



Know Your Network:

The Complete Guide

by Adam Dachis and Whitson Gordon



Know Your Network, Lesson 1: Router Hardware 101

Home networking is something we all have to deal with, but it can be confusing as heck. This week, we're going to turn you into a networking wizard, starting with getting to know the most important device on your network: the router.

Router Basics

Your router is the glue that holds your home network together. It connects all your computers to one another, either through Ethernet cables or a wireless connection. A router is different than a modem: your modem connects you to the internet, while your router connects your computers to one another. When you hook up your router to the modem, however, you're then able to share that internet connection

with all of the computers on your network. Sometimes modems will come with routers built-in, but this isn't always the case.

Devices that connect to your router—that is, the computers, tablets, smartphones, DVRs, game systems, and so on—are called *clients*. Each client on the network is given an IP address, which helps your router direct traffic. Clients within the network get a *local* IP address, while your modem gets a *global* IP address. Global IP addresses are like street addresses, while local IP addresses are like apartment numbers: one lets you find the building in relation to the rest of the world, while the other lets you find the specific location within the complex. These addresses make sure the right information from the outside world gets to the right computer on your network.

Routers have a number of different features, so we'll go through some of the most common router specs and how they affect your home network.

Wired vs Wireless



You'll want to hardwire any computer that doesn't need to move around, like a desktop, since wired connections are [fast, reliable, and cheap](#). They're far from ideal for devices you pick up and move around, though, like laptops, so for those we use a wireless connection (commonly known as Wi-Fi). Wi-Fi is more than adequate for simple web browsing, though wired connections are ideal if you're transferring big files, gaming, video chatting, or streaming video.

Most people have a mix of wired and wireless devices on their network, so most of our discussion today will be focused on wireless routers. Since wireless routers allow for both wired and wireless connections, you can wire up when necessary, and connect over Wi-Fi everywhere else.

Wireless Throughput

Throughput is the speed at which a router can transfer data. The transfer speed of your wireless connection is dependent on the wireless *standard* it uses. The most common standards today are 802.11g and 802.11n (also known as "wireless G" and "wireless N", respectively). Wireless N is faster than wireless G, though routers that support wireless N are also more expensive. Most new devices—like smartphones and laptops—support the faster wireless N.

Your router isn't the only thing that determines wireless speed: you also need the correct kind of wireless card in your computer. If you have an older laptop, it might have an older wireless G card inside, meaning it can't take advantage of wireless N speeds. If you have a mix of N- and G-capable computers, you can turn on a wireless N feature called "mixed mode", which will let you use both on the same network. You'll get faster speeds on the wireless N clients and slower speeds on the wireless G clients. Some claim, however, that running both N and G devices on the same network can [lower speeds across the network](#), even between a wireless N router and wireless N computer. So if you want the fastest possible speeds, you'll probably want all wireless N devices on that network.

Wired Throughput

The wired half of your router will come in one of two speeds: 10/100 Mbps and 10/100/1000 Mbps (also known as "gigabit"). 10/100 routers are cheaper, but won't transfer data between computers as quickly as gigabit routers will. If you're only using your router to connect to the internet, 10/100 is fine, since your internet connection is probably slower than 100Mbps, meaning you wouldn't be able to

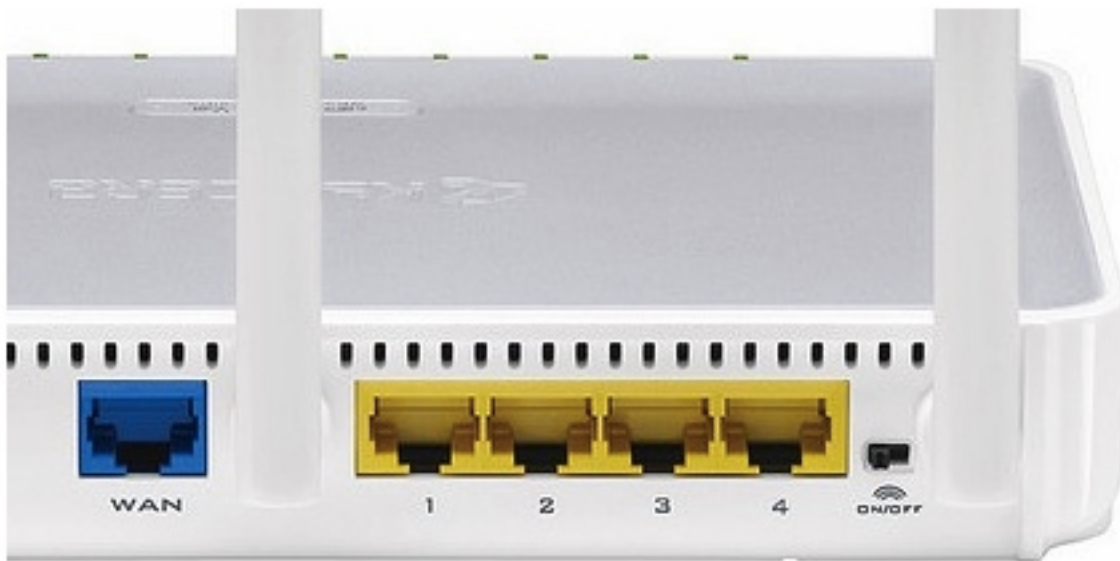
actually take advantage of the router's full speed. If you're transferring data between computers, however, you'll want to go with a gigabit router, since it'll transfer that data much faster than a 10/100 model.

Range

Wireless routers can only reach so far. If you have a big house and have the router on one side, you might not be able to access the network from the other side of the house. Your range, like your speed, is determined by the wireless standard you use. Wireless N has a longer range than wireless G, so if range is important you'll want to use wireless N.

That said, there are many other ways to connect to your network from afar. Wireless extenders (also called [wireless repeaters](#)) are products you can buy that do exactly what they say—extend your network further. Alternatively, you can [buy a powerline adapter](#), which lets you use your home's electrical wiring to hook a faraway device up to your router with an Ethernet cable (and thus get a faster connection than wireless would allow for).

Number of Ports



Routers have two types of ports in the back: LAN ports and WAN ports. Your WAN port hooks up to your modem (which, again, is what connects to the internet), while the LAN ports hook up to your computers and other clients. Most routers have one WAN port, but you'll need as many LAN ports as you have wired devices. If you have more wired devices than can fit on a router, you can plug them all in using a [wired switch](#). A switch is like a power strip for your router: it lets you plug in more devices than the router originally allowed. *Photo by [Ari Zoldan](#).*

Number of Bands

Wireless routers broadcast on a [radio band](#), and many new wireless N routers can broadcast on two bands. These are called, appropriately, *dual band* routers. Older routers and computers operate on a 2.4Ghz

band only, while dual-band routers allow for both the 2.4Ghz band and a 5Ghz band. The 5Ghz band is great because it has less interference, since tons of other devices—from other networks to Bluetooth to cordless phones to microwaves—operate on the 2.4Ghz band.

The main downside of the 5Ghz band is that, since it uses a higher frequency, it isn't as good at penetrating walls. As such, if you run your router in 5Ghz mode, you might have a shorter range than if you ran it in 2.4Ghz mode. In addition, some older devices don't support 5Ghz. The solution to this problem is to use a *simultaneous* dual-band router, which can broadcast on both bands at once.

Wireless Security



Unless you don't mind strangers eating your bandwidth and potentially accessing your networked files, you should always protect

your wireless network with a password. WPA2 is currently the most secure type of wireless encryption, so make sure you use WPA2 if you can. Some old wireless devices won't support WPA, in which case you'll have to use the less secure WEP instead. Basically every device made in the last four years supports WPA2 encryption.

If you're planning to use your router for a small business, you might want to look for a router with the "guest network" feature, which allows other people to access the internet without giving them full access to your computers and sensitive data.

