STEPHOUSE

HIGH-SPEED INTERNET

Stephouse Networks: The Northwest's truly local high-speed internet service.

Securing and Optimizing Wi-Fi at Home

CONTENTS

INTRODUCTION 2

WIRELESS IS A MAGICAL DONUT: UNDERSTANDING ITS ANATOMY 4

SETTING UP: WHAT YOU'LL NEED & WHAT TO DO 6

SECURITY: PROTECT YOUR WI-FI CONNECTION 8

A GREAT START: LOCATION AND SECURITY 9

Introduction

Setting up your internet connection can sometimes be a hassle. Some of us are so happy to be done with the setup that we forget to consider some of the most basic principles of a properly secured home network: **coverage and security.**

Figure 1: Here's an example of a trusty wireless router.

A poorly set up network leaves you vulnerable to neighbors stealing your internet access via your unprotected Wi-Fi router. According to a D-Link and Wakefield research survey, about 31% of respondents admit to stealing Wi-Fi from their neighbors!

To protect your network from those pesky thieves, we've come up with a quick guide that explains a few home networking basics.

This guide is meant for:

- Internet users who are setting up a network for the first time in a new place.
- People who realize that they want better or stronger network coverage in certain parts of their home.
- Or, curious people who want to understand the basics of a home or small office wireless network.

Let's solve for these overlooked issues.

Often people will overlook one or more of the following issues when configuring their home network:

Location: It makes a big difference where you put your wireless router. Walls and other physical barriers will have a dramatic effect on the area that is able to receive a decent Wi-Fi signal.

Bottom Line: *Find a central, unobstructed location to place your router to get the best wireless coverage.*

Security: Securing your network is essential to those living in close proximity to their neighbors. If your network is unsecure, that will allow anyone with a Wi-Fi-enabled device to jump onto your connection and leech your internet away from you.

Bottom Line: *Always take the extra step of setting up one or two layers of security on your network to deter strangers from hopping onto your network.*

Wireless is a Magical Donut: Understanding Its Anatomy

Okay, it's more physics than magic. Imagining magical donuts seem like a more entertaining way to explain wireless signals.

Wireless radios will send signals in certain shapes and sizes. Yeah, there are a lot of them out in the world. Fortunately, most home and small office routers all have a similar shape.

Figure 2: The shape of wireless coverage from a generic router looks a lot like this delicious donut.

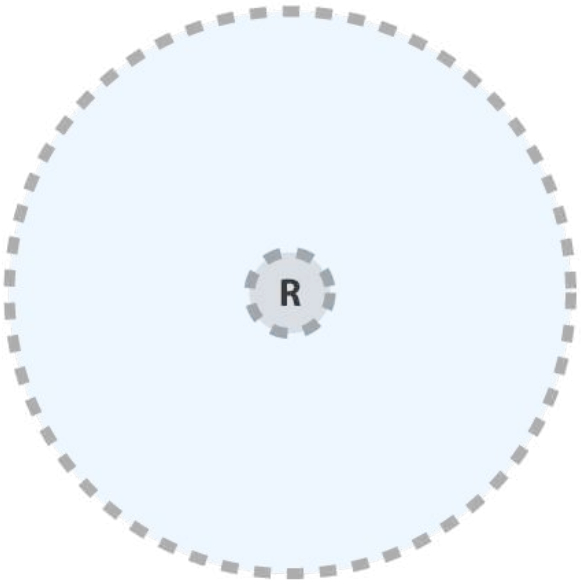

Figure 3: Here's a flat look at that donut. Let's say "R" is the router.

Understanding this shape allows us to realize how to best use this technology and make the most of our internet access and networking.

Imagine a donut-shaped zone around your router. There's a hole in the middle of the donut, so the signal won't be as great there. The area around the wireless router is where wireless devices of all kinds can connect well.

Concrete and metal are common signal "blockers" for conventional wireless routers. If part of this magical donut runs into a concrete or metal wall or framing, the signal becomes weak. We'll explain the best places to place wireless routers later in this document to avoid weakening the donut, er… I mean, wireless signal.

Figure 4: Placing a router near signal blockers can be like someone taking a big bite out of your wireless donut!

