Wireless Access Point's ability to have two completely separate networks and two completely separate network names (SSIDs). You and your employees will connect to SSID 1 ("Laundry-Private") and your guests will connect to SSID 2 ("Laundry-Guest"). Although the networks are separate, you may not want to make your private network name obvious.

OPTION TWO

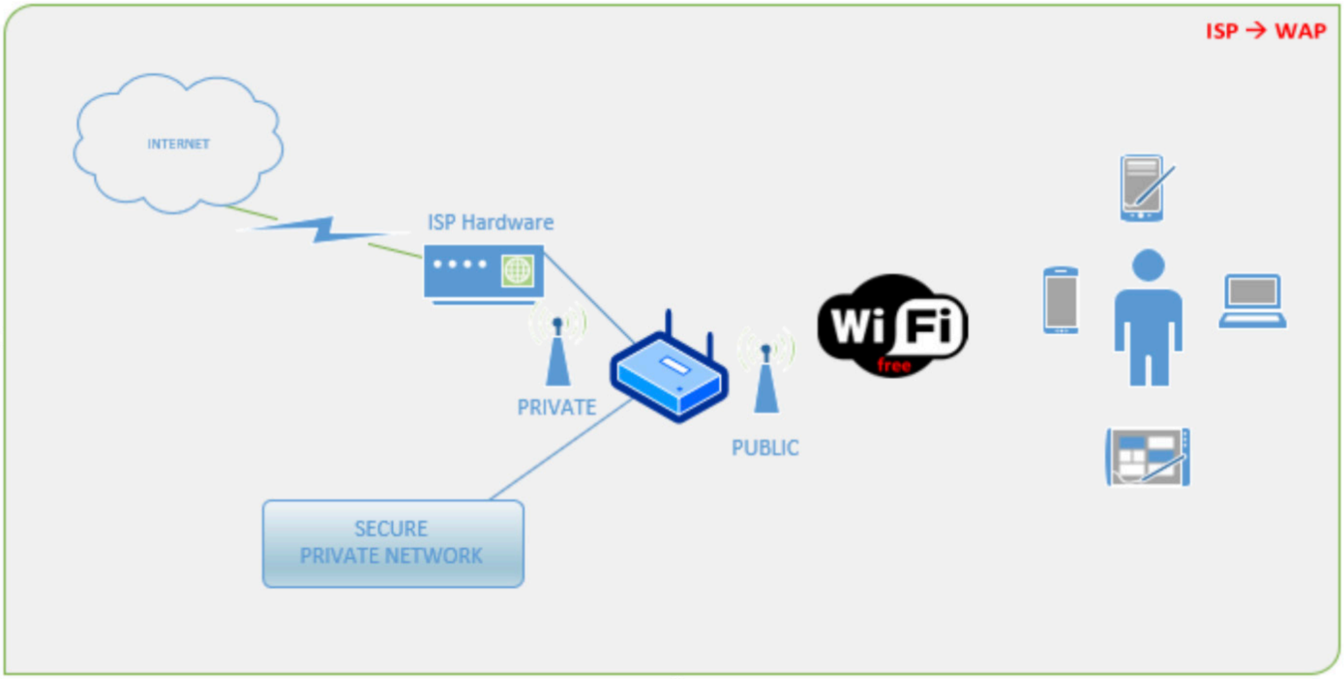


Option Two Highlights

- Private and public networks
- Dedicated guest WAP direct to ISP
- Firewall dedicated to private network
- Unmanaged switch
- Dedicated private WAP

Option Two physically separates your private network from the guest network. This allows you to provide wireless to your customers without having to think about whether or not a separate firewall port or VLAN is configured properly. Due to the fact that the guest wireless access point is connected directly to the ISP modem and not directly to your firewall, you don't need to configure a separate port or VLAN on your firewall. Also, with this configuration, there is no need to configure and secure a managed switch to support two separate networks. This is obviously much simpler than Option One and may be a good choice for many laundries that have a private network and still want to offer guests internet access. Since the guest wireless network will not be plugged into your firewall, the firewall will see guest traffic the same way it sees internet (WAN) traffic – as unsecured public data. WAN should always be blocked from passing through to your private network (LAN). Firewalls generally block WAN to LAN by default.