Hackability

Hardware specs like these are important, but routers also come with a lot of software and firmware features, like [DHCP reservations](#), [Quality of Service](#), or firewalls that can make managing your network easier. However, the more of these features a router has, the more expensive it's likely to be.

If you're comfortable with flashing a new firmware on your router, you're better off getting one that's compatible with a [third-party firmware like DD-WRT](#) or [Tomato](#). Make sure your router is on [DD-WRT's list of supported devices](#) or [Tomato's list of supported devices](#) if you want to go this route.

When It Comes Time to Buy a New Router

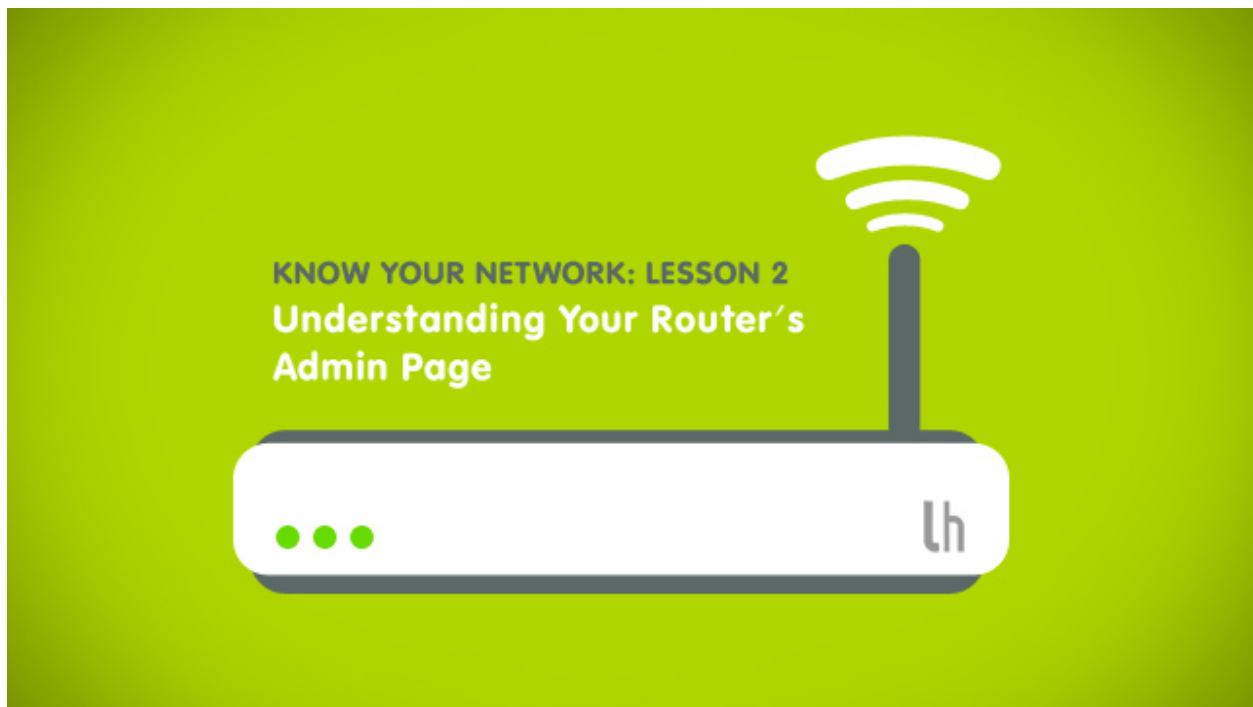
If you have a particularly old router, you may read a lot of the above information and decide it's time to upgrade. Be sure to check out [our guide to buying a Wi-Fi router](#), and take all the above information into

account as you shop: for example, if you need your network to reach long distances, make sure you get a simultaneous dual-band router for maximum range.

A note on user reviews: unlike most technology, reviews for wireless routers are not to be trusted. Most routers have a mix of 5-star "works perfectly" reviews and one star "totally sucks" reviews, and it's because *everyone's home is different*. There are so many other factors that go into network quality, like the walls, interference from other devices, and so on that you can't really extrapolate much from a given person's experience. The best thing to do is evaluate your needs, buy a router from a trusted brand that fits those needs, and return it if it doesn't work for you.

Understanding your router is merely the first step in the process, but it's an important one. In the next few lessons, we'll be talking about some of the software and firmware features of your router (like the aforementioned [DHCP reservations](#) and [Quality of Service](#)) and how they can make your network as fast and reliable as possible.

You can contact Whitson Gordon, the author of this post, at whitson@lifehacker.com. You can also find him on [Twitter](#), [Facebook](#), and lurking around our [#tips](#) page.



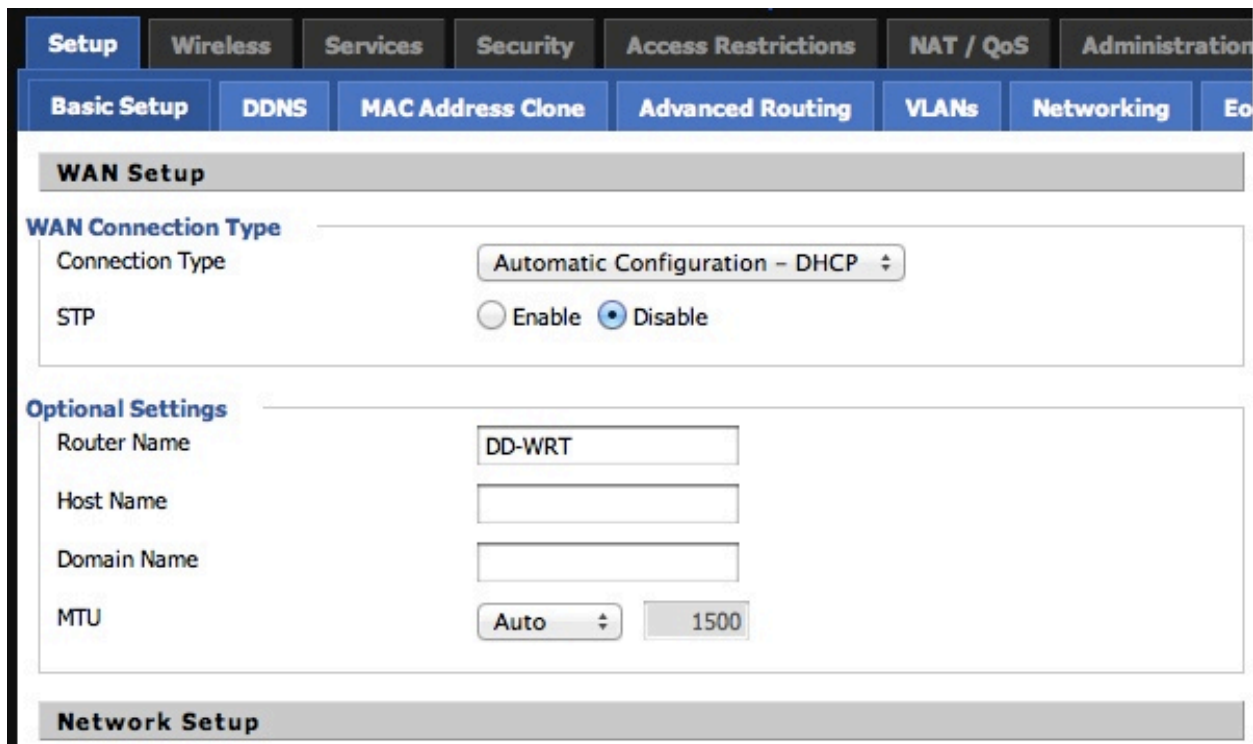
Know Your Network, Lesson 2: Understanding Your Router's Admin Page

In the first lesson of our networking night school, we looked at [the basics of router hardware](#). Today we're going to start setting things up.

