# How to Design and Troubleshoot Your Wi-Fi Network

EIRE

Wi-Fi networks allow the effortless connection of multiple devices to internal resources and the internet without the constraints of using physical network cables. With mobile devices fast overtaking desktop devices, wireless internet is no longer a luxury; it's necessary. As transmission speeds increase, so does the speed of technological progress. This article explores everything you need to know about how to design and troubleshoot your Wi-Fi network.

## Terminology You Need to Know

Let's look at some of the most critical terminologies you'll need to know when configuring and troubleshooting a Wi-Fi network.

### Wi-Fi

Wi-Fi describes networking products that conform to the 802.11 wireless communication standards. You can find the certification emblem or Wi-Fi icon on practically any recent wireless equipment, and you'll also see a sticker with the logo in any place that offers a free Wi-Fi connection. Most network equipment now uses the 802.11 wireless communication standards. The term Wi-Fi is simply used to describe any wireless internet connection and the tools used to set it up.

### WLAN

A wireless LAN (WLAN) is a wireless computer network that links two or more devices using wireless communication to form a local area network (LAN). You'll find LANs in most businesses, schools and homes, and while it's possible to have more than one in your office, it's uncommon.

### WPA, WEP and Wardriving

Understandably, network security is a priority for every Wi-Fi user, including home and small business users. In the same way a TV can tune into a network broadcast, it would be just as easy for someone to tune into your wireless connection if there were no security measures in place. Anyone could tap into your network, use your credentials and spy on what you're doing.

The practice of Wardriving helped focus people's attention on WLAN vulnerability. Smart tech enthusiasts used cheap, homemade equipment while walking or driving through different neighborhoods, showing that it's possible to snoop on nearby homes' internet traffic. War drivers found they could log into people's home networks, stealing free Wi-Fi access from unsuspecting bill payers.

Wired Equivalent Privacy (WEP) was the initial solution to the problem. It encrypts network traffic using algorithms so that computers can read and understand the information, but people can't.

While WEP became outdated a few years back, other security options such as Wi-Fi Protected Access (WPA) replaced it by improving on its authentication and encryption features. All popular wireless equipment supports WPA, and it protects you and your computers from prying neighbors, opportunistic war drivers and anyone else looking to access your personnel information. WPA can be toggled on and off, so be careful to set it up correctly in the first place.

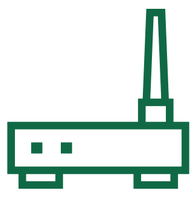
## 802.11a, 802.11b, 802.11g, 802.11n and 802.11ac

Created and maintained by the Institute of Electrical and Electronics Engineers (IEEE) LAN/MAN Standards Committee, these codes represent the most widely used wireless communication standards. While it's possible to build your wireless network using any of these standards, 802.11ac (also known as Wi-Fi 5), utilizing dual-band wireless technology, is widely regarded as the fastest and most efficient choice.

The latest iteration of these standards is 802.11ax (marketed as Wi-Fi 6), which will be exponentially faster than its predecessors, with overall throughput improvement (over an entire network) of 400%, however, we do not have the devices (phones, laptops etc.) to support this standard yet.

# Wireless Equipment

There are three main types of wireless equipment needed to build a Wi-Fi network: a wireless router, a wireless network adapter and a wireless access point. Some might be optional, depending on the network settings and your requirements. One thing you won't need is an Ethernet cable!



## Wireless Router

A wireless router is a device that performs the same functions as a router on a wired network. It includes the functions of a wireless Access Point or AP and firewall technology to improve your network's security. It is used to provide access to the Internet. Depending on the manufacturer and model, it can function in a wired local area network (LAN), a wireless-only LAN, or a mix of both.

The wireless router can disperse signals throughout an entire office. As such, when it comes to ensuring the whole building is covered by a reliable Wi-Fi signal, a WLAN with a combination of a wireless router and APs is best.

If your wireless LAN design does not include a wireless router or APs, your network adapter will need to run in ad-hoc mode (ad hoc is a communication setting that allows computers in the Windows operating system to directly communicate with each other without a router). On the other hand, if your network connection includes APs, you should run all Wi-Fi adapters in infrastructure mode.

## Wireless Network Adapter

Every desktop and mobile device that's paired to a WLAN will have a wireless adapter. Early adapters were commonly implemented on expansion cards that slotted into your computer. However, most newer computers have a network interface built into the computer motherboard or connect to a USB connected dongle. For laptops, wireless adapters used to look something like a sturdy credit card, but they're usually now small chips, like what you'd find in a smartphone, tablet or other wireless device.