Setting Up: What You'll Need & What to Do

You'll need a few things to get started:

- A wireless router
- ISP provided modem or router
- Network cable (also sometimes known as Ethernet or Cat5 cable)

Location: Wireless Router Placement

At Stephouse Networks, a common technical support issue that arises is when a customer wonders why their wireless signal is so poor. After investigation, we realize that it's because the router is somewhere it shouldn't be.

Maybe we want to hide the router for aesthetic reasons. Maybe we want to keep it nearby other "computer stuff" around the house. There are all kinds of reason why we keep technical devices in particular areas.

But, we need to keep in mind that wireless routers have a radio frequency that most solid objects can block. When concrete and metal or other solid objects hinder a wireless signal, coverage is much less than we expect within the home or small office.

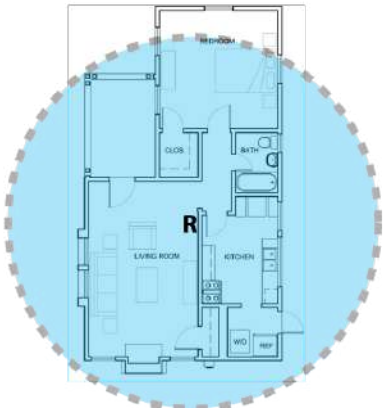

Figure 6: This placement gives great coverage.

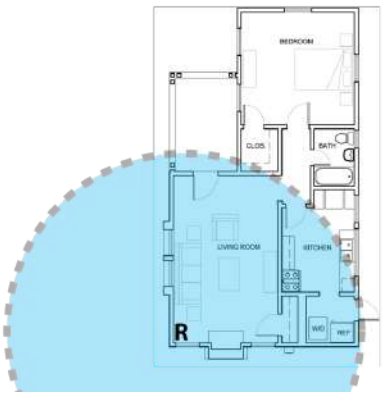

Figure 5: This placement covers a bit of the living room, but sends most of the signal out of the house.

Where your wireless router should go: Central rooms, living rooms, offices unobstructed by concrete or metal-framed walls, closets, and other similar areas.

Try to avoid: Basements, attics, garages, and other rooms that might have walls made of concrete or metal.

Setup: What To Do

Once you're ready, here are some step-by-step instructions on how to complete your initial setup, and how to lock down your Wi-Fi network once you're up and running.