The goal here is to get the most important things set up and then explain all the other details you ought to know. You may not use every section in your router's admin page, but understanding the features will help. We're going to use the [DD-WRT](#) router firmware in our examples—since it's a Lifehacker favorite available for many routers—but we'll explain how each topic applies to whatever router you have. Your router may not have every feature we talk about today, but if you're still [considering which router to buy](#) you may want to take the contents of these lessons into consideration.

Note: In future lessons we'll cover some of the more exciting and complex things you can do with your router, but first this episode just focuses on the basics.

Naming Your Router



The screenshot shows a router's configuration interface. At the top, there are tabs for 'Setup', 'Wireless', 'Services', 'Security', 'Access Restrictions', 'NAT / QoS', and 'Administration'. Below these, there are sub-tabs for 'Basic Setup', 'DDNS', 'MAC Address Clone', 'Advanced Routing', 'VLANs', 'Networking', and 'Eo'. The 'Basic Setup' tab is selected, and the 'WAN Setup' section is active. Under 'WAN Connection Type', the 'Connection Type' is set to 'Automatic Configuration - DHCP' and 'STP' is set to 'Disable'. The 'Optional Settings' section includes fields for 'Router Name' (DD-WRT), 'Host Name', 'Domain Name', and 'MTU' (Auto, 1500).

WAN Setup	
WAN Connection Type	
Connection Type	Automatic Configuration - DHCP
STP	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Optional Settings	
Router Name	DD-WRT
Host Name	
Domain Name	
MTU	Auto 1500

While it may seem trivial, there are actually a few things you need to know about naming your router. To start, the name of your router and wireless network *are different*. Naming your wireless network is really naming the [service set identifier](#) (SSID) that the router broadcasts and you select on your computer when you want to connect. The name of your router, however, is how it is identified to other devices on the network. In most cases, this name is much less important than what you choose for your SSID.

Choosing your SSID can be important, however. Leaving it as the default can lead to confusion with other networks, so it's important to pick something specific to you. You can even choose a name that's the first half of a phrase so it's easier for you to remember. This is, of course, somewhat less secure. Clever names can even [discourage people from trying to use your network](#) (e.g. "c:\virus.exe") or even communicate a message (e.g. "SexIsTooLoud"). Change it to whatever suits your purposes, but do make sure you change it.

Basic Wi-Fi Configuration and Security

The screenshot shows the WinBox interface for configuring the wireless interface wlo. The top navigation bar includes tabs for Setup, Wireless, Services, Security, Access Restrictions, NAT / QoS, and Administration. The 'Wireless' tab is active, and the 'Basic Settings' sub-tab is selected. The main configuration area is titled 'Wireless Physical Interface wlo'. Below this, the 'Physical Interface wlo - SSID [Chocolate] HWAddr [00:1E:E5:4E:CC:75]' section contains several settings: 'Wireless Mode' is set to 'AP'; 'Wireless Network Mode' is set to 'Mixed' with a red arrow pointing to it; 'Wireless Network Name (SSID)' is set to 'Chocolate'; 'Wireless Channel' is set to '6 - 2.437 GHz'; 'Channel Width' is set to '20 MHz'; 'Wireless SSID Broadcast' has 'Enable' selected with a red arrow pointing to it, and 'Disable' is also visible; 'Sensitivity Range (ACK Timing)' is set to '2000' with a note '(Default: 2000 meters)'; and 'Network Configuration' has 'Unbridged' and 'Bridged' options, with 'Bridged' selected. Below the main settings is a 'Virtual Interfaces' section with an 'Add' button. At the bottom, there are three buttons: 'Save', 'Apply Settings', and 'Cancel Changes'.

Setup	Wireless	Services	Security	Access Restrictions	NAT / QoS	Administration
Basic Settings	Radius	Wireless Security	MAC Filter	Advanced Settings	WDS	

Wireless Physical Interface wlo

Physical Interface wlo - SSID [Chocolate] HWAddr [00:1E:E5:4E:CC:75]

Wireless Mode	AP
Wireless Network Mode	Mixed
Wireless Network Name (SSID)	Chocolate
Wireless Channel	6 - 2.437 GHz
Channel Width	20 MHz
Wireless SSID Broadcast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Sensitivity Range (ACK Timing)	2000 (Default: 2000 meters)
Network Configuration	<input type="radio"/> Unbridged <input checked="" type="radio"/> Bridged

Virtual Interfaces

Add

Save Apply Settings Cancel Changes

There are a few things you need to do when configuring your Wi-Fi and they're all very simple. First, you need to make a few basic setup

decisions. Generally you'll find these settings in the Wireless tab on your router's admin page. This is the case in DD-WRT and on Linksys routers. For Dlink routers, it's generally in the Setup section under the Wireless Settings subheading. Netgear also calls it Wireless Settings, and Belkin tends to stick it under a Wireless header but label it Channel and SSID. There are a lot of router brands out there so we can't go over every naming convention, but as you can see they're pretty similar. You're basically looking for the word "wireless" and "setup" and/or "settings" in some combination.

Once you're there, the first thing you want to do is choose your SSID as we discussed in the section above. Choosing a wireless channel is also important, but we're going to talk about that in depth in the next lesson. The goal is to pick the channel with the least interference, and since the default channel is 6 for most routers you're likely to run into more interference on that channel. Feel free to pick another one for now, or just stick with the default and see how things run. If you're not getting the quality signal you'd hoped for, we'll talk about what you can do to about it in the next lesson.

Next you may need to choose a broadcast mode. In most cases you'll be working with a router that broadcasts both 802.11g and 802.11n, if not also others as well. As we discussed yesterday, mixed mode is going to reduce your speeds somewhat. If you really want to maximize throughput, broadcasting only 802.11n is your best bet. If you need backwards compatibility with 802.11g, however, you'll need to choose mixed mode.

Wireless Security w10

Physical Interface w10 SSID [Chocolate] HWAddr [00:1E:E5:4E:CC:75]

Security Mode: WPA2 Personal

WPA Algorithms: TKIP+AES

WPA Shared Key: ☐ Unmask

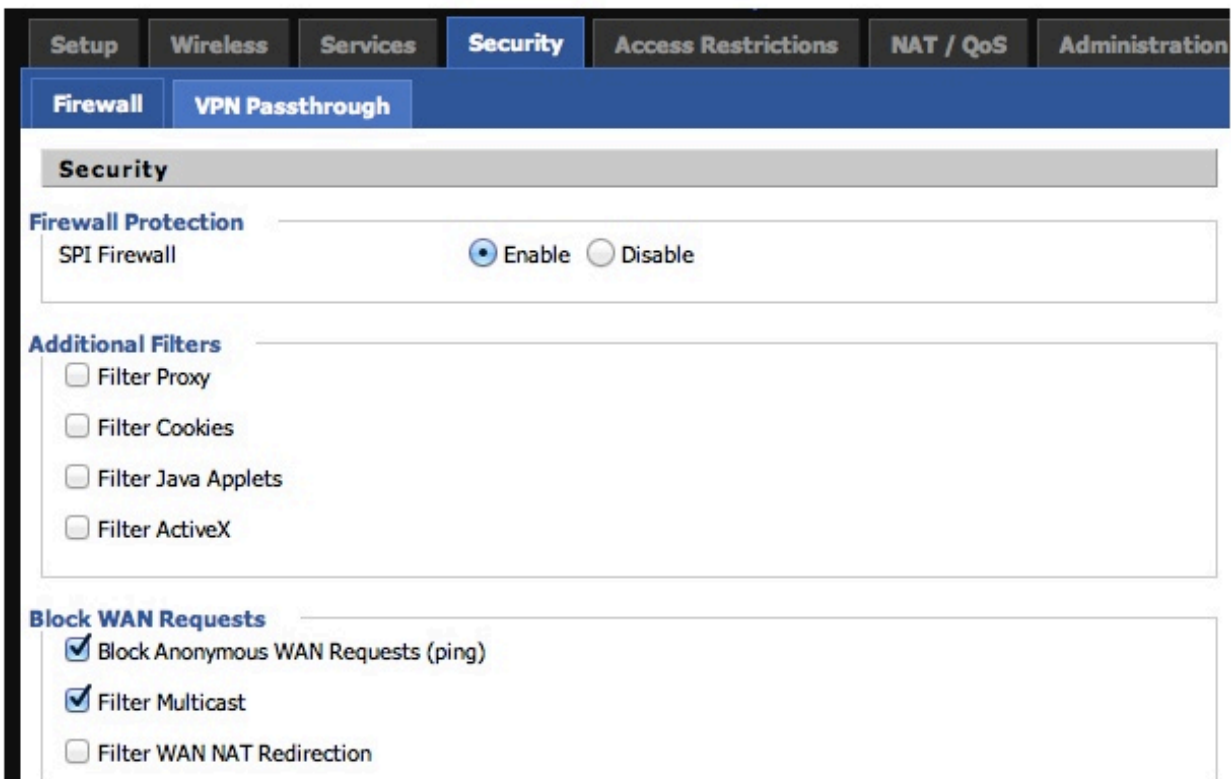
Key Renewal Interval (in seconds): 3600 (Default: 3600, Range: 1 - 99999)