OPTION THREE

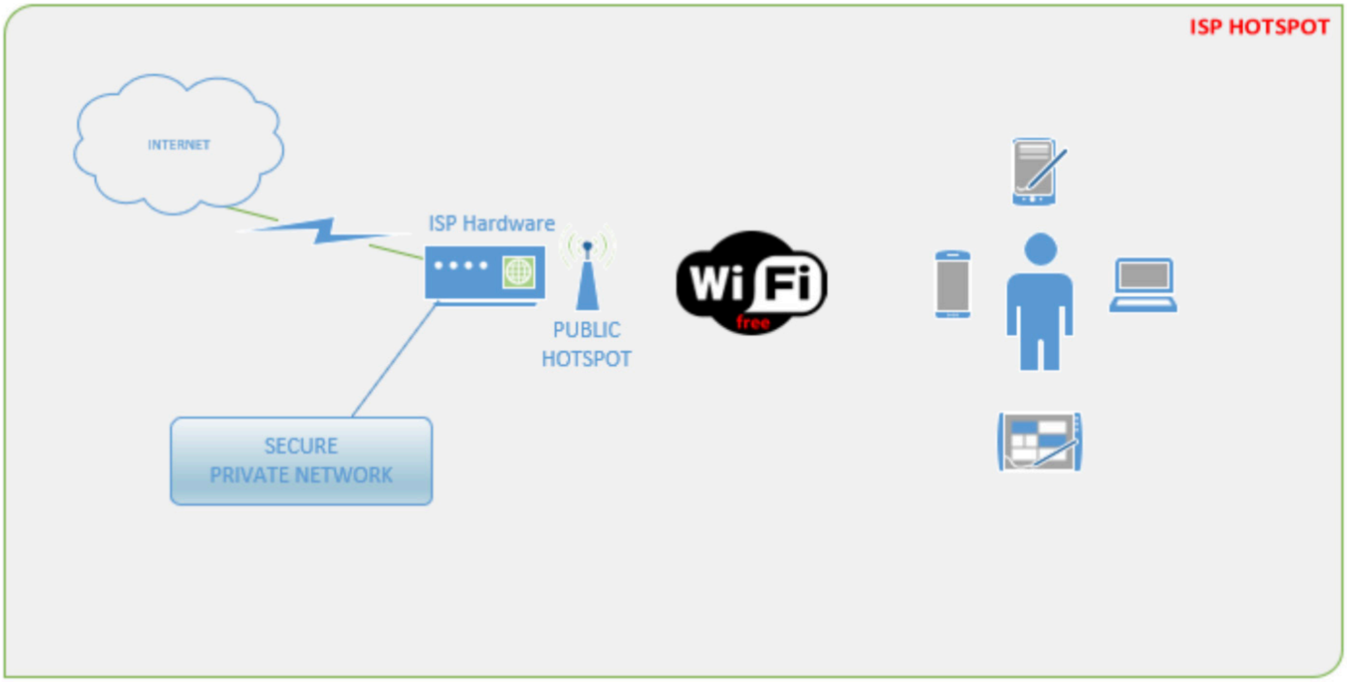


Option Three Highlights

- Private and public networks
- No separate firewall
- Access Point with both private and public SSIDs

Option Three offers a simpler possibility and is designed for use where you don't necessarily conduct business in your space, but you do occasionally wish to connect your laptop or you have hardware such as cameras installed. The Wireless Access Point should have a built-in firewall and should be designed to keep private and public traffic separated.

OPTION FOUR



Option Four Highlights

- ISP modem only
- ISP built-in public hotspot
- Private network

Option Four is actually more secure than Option Three. You're relying on the firewall capabilities within your ISP's modem to protect your private network. The hardware that is provided is often very similar to the hardware you would have at home. All of your devices plug into the ISP modem – you may even take advantage of the wireless capabilities of the modem.

In this scenario, your guests never actually connect to your network directly. How do they connect? They will connect to the "hotspot" feature provided by the ISP.

What's a hotspot? I will use Chicagoland as an example and – depending on your location – you may see the same. Here in Chicagoland, Comcast/Xfinity has public hotspots nearly everywhere you go. When you search for Wi-Fi, they show up as "xfinitywifi." If you have an Xfinity account, you can use all of these hotspots for free. If you don't, you have the option to pay for blocks of time. This is made possible by all of the modems that are installed throughout the city (including homes). Many of their devices that have built-in wireless have separate hotspots that are always broadcasting for people to connect to. According to Comcast, "the Xfinity Wi-Fi service is designed to work on a separate network so that your home (insert business) network remains entirely secure."

This option is very convenient for many customers and often the simplest, as many people have Xfinity. Your ISP may also provide you with stickers promoting your laundry as a hotspot. However, keep in mind that allowing this will not enable you to capture any statistical usage data or present your patrons with a landing page or sales materials.