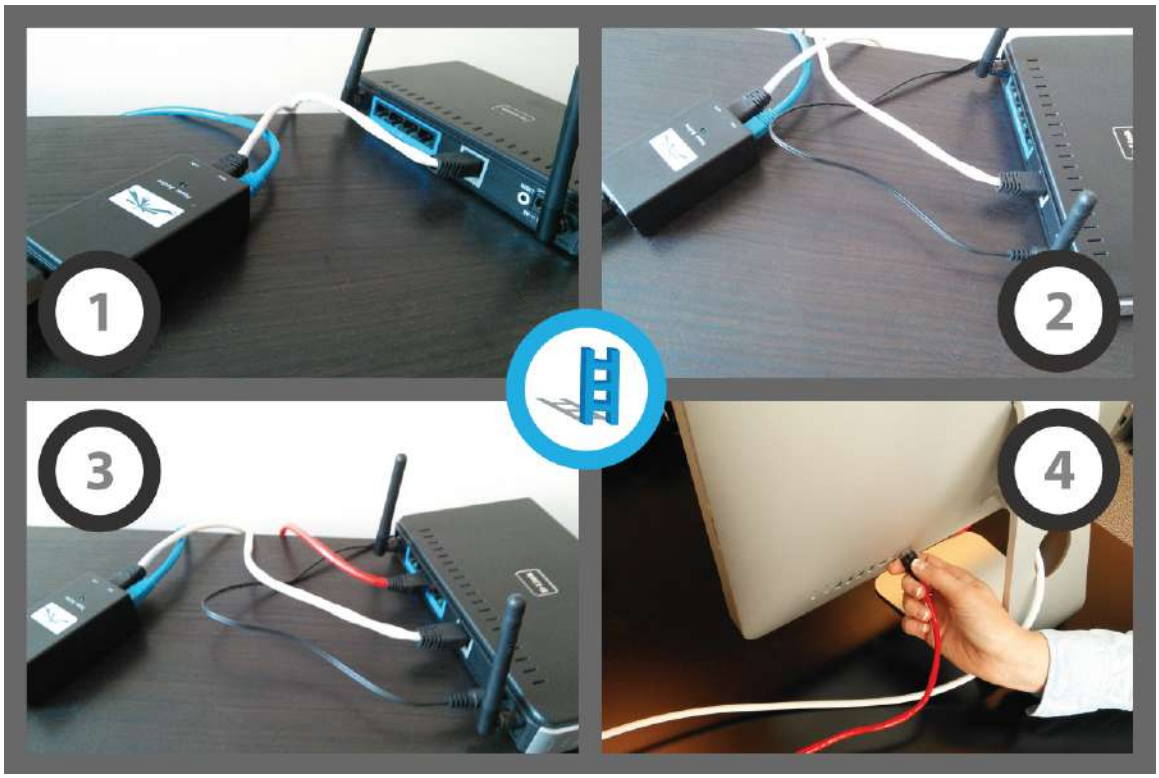

Figure 7: You'll set that router up in no time.

Initial Setup (after finding a great location for your router):

1. Plug in the network cable from the modem (provided by your Internet Service Provider) to your router's WAN or "Internet" port. This is basically feeding the router your internet access from the modem. We used a white cable in our example.
2. Ensure that all power and network connections are plugged in.
3. Wired Connections: Using one of the numbered ports, connect your wireless router to your computer using an additional cable (ours is red in the example).
4. Plug the internet cable into your computer. Or if using wireless, instruct your computer to connect to your newly set up network.

Security: Protect Your Wi-Fi Connection

Once you have your wireless network up and running, it's a good idea to secure it. Not only does it help keep unwanted guests off of your internet connection, but it makes your Wi-Fi network that much safer.

According to Wigle.net, a volunteer-run community of people mapping out Wi-Fi nodes, nearly 28% of the mapped networks in 2012 were unprotected. *Do you own one of these networks?*

Follow these steps to bring a basic level of security to your Wi-Fi network.

NOTE: *To change your router's setting you will first need to access the router setup menu. Most routers will use your internet browser for the setup menu so go ahead and open up Chrome, Firefox, Safari or Internet Explorer. In the address bar of your browser, type in the router's IP address which will probably be 192.168.x.x (x being a manufacturer specified number). Check the user manual to find the exact IP address needed.*

Change your router's default username and password. Right out of the box, your router's username and password might be something like: "Username: admin" and "Password: password". Router manufacturers make it something easy so that you won't have any issues changing it. If you are unsure of your router's default login info consult the owner's manual. If you no longer have your owner's manual, Google will be an invaluable asset as almost every router manual in existence is readily available and all you have to do is search for the make and model that should be displayed somewhere on your router.

Change your router's SSID. SSID stands for "Service Set Identifier," the name that you select when you choose a wireless network to connect to. A default SSID, like the router brand name, is a dead giveaway that your network has not been configured past the defaults and is most likely fair game to connect to. Most people looking for free wireless keep an eye out for all the standard default SSID's so don't let yourself become a victim!

Figure 8: You can typically access unsecured networks without a password.

Enable some form of wireless encryption. Encryption basically works to garble your wireless signal to those who do not have access to your Wi-Fi password. You will probably want to choose "WPA2" as that is the most secure form of wireless encryption available on most home routers.

A Great Start: Location and Security

And there you have it: a solid set of steps that will lead you to solid wireless access around the house or at the office.

Location: Remember that concrete and metal can dampen the signal strength of a wireless router. Living rooms, family rooms, and offices are the best place to put wireless routers. Basements and attics may seem like a great idea since it hides technology (if aesthetics are important), but they also hinder the strength of your wireless network if you're trying to cover your entire home.

Security: Set up a custom username and password, change your router's SSID, and enable encryption as a basic layer of security to fend off internet moochers. It's an extra bit of time to set this up, but it's well worth it if you don't want people stealing your internet access.

Learn More: Check out the Stephouse Networks Blog for more information on high-speed internet for home and business, as well as tips and tricks on how to improve your wireless coverage or internet experience. We also send tips and tricks out on our Facebook, Twitter, and Google+ Pages as well—let's connect soon.

Made with a whole lot of care by: DD, MH, AN.