[Save](#) [Apply Settings](#)

Next, hop on over to the Security section of your wireless settings. Most routers will separate these settings from your basic channel and SSID setup, but some keep them together. If you look for a section with a label approximating "wireless security" you should find what you're looking for. When you do, this is where you can enter a password. Generally [WEP is easier to crack](#), so using WPA2 (or WPA if WPA2 is not an option) is a better choice. You also can choose a more complex password when using WPA2. One thing to note is that some Wi-Fi cards (in your computers) will have trouble connecting to a WPA2-secured network via 802.11n when you don't support multiple WPA2 algorithms. If you find that you or visitors have difficulty connecting via 802.11n, be sure to set your WPA2 algorithms to *both* AES and TKIP. This is usually represented as "AES+TKIP" or something similar.

You don't need to mess around with much else beyond that to get your Wi-Fi up and running securely. While there are a few more advanced options worth looking at, too, we'll cover those in tomorrow's lesson.

Security Settings



Setting a Wi-Fi password isn't the only security you're going to have on your router, and generally various security settings will be split up into different sections. For example, password-protecting your router's admin page will generally be in the Administration section and some things like MAC Address Filtering like to find themselves in no consistent location between the various brands of routers. Often times you'll have to go looking around for what you want to find, but generally you'll also find a few things clumped together. They often deal with your router's firewall.

The [firewall](#) is the greatest challenge to any Hollywood actor playing a hacker in a film, but in reality it's not that big of a deal. Basically, you receive many network transmissions you're not aware of because your router's firewall is blocking them from getting through to you. It has a

set of rules that allows certain kinds of data to reach you while blocking others that you presumably don't want. A [semipermeable membrane](#) is likely a better metaphor, but it's not quite as exciting or dramatic as firewall.

For the most part, the default firewall settings should be just fine for most people, but you should know that can less or more types of data if you choose. For example, you can filter out things like cookies and Java applets. You'll find that most routers are already filtering anonymous ping requests, which you may want to disable. It's also a good page to look at for troubleshooting purposes, as sometimes settings in your firewall will prevent certain applications from working properly as they require communicating outside of your [local area network](#) (LAN). If you're trying to debug a problem, *temporarily* disabling filters and/or features on your firewall can help you do so. Most of the time, however, you can just leave things as they are.

NAT and QoS

Port Forwarding

Port Range Forwarding

Port Triggering

UPnP

DMZ

QoS

Port Forward

Forwards

Application	Port from	Protocol	IP Address	Port to	Enable
VNC (Grey)	5900	Both ↕	192.168.1.100	5900	<input checked="" type="checkbox"/>
VNC (Hunter)	5901	Both ↕	192.168.1.101	5900	<input checked="" type="checkbox"/>
SAB (Grey)	8080	Both ↕	192.168.1.100	8080	<input checked="" type="checkbox"/>
SB (Grey)	8081	Both ↕	192.168.1.100	8081	<input checked="" type="checkbox"/>
Web (Grey)	80	Both ↕	192.168.1.100	80	<input checked="" type="checkbox"/>
SSH (Grey)	22	Both ↕	192.168.1.100	22	<input checked="" type="checkbox"/>
AFP (Grey)	548	TCP ↕	192.168.1.100	548	<input checked="" type="checkbox"/>

AddRemove

Save

Apply Settings

Cancel Changes

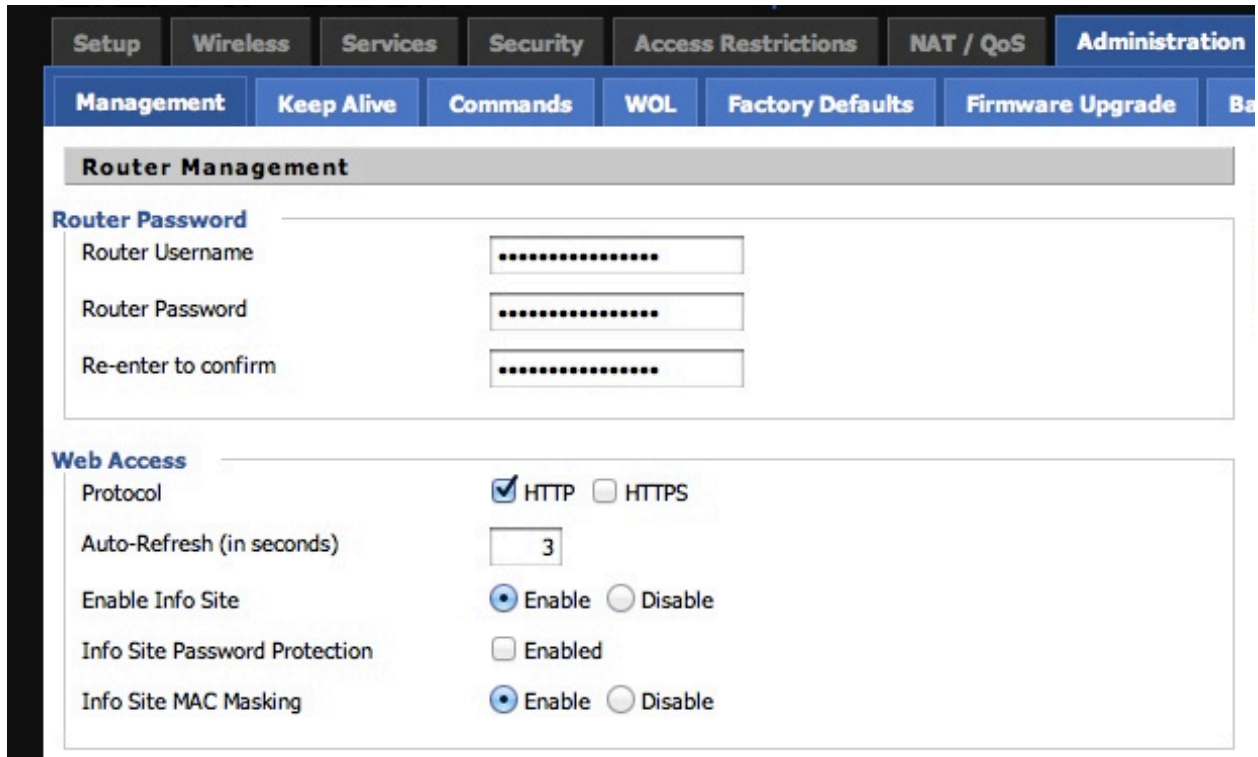
NAT stands for [network address translation](#) and QoS stands for [quality of service](#). As NAT and [port forwarding](#) are related, you'll generally find them together. Sometimes port forwarding is also known as Virtual Servers in some routers. QoS is often paired with these features as well but not always.