Managing Multiple Applications

Next, let's discuss managing multiple applications. Managing devices is much simpler using web-based interfaces. Therefore, everything here will be based on devices that are configured via a web browser. Keep in mind though – just because a device has a fancy interface does not mean that everything is straightforward and done automatically for you. Let me repeat the standard disclaimer from throughout this paper: always seek a technical professional to ensure your settings and configurations are secure, especially with security devices such as firewalls. *Please note that we are only focusing on the "Technical Requirements" of Options Two, Three, and Four.*

OPTION ONE

- Private
- Guest/Public
- ISP ➙ Access Point

Private

ISP ➞ Firewall ➞ Switch ➞ PC's/Laptops/AP

Firewall

A firewall is the device or software that protects you from the outside world. Security is always of the utmost importance; therefore, a firewall should always be in place. The firewall can be a dedicated security appliance, such as a Sonicwall, or built into other devices, such as your ISP hardware, router, or wireless access point.

Software firewalls can be very good; however, they are usually installed on the opposite side of your firewall. In other words, traffic comes through and then you rely on software such as the Windows Firewall to protect you. The negative side of this is that you are allowing the traffic in and then relying on your computer to protect you.

On the other hand, dedicated hardware stops traffic before it can even see that your computer is there. People always ask, "Well, if that is the case, and hardware is so much better, then why do I still get viruses or get hacked?" This is simply because you use applications on your computer that allow traffic in – a web browser, a downloader, a movie player, etc. Any of these applications can have holes that open you up to infections. This is one of the reasons we always push for additional protection on your computer.

Since your device is only as secure as the software it uses, having the most up-to-date firmware is extremely important. One of the downsides of using discontinued hardware or out-of-date (end-of-life) legacy hardware is that the protection is not as strong as up-to-date devices. Always keep this in mind when shopping. Saving a buck can cost you a lot more in the future. Now onto the fun part – configuring!

Backing up your settings is as important as backing up your computer data. You would hate having to reconfigure your devices if anything were to happen. Back those up so that you always have a copy of your hard work.

The first step in configuring your hardware-based firewall is to plug in your internet line to the WAN/internet port. Now, plug your switch into the LAN port, and then your laptop or PC into the switch. Ignore the Wireless Access Point and additional PCs and laptops for now. We first need to configure the firewall. Follow your manufacturer's quick setup guide to find the default IP address of the firewall. You will connect to your hardware using that IP address via a browser. Since many devices give you an address and access to the network right when you plug into them (via what is called DHCP), you will be able to proceed to Step Two easily.

The second step is to open your internet browser and enter the IP address given to you in the manual directly into the address bar of your browser. Such as http://192.168.1.1. Now enter the default username and password that was provided.

Once logged in, go through the wizard and choose your setup. Depending on the manufacturer, you will be asked what type of connection your laundry has. Cable? DSL? Dialup? Your answer tells the firewall how to give you internet access. At this point, you may also be asked what subnet you want your LAN to be on. Think of a subnet as the street your house is on, and your home address as the IP address. No two houses on your street can have the same address, and different computers should never have the same IP address. The subnet such as 192.168.1.0 is different then 192.168.2.0. Feel free to leave the LAN settings as they are. Depending on the device, that is not uncommon.

The third step is to change the default password of the device to a secure password of your choice. Remember that the more difficult and longer the better. Also document this information in an inconspicuous area – if you lose your password, then you will have no choice but to reset the firewall to factory settings and start all over again.

The fourth step is to register your device and then download and install the latest firmware. Your firewall will most likely warn you that it will need to reboot and then take up to five minutes to come back online. Once it has finished installing the new software, connect back to your firewall and enter the username and your new password that you previously entered.

The fifth step is to ensure everything is secure and working properly. Test the internet and also go to *www.grc.com* and look for "ShieldsUP!" which has a few wonderful web-based tools to test your security. Again, having an IT professional is always suggested to make certain you are truly secure.

Once you know everything is in order, you can connect your additional devices, which may include multiple PCs, laptops, etc. Are they able to all get online? If so, nice work! We can now begin the configuration of your Wireless Access Point(s).

Wireless Access Point (WAP)

How you log into your WAP will depend on what kind of access point you purchased. Did you buy a "controller-based" AP or a "controllerless" AP? As an example, the firewall you just configured can be seen as "controllerless" since you logged right into the device and did not need a "man in the middle" to configure. Controller-based access points require you to log into a controller, which is "software" separate from the access point. The controller can still be web-based but you don't log directly into a controller-based access point. Although they can be more involved than controllerless – as previously mentioned – they often offer far more control over one or many access points from one single interface.

Your access point may also have a power injector. The power injector plugs into your LAN (your switch) and the other port on the injector, which is generally labeled as PoE, plugs into your access point. If you purchased a PoE WAP and did not receive a power injector, you must use a PoE switch. PoE stands for Power Over Ethernet, which means exactly what it says. The device receives its power over the ethernet cord, which is plugged into an injector or a PoE switch. All we need at this point is for you to power it up and plug it into your new switch.