Wireless network adapters contain a radio receiver and transmitter, known as a transceiver. The function of wireless transceivers is to translate, format and organize the flow of information between wireless networks and the computer, and thus send and receive messages.

When building your office network, one of the first steps is to find out how many devices are already equipped with a network adapter that can connect to the Wi-Fi network. You can look at your devices' technical specifications to find out if they already have built-in network adapters.


### Access Point (AP)

A wireless AP is a network hardware device that allows other Wi-Fi devices to connect to a wired network. Also known as base stations, APs are lightweight, slim boxes often with flashing LED lights on the front. In your office environment an AP will connect with multiple wireless devices within its range (PCs, laptops, mobile phones), to a pre-existing internet connection via their one wired connection.

## Installing a Wireless Router

A single Wi-Fi router supports a single WLAN, so you'll need a wireless router whenever:

- You want to simplify the WLAN installation process
- You're rebuilding your office network so it's all wireless

If you are working in a small office, install the wireless router in a central location so the Wi-Fi signal has the best chance of reaching all devices. In general, when it comes to wireless computing, being closer to the router means better internet speeds and fewer network issues. Here are the steps you take to set up your wireless router:

1. Connect the router to a power source and an internet connection/modem provided by your local internet service provider.
2. Select the network name, which is often called the SSID. It's recommended that you amend the manufacturer's default name to something you've configured yourself for security reasons. You can find the network name in your product's documentation.
3. Use the documentation that comes with your router to turn on firewall features, enable WEP security and set the necessary parameters.

## Install an Access Point

You will need to use a wireless AP if you are a medium to large organization, in this case:

- You are not planning on using Ethernet cables
- You wish to connect multiple computers/devices to your network
- Your office is too large to be covered by a single wireless router

Connect the AP(S) to your modem and router via a LAN cable. Set a Wi-Fi network name and ensure you have WPA2/WPA3 enabled.

## Configure Wireless Adapters

Once your AP or router is up and running, it's time to configure the Wi-Fi adapters. Your product documentation should provide step-by-step instructions for installing the adapters to your devices. All Wi-Fi adapters require that you've also installed TCP/IP on the host computer.

All manufacturers offer configuration resources for adapters. For example, on Windows' operating system, there's a graphic user interface you can access from the taskbar or start menu once you've installed the hardware. You can use this GUI to set the SSID and turn on WPA2/WPA3, as well as to be able to control other parameters.

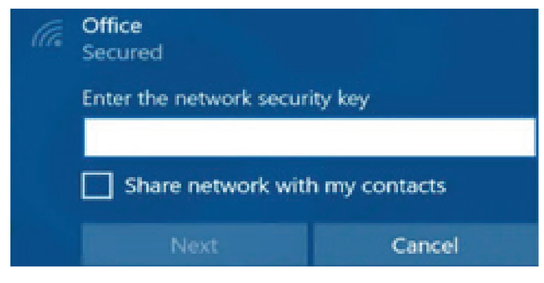
## Configure WLAN

All Wi-Fi adapters require that you select between infrastructure mode and ad-hoc mode. Most offices choose infrastructure mode so adapters can automatically discover their WLAN channel number and match it to the AP or router. Alternatively, if your office has fewer than three computers and they're all located close to each other, the ad-hoc mode might be sufficient. It's also a pretty decent fallback in case your router or AP breaks.

# Pre-shared key Authentication

Most home Wi-Fi deployments use a Pre-shared key to permit access to the wireless network.

A Pre-shared key is an agreed-upon string of characters that a user inputs after selecting the appropriate network SSID. The benefit of this authentication method is that it can be shared relatively quickly, especially in a home environment. However, keeping track of who has access to a key can be very difficult. If you ever have any security concerns and need to change the key on an AP, you will also need to manually change it on all clients connecting to that AP.




Having a way to authenticate users without having to input a shared wireless key individually is a huge time saver as well as being more secure. To do this, you can set up Radius authentication to dynamically manage your security keys.

# Radius Authentication

The Radius protocol, short for Remote Authentication Dial-In User Service, uses a remote server that provides authentication and accounting facilities to various network appliances and provides the following:

- Authentication - Verification of the user.
- Authorization – Control of the level of access permitted.
- Accounting – Collection of session information (what/when the user connected etc.).

In a wireless environment, we can use Radius to leverage a pre-existing database, e.g. active directory, for authentication.

## Advantages

- Users can be authenticated with their PC login credentials, which are updated dynamically on the server.
- Identification of users with the credentials they use to access the wireless.
- Pre-shared keys can be phased out, so reduced risks of unauthorized access, no need for downtime to share new password with all users.
- Deletion of a user account also removes access to the wireless network.