So what do they do? Let's start with NAT and port forwarding. You're probably aware that you have local IP addresses that differ from the IP addresses out on the internet. On your local network, they usually look like 192.168.x.x or 10.0.x.x but they can essentially be anything because they're local. NAT is what translates the outside IP addresses to your local network so you can interact with people as far as the wide internet can take you. Port forwarding relates to this because, by default, nobody on the outside can access your local machines. You

can use port forwarding, however, to open up certain ports for certain machines on the network. For example, if one computer has a web server and another has an FTP server, you could open up ports for both of those services so people could access them from outside of your local network. If this is new to you and a little confusing, don't worry—we're going to cover this in a lot of depth in the next lesson.

QoS is designed to keep your network's bandwidth evenly distribute, and it's something we've[previously covered](#). Basically, the idea is that certain users and/or applications may hog the bandwidth on your network and from your connection to the internet, but QoS will let you define rules to let you throttle users and services when they are using too much. This allows for the network to run more smoothly in general and can help the router from getting so bogged down that you need to manually restart it. QoS isn't available on all routers, but it's becoming more and more common. If you use custom firmware like DD-WRT it'll be there when you need it.

Administration and Status

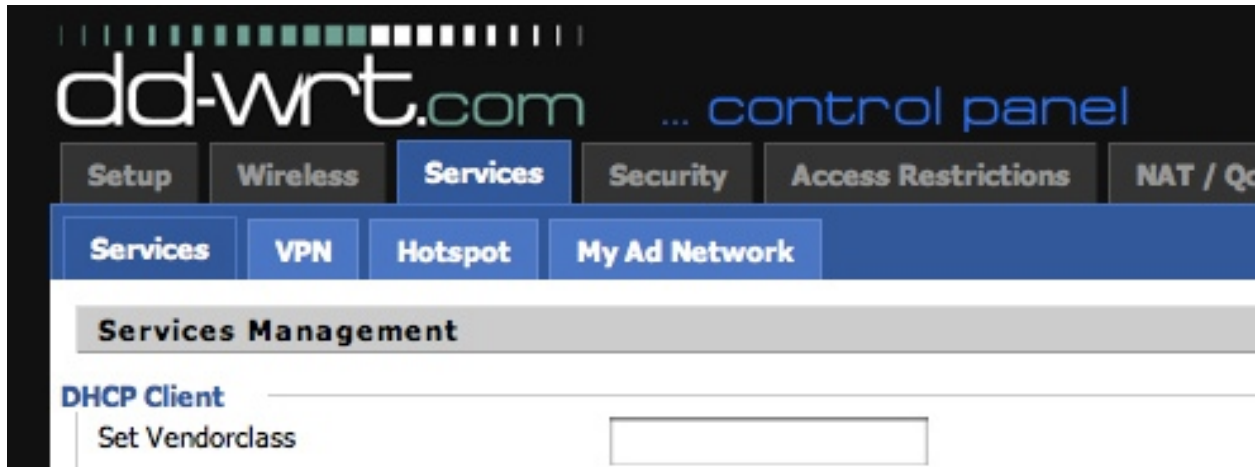


The screenshot shows a router's web interface with a top navigation bar containing tabs: Setup, Wireless, Services, Security, Access Restrictions, NAT / QoS, and Administration. Below this is a sub-navigation bar with tabs: Management, Keep Alive, Commands, WOL, Factory Defaults, Firmware Upgrade, and Backup. The main content area is titled "Router Management" and contains two sections:

- Router Password**: A section with three input fields for "Router Username", "Router Password", and "Re-enter to confirm", each masked with dots.
- Web Access**: A section with several settings:
 - Protocol**: Radio buttons for ☒ HTTP and ☐ HTTPS.
 - Auto-Refresh (in seconds)**: A text input field containing the number "3".
 - Enable Info Site**: Radio buttons for ☒ Enable and ☐ Disable.
 - Info Site Password Protection**: A checkbox for ☐ Enabled.
 - Info Site MAC Masking**: Radio buttons for ☒ Enable and ☐ Disable.

Your router generally has two sections that go by the same name with pretty much every router on the market: Administration and Status. Administration is where you add a password to your router's admin section, choose whether or not the router admin pages can be accessed outside of your local network, and also accomplish tasks like settings backup and firmware upgrades. The Status section will give you information about your router, such as its current [wide area network](#) (WAN) IP address, the computers that are connected to it, and more. This is also where you can check your router's logs. Generally you won't need to spend much time in either of these sections, but knowing what they do and what's inside can be particularly helpful.

Various Router Services



Your router may have a section called Services, Tools, Advanced, or something that isn't particularly descriptive. This section will often let you set up things like a VPN, turn on advanced options like SSH, and enable or disable the system log (although you'll usually find that in the Status section, too). We'll cover these items more later, but if you're looking for anything that doesn't seem to fit in the available categories you'll generally find it in your Services/Tools/Advanced tab.

That's all for today. Our next lesson will concentrate on improving your network speed—both wired and wireless—and router performance, so be sure to check back tomorrow night for the next article!

You can follow Adam Dachis, the author of this post, on [Twitter](#), [Google+](#), and [Facebook](#). Twitter's the best way to contact him, too.



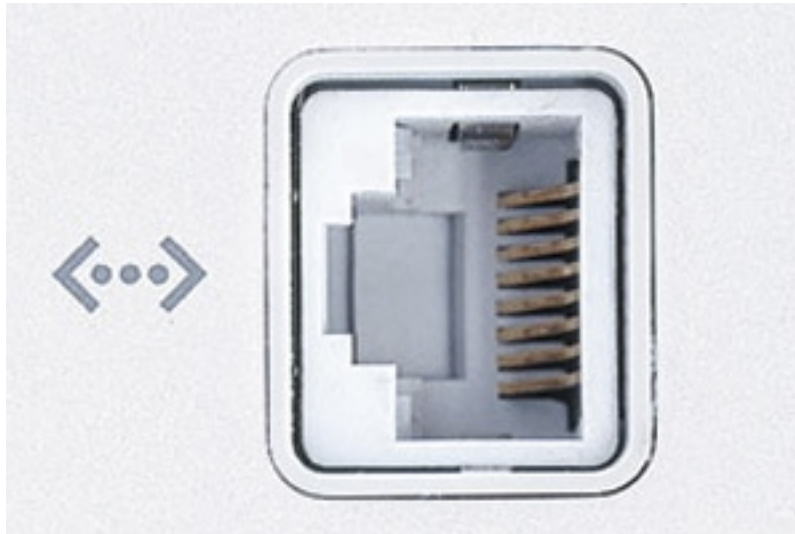
Know Your Network, Lesson 3: Maximize Your Speed, Performance, and Wireless Signal

You've [picked your router](#) and [set up all the basics](#), so now it's time to optimize your network. In this lesson, we're going to look at how to improve your network's speed and wireless signal so it's operating at full capacity.

In theory, your network should work just fine as-is, but we all know that reality can differ from what should ideally be the case. How well your router performs is going to depend on a lot of factors, so these tips and tricks might work better for some than others. For example, strategies for improving your wireless signal aren't going to do much unless your router is dealing with some interference. On the other

hand, tweaks can only do so much if you're dealing with really bad interference. That said, whether the improvement is marginal or great, we're going to look at all sorts of ways to get your network running as fast and efficiently as possible.