Access points can be configured in one of three ways. One, using software that you received. The software will scan the network for your new AP and allow you to configure everything from the software. Two, you need to plug directly into the AP with your computer and give yourself a static IP

address to connect to the default IP address of the unit. Or, three – the WAP will receive an address from the firewalls DHCP server, and you connect to the given IP address.
We have to assume that you have the IP address and are connecting to the device using one of the methods below. All devices are different and, therefore, the steps shown may not be in the same sequence as the device you have.

Controllerless

1. Open your browser and enter the IP address of the wire less device, as well as the given username and password. Following similar steps as the firewall, go through the default settings.

2. Again, similar to the firewall, if you were presented with a wizard – run through the choices/options and change the default password of the device to a secure password of your choice. Keep to the rule of the more difficult and longer the better.

3. Register your device and then download and install the latest firmware. Your AP will most likely warn you that it will need to reboot and take some time to come back online. Once it has finished installing the new firmware, connect back to your WAP to complete the steps.

4. Create your wireless network. Give your private wireless network a name (SSID) that makes sense to you. Set a difficult password using at least WPA2 encryption. Same rule applies – passwords – do not make them easy!

IMPORTANT NOTE:
WPA2 security was cracked in 2017 and has put an extremely unfortunate number of devices and personal/private information at risk. Installing the latest firmware and security updates is even more important than ever. Many manufacturers have already patched or are working on patches for WPA2 security. Sadly though, companies often disregard older devices no matter what you paid for them. This brings to mind the importance of keeping up to date with both software and hardware. Research your devices and check with the manufacturers to see if they have patches available. Google "WPA2 Security," "Krack," "WPA2 Patch," etc.

Controller

You may have purchased a single access point, which requires a controller (such as a Unifi). Or you may have purchased many. Controllers help manage multiple APs by allowing you to manage and configure them all from one location – the controller.

1. Connect your access point or all of your access points to the network and allow them to power on.

2. Install and run the controller software, which may then open a browser for you to login to.

3. Configure the network settings as well as your wireless network settings similar to the controllerless steps. The joy here is – when done properly – the configurations you make will flow automatically to your access point(s). Future changes and updates will work the same – the controller allows you to control everything from one single point. Yes, this includes firmware upgrades.

4. Once your settings are complete, including your wireless network settings and security, following your particular products manual – allow your settings to propagate down to your single or multiple WAPs.

5. Once you are sure your Access Points are up to date and configured properly (again – always advised to consult an IT professional), begin connecting devices and testing your wireless network.

Guest/Public Network

Configure your guest Access Points using similar steps as your private network. The main difference here is the guest network should not have (nor ever have) access to your private network. Guest networks are not secure, and you have no control over the devices that connect to them. In other words, there is no way for you to know whether or not John Doe's laptop is full of viruses or if Jane Doe is a hacker looking to steal everyone's data. Always make absolutely certain that public networks can't access the private network.

With Option Two, the guest network is plugged directly into the ISP modem and your firewall is blocking the guest network. This option is more secure than Option Three.

Option Three is relying on a device that offers both private and public networks from a single box, which is not a dedicated security appliance. Although this may be business hardware, this is similar to your home setup. Be extremely mindful with Option Three configurations.

Option Four, in which you are using your ISP hardware for your basic private network, is more secure than Option Three. The reason being that this option is taking advantage of the ISP's public hotspot feature. Unfortunately, however, with Option Four you have no way of keeping track of usage, configuring capture pages, advertising, etc. This option offers convenience for your customers but no possible wireless revenue for you – aside, of course, for the fact that they may choose your location over another due to the available hotspot.

Remote Administration

Lastly, making changes to your devices, as well as viewing access logs and usage, goes with the territory of managing your own equipment. How do you do this if you are not always in the office or if you want to keep manual tabs on how many people connected to your network after you ran a special or event? Simple. There are multiple ways of going about this. Depending on your hardware, a few choices are:

1. Use remote control software, such as LogMeIn, on a computer at your office. Log into that machine directly and access your devices.

2. Configure the remote administration feature on your devices that allow access from the internet. (Be very careful with this one.)

3. Use a network-based controller, which is always securely available.

4. Use a third-party service from your manufacturer that allows remote access, logging, and reporting of usage, etc.

This concludes our journey into wireless networks. Hopefully, you now have a fuller understanding of this important and sometimes complex topic.

The Coin Laundry Association provides this paper as a general educational tool. It does not replace the judgment of qualified professionals based on individual facts and circumstances. The CLA disclaims liability based on the use of this paper. Regarding legal matters, advice should be sought from a licensed attorney.

Check out all of the Coin Laundry Association's White Paper topics at *www.coinlaundry.org*

Gold Book
Research Series
Your Guide to Laundry Excellence