## Disadvantages

- Additional configuration of server, firewall or local database is needed to implement.
- Multiple incorrect login attempts may lock user account if using active directory.
- Domain username syntax can occasionally cause issues for users.
- Point of failure increase - authentication relies on the radius server itself and connectivity to it.

# How to Troubleshoot Wi-Fi Network

Finished your setup but still don’t have a Wi-Fi connection?

If your internet isn’t working correctly straightaway, don’t worry - it happens to the best of us. Here are some tips for methodically troubleshooting your wireless adapter and performing Wi-Fi signal strength and speed tests, plus wireless diagnostics for the main types of connection problems you’re likely to come across.

Underlying issues with the wired network carry over to the wireless network, so ensuring convergence of all routing protocols and connectivity to default gateways is essential.

Below are some common issues and solutions:

## SSID is not visible

- Confirm Wi-Fi router is powered on.
- Confirm Wi-Fi is enabled on the laptop/tablet/airplane mode is disabled (happens very often).
- Check SSID has been set to broadcast mode and not hidden. (If the SSID has purposely been set to hidden, every host device will need the network details entered manually before they can connect).
- Confirm 2.4Ghz/5Ghz radio setting (not a common issue but ensures client device support the active radios of the access point).

## Cannot connect even with correct password

- Confirm the password is correct with a device that is already connected (open up command prompt; windows key + R – type cmd then enter). Then in the command prompt: NETSH WLAN SHOW PROFILE “wireless network SSID” KEY=CLEAR.
- Test password with another device.
- If some devices connect, make a note of the devices that are having issues and look for a common theme. (Check client/wireless router documentation and firmware updates for bug fixes.)
- If multiple devices cannot connect, try resetting the password. Use a simple alphanumeric key first then change to more complex passwords to see if this makes a difference.

## Wireless access is slow

- Perform a speed test and MTR test on the wired network then on the wireless. (Ensure the wired network is operating flawlessly before suspecting it is a wireless issue).
- Relocate access points if possible, (ensure access point is not being blocked by large cabinets/ fish tanks or machinery).
- Ensure the access point is not oversubscribed with users (access points have a maximum number of clients they can serve).
- Confirm with IT if they are throttling or traffic shaping on the network (some companies set speed limits for certain types of traffic e.g., non-essential traffic).

## Wi-Fi connection is dropping

- Are you near an airport? (Avoid using the UNI-2/UNI-2 extended channels, these will automatically drop clients if a radar is detected).
- Proximity (confirm this is not a proximity issue by testing connectivity closer to the access point and then slowly moving away).
- Interference (investigate if this happens at a certain period or in a certain location). Certain wireless cameras/printers etc., can cause issues with Wi-Fi.
- Check the hardware (are APs and client drivers up to date and are there any faults with the client or wireless adapter)?

## Miscellaneous troubleshooting

- If Wi-Fi issues persist, try turning off the firewall to check if there’s a configuration issue.
- Use the control panel to check that you have a valid IP address.
- Check the wireless adapters of all connected devices to see if the problem is isolated to a single device.
- Toggle between ad-hoc and infrastructure mode in Wi-Fi adapter settings to check both the router and the access point.
- Create a backup and system restore point and reset devices to factory settings before going through the process again.
- Use your computer’s network diagnostic tools to get to the root of the problem. This only works with Windows, but it’s a helpful way of determining the problem, even if it’s something you’re unable to fix yourself. Right-click the network icon and select diagnose and repair. If you can’t find it, type “control” in the search box on the taskbar, click on the network icon, and click on troubleshooting which will walk you through some additional steps.

- Most Wi-Fi routers are DHCP servers, which mean devices can automatically connect to a network without someone manually setting up an IP address. Check the TCP/IP settings to ensure the computer is automatically getting settings configured by the DHCP server. If it doesn't automatically happen, you'll end up with a static IP address, which can be a problem. For an Android device, open the Wi-Fi option from the settings menu and select the network name. You can use the edit option to get to advanced settings and amend DHCP and static IPs.
- To troubleshoot the DNS server, you have a few options. First, switch to a different browser or try starting your computer in safe mode. If these options don't work, try temporarily turning off your firewall or antivirus software and checking if the internet works. If it does, you'll need to reconfigure settings or switch antivirus software.
- Try installing updates for all your computer's drivers.
- Amend the default DNS server if you have a Windows device.
- Flush DNS cache and rest your IP address.

## Let the Experts Take Care of Your IT Problem

At EIRE Systems, we're Wi-Fi experts, and we've been helping people master their IT systems since 1996. Get in touch today if you need help setting up or troubleshooting your wireless network.