Use Your Wires Whenever Possible



Wi-Fi is nice, but it's rife with signal issues and slower than a wired ethernet connection—even when Wi-Fi is performing its best. If you can wire up your devices, [you should](#). When transferring files

between devices you'll always get better performance over a wire, and internet connections over 25mpbs will also benefit from wires. That may seem strange when many routers advertise wireless speeds that are much higher, but real-world performance is generally far lower. If you can't wire up your home, power line ethernet adapters (like [Belkin's gigabit option](#)) can be a good alternative. It's pretty rare that you'll have a power line capable of maintaining gigabit speeds, but you may still achieve better performance than you would over the air with 802.11n. If you want to give power line adapters a shot, just buy a set from a store with a good return policy and see how they work. If they don't, you can always take them back. If they do, you can buy as many as you need. Just be sure to test them on every outlet you're going to

use, since some outlets work better than others with power line adapters.

Check out our [guide on ditching wireless and going completely wired in your home](#) for more tips.

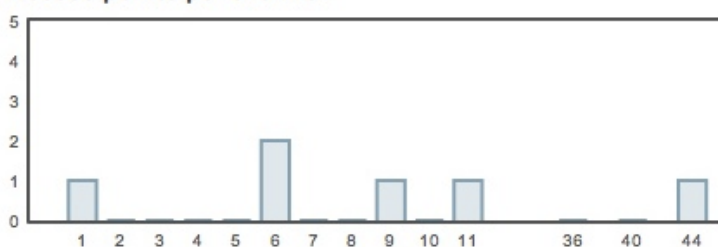
Improve Your Wi-Fi Signal

There are plenty of tricks you can employ to improve your Wi-Fi signal. Your mileage may vary depending on your situation, but most methods are pretty easy and worth a look. In this section, we're going to take a look at our favorites. They're all things you can accomplish with very little effort.

Choose the Best Wireless Channel

meraki  TOOLS | WIFI STUMBLER ^{BETA}

Access points per channel



While radio frequency interference is going to be an issue in your home, one of the biggest causes of interference that'll slow down your Wi-Fi speed is other Wi-Fi routers in your area. That's often

because most Wi-Fi routers default to the same channels: 6 or 11. (You don't need to understand all of this to fix the problem, but we'll explain.) Additionally, the standard channel width is 20 MHz, which means that even though you're on channel 6, which has a frequency of 2.437 GHz, your channel width spans 20 MHz around that frequency. Since each channel is only 5 MHz apart from the next, your signal is bleeding into the others. While you can adjust the channel width, this

may only help some of the time as your router's needs will change. Ideally [channel width would be adaptive](#), but since that isn't a reality the best thing you can do is pick a channel as far from the others as possible.

[Previously mentioned](#) wireless network locator [WiFi Stumbler](#) is a webapp that provides a simple way to check what channels are in use in your computer's range. Simply look for the channel with as much space around it as possible and use that channel instead of what you're currently using. Also note that while you may pick up competing signals on the same channel, if they're all very weak that can be a better choice than choosing a lesser-used channel with a strong, competing signal.

Basically, if your neighbor's on channel 1 and a few people down the block are using channel 4 (and you're somehow picking up their Wi-Fi), you're still probably better off using channel 4 for your Wi-Fi. That is, unless there's a huge amount of interference on channel 5. As you can see it can get a little tricky, but the goal is to pick a channel that keeps its distance from other signals with the same or overlapping frequencies.

We discussed where to change this settings in the [previous lesson](#), but you'll generally find it in your basic wireless settings on your router. It tends to sit in the same section as your SSID.

Boost Your Signal's Transmit Power

Preamble	<input type="text" value="Long"/>	(Default: Long)
Shortslot Override	<input type="text" value="Auto"/>	(Default: Auto)
TX Power	<input type="text" value="71"/>	(Default: 71, Range: 1 - 251mW)
Afterburner	<input type="text" value="Disable"/>	(Default: Disable)
Bluetooth Coexistence Mode	<input type="text" value="Disable"/>	(Default: Disable)
Wireless GUI Access	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	(Default: Enable)

Your Wi-Fi router transmits its signal with a set amount of power, but that's something you can adjust. In theory, if

your signal sucks you'd want to just transmit it as powerfully as possible. In reality, boosting your router's transmit power too much can actually make things worse. But there's a magic number: 70 mW.

In general, your router's transmitting at 28 mW, but most routers can handle 70 mW without issue. [According to the DD-WRT documentation](#), setting this any higher could fry your router's radio chip because your router's not designed to handle the excess heat. You technically *can* turn it all the way up to 251 mW, but if you do you're just asking for trouble. If your router overheats, it's going to perform far worse—or die. Staying in a safe range may only show marginal improvements, but that's much better than a dead router.

Unfortunately most routers don't allow you to boost your transmit power, so if you're not using custom firmware like DD-WRT or Tomato, you're probably out of luck on this one. If that includes you, just read on as the next section can help solve signal issues with virtually any router.

Extend Your Signal with DIY Projects



Sometimes router settings just aren't going to cut it, so you need to put on your tinkering hat and make a DIY booster. In [episode four of the Lifehacker Show](#), we built [this simple Windsurfer booster](#) out of card

stock and tinfoil. On top of that, we have [many more Wi-Fi boosting projects](#), such as [this tin can extender](#) or [a repurposed satellite dish](#). There are also several range-boosting products on the web (like [this one](#)), but if you can avoid shelling out another \$70, it's worth giving a DIY option a try.

Use QoS to Help Prevent Bandwidth Hogging and Network Overloads

Quality Of Service (QoS)

QoS Settings

Start QoS ☐ Enable ☒ Disable

Port

Packet Scheduler

Uplink (kbps)

Downlink (kbps)

Optimize for Gaming ☐

Services Priority

Delete	Service Name	Priority
<input type="button" value="Add"/>	<input type="text" value="100bao [0 ~ 0]"/>	

Netmask Priority

Delete	IP/Mask	Priority
<input type="button" value="Add"/>	<input type="text" value="0 . 0 . 0 . 0 / 0"/>	

MAC Priority

Delete	MAC Address	Priority
<input type="button" value="Add"/>	<input type="text" value="00 : 00 : 00 : 00 : 00 : 00"/>	

In our [previous lesson](#) we talked a little bit about Quality of Service, which is essentially a set of rules that throttles bandwidth when a person (your roommate) or application (BitTorrent) is trying to hog it all. Say, for example, you want to video chat while your roommate is downloading a movie. QoS helps make sure both endeavors have

enough bandwidth. We have a [full guide on configuring QoS](#), but here's a quick overview of what you need to do.

First things first, navigate to your router's QoS page (if it exists—not all router firmwares have this feature) and enable QoS. That's not going to do anything yet, because we have some settings to fill out first, but I always forget to enable features so I like to do that first. In your QoS settings you should have a few settings and toggles to deal with. Here's a quick look at your options in DD-WRT (note: this will vary from router to router, but obviously we can't go over every single brand's firmware):

- 1 WAN, LAN, or Both** - Generally QoS is used to handle traffic from outside your local network, so it defaults to WAN (Wide Area Network). Unless you have a reason to change it, just leave this setting as-is.
- 2 Packet Scheduler** - This can be set to HTB or HFSC. HTB is the default method that uses a "token" system to manage bandwidth. Don't change this to HFSC unless you know what you're doing.
- 3 Uplink and Downlink** - Here you can set a limit for the total network bandwidth can be used on your network. If you don't want to max out your connection, you can set these speeds to less than their theoretical maximums. DD-WRT recommends 80-95% for uplink and 80-100% for downlink.

Once you've got those global settings taken care of, you can start specifying rules. DD-WRT splits these rules up into three categories: Services, Netmask, and MAC priorities.

Services Priority will let you set bandwidth priorities for different applications. These applications are pre-set and include everything from SMTP to BitTorrent to Xbox Live. If a particular service isn't listed, you can add it yourself.

Netmask Priority can give bandwidth priority to a range of IP addresses. For example, if you have three computers that use the IP addresses 192.168.1.10, 192.168.1.11, 192.168.1.12, you can specify that range to receive priority. This can be useful if you want to ensure that your machines will always take priority over any guest computers that show up on your network.

MAC Priority is a way to set which specific devices receive priority over others. Here you enter your device's MAC address (a MAC address is a unique identifying address for your computer's network adapter) and set a relevant priority.

Once you've chosen a service, IP range, or MAC address, and added it to your priorities list, you have to actually define the priority. By default the priority will be set to Standard, but you can promote it to Express or Premium to give it a higher bandwidth priority over other items on the list. These categories are good for applications that will sometimes require additional bandwidth, such as video chat and VOIP. You can also set any item to Exempt to let the app or computer use as much bandwidth as it wants and Bulk if you want it to only use bandwidth that is left over from other applications.

After you've finished adding all your devices and setting their priorities, you can save your settings and let your router reboot (if necessary). That's really all you have to do to get QoS working.

That's all we've got for today's lesson. Join us again tomorrow when we'll be going over how to set up your computers for remote access. If you've missed any previous lessons, you can always find them on the [Lifehacker Night School tag page](#).

You can follow Adam Dachis, the author of this post, on [Twitter](#), [Google+](#), and [Facebook](#). Twitter's the best way to contact him, too.



Know Your Network, Lesson 4: Access Your Home Computers from Anywhere

You've [picked out your hardware](#) and [set up the basics](#), and [configured your network to perform at its best and fastest](#). Now it's time to open the gates to the outside world. In this lesson, we're going to walk you through how to set up your router so you access your home computers from anywhere—and with your own friendly, easy-to-remember URL.

Setting up remote access to your local network is one of the coolest things you can do with your router, as it allows you to remotely view your screen, access files, control services like BitTorrent remotely, and so on. Basically, anything you can do at home can be made possible by just opening a few ports on your router. It can seem a little daunting if you've never done it before, but once you understand what everything means and where to find the information you need, you should have

no trouble getting things to work. We're going to go over basic setup and then talk briefly about a few bonus options as well.

Port Forwarding and More

By default, your local network is local and cut off from the rest of the internet. In most cases you have just one IP address that's shown to the world, despite the many that your router distributes to your individual computers and devices locally. What port forwarding does is take a port on that shared IP address that's available to the rest of the web and forwards it to one of your local machines. This lets people from outside access services on your local network.

Setting up port forwarding is pretty straightforward, but before you get started, you need to know what ports you want to open up. Most of the time, you'll set up port forwarding on an as-needed basis—say after you've set up a new service on your computer. For example, if you're trying to run a web server off your machine you'll need to open up port 80. If you want to open up SSH access, you'll need to open up port 22. Those are just two of many possibilities, and you probably don't have every port for every service memorized.

This is where a site like PortForward.com can help, as it provides a handy [list of common ports for specific services](#). You can use this list to check which ports you need to open for whatever services you want to make available from outside your home network.

Once you've figured out all the ports you want to open, just head on over to the port forwarding section of your router (if you don't know where it is, just click around a little). In DD-WRT, it's in the NAT & QoS section. Other routers may list it simply as Port Forwarding (all

on its own) or Virtual Servers. Let's take a look at what a filled-out port forwarding table looks like:

Port Forward					
Forwards					
Application	Port from	Protocol	IP Address	Port to	Enable
VNC (Grey)	5900	Both ↕	192.168.1.100	5900	<input checked="" type="checkbox"/>
VNC (Hunter)	5901	Both ↕	192.168.1.101	5900	<input checked="" type="checkbox"/>
SAB (Grey)	8080	Both ↕	192.168.1.100	8080	<input checked="" type="checkbox"/>
SB (Grey)	8081	Both ↕	192.168.1.100	8081	<input checked="" type="checkbox"/>
Web (Grey)	80	Both ↕	192.168.1.100	80	<input checked="" type="checkbox"/>
SSH (Grey)	22	Both ↕	192.168.1.100	22	<input checked="" type="checkbox"/>
AFP (Grey)	548	TCP ↕	192.168.1.100	548	<input checked="" type="checkbox"/>
<div>Add Remove</div>					

While things may differ slightly depending on your router's firmware, this table is pretty standard. Here's what all of those fields mean:

- 1. Application** - The name of the application you're forwarding this port for. You can use any descriptive text you want—this field is here to help you remember why you set this up; like the name suggests, you normally want to use the name of the application you're setting up port forwarding for. I also include my computer's name along with the service, since I forward ports for the same applications on different computers. For example, you'll see VNC service set up for both Grey and Hunter. I include their names in the Application section so I know which port forwarding rule is for which computer.

2. **Port to** - "Port to" is the port on your local IP address. If you were setting up VNC for a local computer, you'd fill this in with 5900 as that's the port number VNC uses.
3. **Port from** - "Port from" is the port on your external IP address. Generally you'll also enter the same port as you would in the "Port to" field. This works just fine when you're configuring only one machine for one type of service. But say you wanted to be able to remotely access two or more computers using VNC. If you used 5900 on a single, external IP address they would be in conflict. The router would see a request for port 5900 and not know which local IP address should handle that request since the port forwarding table has two. To solve this problem, you can use the standard port for one and not for the other—kind of like an apartment building has a single address but multiple apartments. As you can see in the sample routing table above, Grey's "Port from" is set to 5900 while Hunter's "Port from" is set to 5901. If you try to use VNC normally on my external IP address, you'll be asked to log in to Grey because it uses the standard port. If you want to access Hunter, however, you can easily do so by just using port 5901 instead of the default. This way you can set up identical services with a single external IP address without conflicts.
4. **Protocol** - This is where you specify whether or not your service uses the TCP protocol, UDP protocol, or both. When you look up your ports you'll also want to make note of the protocols used. In most cases it will just be TCP.
5. **IP Address** - This is where you specify the LAN (local area network) IP address of the computer you want to use for this

port forwarding rule. You can easily find this information in your computer's network settings. The IP address will generally be in the 192.168.x.x or 10.0.x.x format. Because these IP addresses are generally dynamic (meaning they can change), you'll want to either set up static IP addresses or DHCP reservations. More information on that is available below.

- 6. Enable** - You need to check this box to enable the port forwarding rule. If you don't check it, you'll still be able to save the rule but it won't be active or function in any way.

Now that you understand what these fields mean, click the "Add" button at the bottom to add a new port forwarding rule. Fill everything out with the desired information (such as port 21 for FTP, 22 for SSH, 5900 for VNC, etc.) and don't forget to check the enable box to make sure everything works. When you're done entering all your rules, save it and you're all set.

Port Range Forwarding

Sometimes you want to open a range of ports on a particular machine and not just one at a time. Some routers offer the option of port range forwarding in addition to regular old port forwarding (like we just discussed). This works in the same way, except you specify a range (e.g. ports 21 - 80).

The DMZ

Demilitarized Zone (DMZ)

DMZ
Use DMZ ☐ Enable ☒ Disable
DMZ Host IP Address 192.168.1.

DMZ stands for De-Militarized Zone and is a simple way to open up *every port* on a single computer. If your router has this feature, just visit the DMZ page and enter that computer's IP address. While convenient if you only have one computer you want available for remote access, this isn't very secure. You're essentially allowing any kind of traffic to be forwarded to this machine. Even if you only have one computer, you're still better off manually entering each service you want to open. Only use this if you really have a good reason to do so.

DHCP Reservations

DHCP Server

Use JFFS2 for client lease DB (Not mounted)

Use NVRAM for client lease DB ☐

Used Domain WAN

LAN Domain

Additional DHCPd Options

Static Leases			
MAC Address	Host Name	IP Address	Client Lease Time
<input type="text"/>	Grey	192.168.1.100	<input type="text"/> minutes

[Add](#) [Remove](#)

One of the annoying aspects of port forwarding is that your router dynamically assigns IP addresses to your computers. That means the local IP addresses of your computers may change, which can render that port forwarding you did incorrect or non-functional. While setting up static IP addresses on your local machine is one option, DHCP reservations are better if you've got the option in your router. This is common in Linksys and D-Link routers but generally not included in Belkin. It's also available in DD-WRT in the Services section, but it's easy to miss.

DHCP reservations let you specify static local IP addresses on the router's side so that when your computer connects to your network, your router will always assign it the same local IP address. To set it up, decide what local IP address you want for a given computer (or other device) and find its MAC address. Your MAC address is a 12-digit alphanumeric string separated by two digits at a time. It generally

looks like 1A-2B-3C-4D-5E-6F or 1A:2B:3C:4D:5E:6F. To locate it on Windows, click the Start menu and choose run. Then type ipconfig/all. The "Physical Address" is your MAC address. On Mac OS X, just open System Preferences, choose Network, click More Info, and then the Hardware tab. Your MAC address should be the first thing displayed. Once you've got that you can just enter it in the reservation list with the local IP address you want and you're also set. Just be sure to save and enable it. You may need to restart your router to see the changes take effect, but once you do the computers and devices in the reservations table will retain the same local IP addresses. This solves pretty much every kind of problem. For information on setting this up, check out our [guide to DHCP reservations](#).

Assign a Friendly Domain Name to Your Router with Dynamic DNS

Dynamic Domain Name System (DDNS)

DDNS

DDNS Service

User Name

Password

Host Name

Type

Wildcard

Do not use external ip check

Disable

✓ DynDNS.org

freedns.afraid.org

ZoneEdit.com

No-IP.com

3322.org

easyDNS.com

TZO.com

DynSIP.org

Custom

Unmask

Yes No

DNS is a service that lets you access your home computers using a nice domain name (e.g. myfancyrouter.net) instead of a numeric IP address (e.g. 72.54.34.90). Depending on your internet provider, however, your external IP address may periodically change. That's why you need

Dynamic DNS. It points a friendlier domain name to your numeric IP address just like regular DNS, but compensates for that IP address' proclivity to change. So, rather than typing in 76.xxx.xx.xx every time you want to remotely access your home computer, you can type something friendly like `myawesomecomputer.dyndns.tv`.

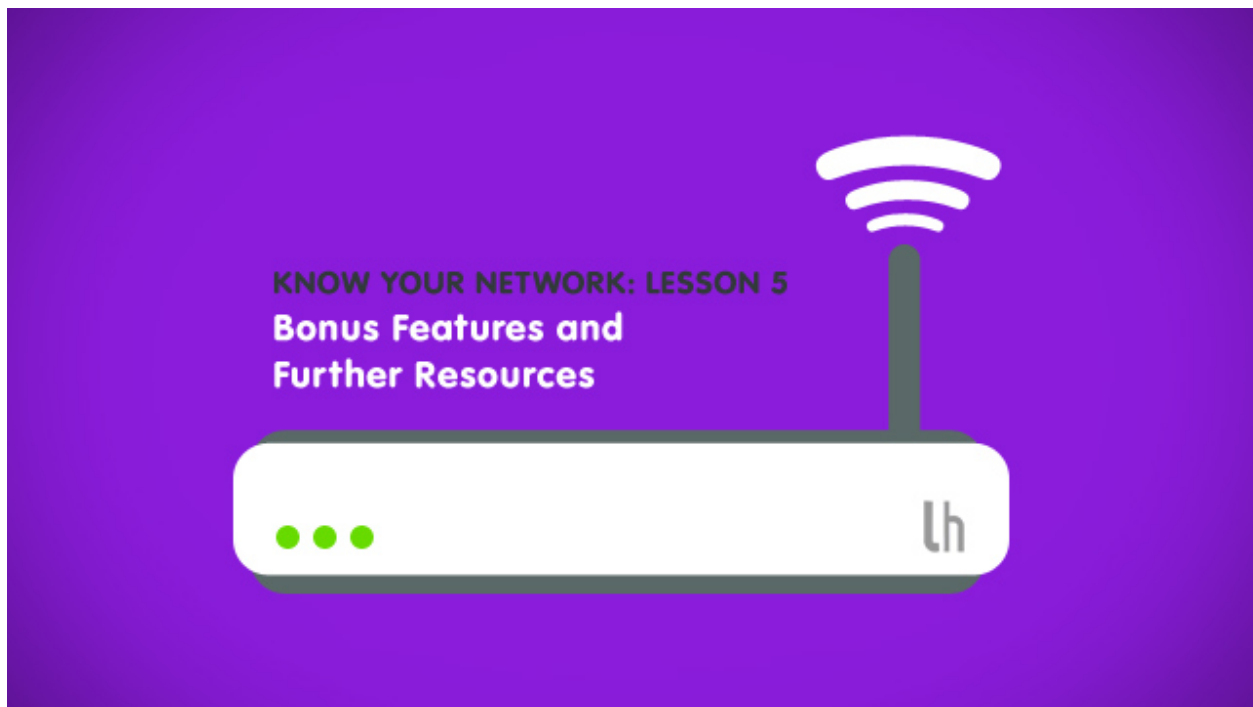
You can accomplish this task in a couple of ways. First, you can download some software from your dynamic DNS provider that will automatically check and update your external IP address at a set interval. Second, your router may already support some dynamic DNS providers and can perform this update for you automatically (which is the easier method). Two of the most popular providers of dynamic DNS services are [DynDNS](#) and [No IP](#), but there are others. These services are generally free but offer perks at a cost. Some routers only support one of these services, but custom firmware like DD-WRT support both and more.

To set up dynamic DNS, you just need to sign up for an account with one of these services and enter your account credentials into the dynamic DNS section on your router. If your router doesn't support your service of choice, you can just download software from your service provider like we mentioned earlier. You'll need to keep this software running pretty much 24/7, so it's definitely better if you can leave the task of dynamic DNS to your router.

If you want further setup instructions, [here's how to set things up with DynDNS](#) and [No IP](#). Your router may support other services, but it's likely to support at least one of those.

That's all for today's lesson. In our final lesson, we'll be taking a look at some fun and useful bonus features you may have on your router plus resources for learning more. As always, if you're behind on our lessons, you can always find everything you've missed on the [Lifehacker Night School tag page](#).

You can follow Adam Dachis, the author of this post, on [Twitter](#), [Google+](#), and [Facebook](#). Twitter's the best way to contact him, too.



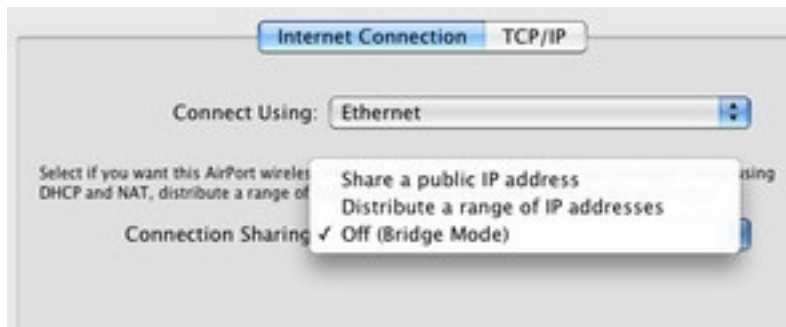
Know Your Network, Lesson 5: Bonus Features and Further Resources

You've [picked out your hardware](#) and [set up the basics](#), [optimized your network for speed and performance](#), and [set up remote access](#). Now it's time for a little fun. Here's a look at some cool bonus features you may have on your router and how you can learn more.

Bonus Features

We've already covered most of the great big things you'd want to do with your home network, but there are a few extras your router may support that could come in handy right now or some day down the line. We're going to give you a brief overview of some of these bonus features so you can decide if you want to give them a shot and learn more about them.

Bridge Mode



If you have more than one router, you probably don't have much use for the second one. That is, unless it's in bridge

mode. Bridge mode will

turn a router into a Wi-Fi repeater so it can take the signal from your original router and broadcast it in another area of your home. If you're trying to get better wireless coverage around the house, this is a good way to make it happen.

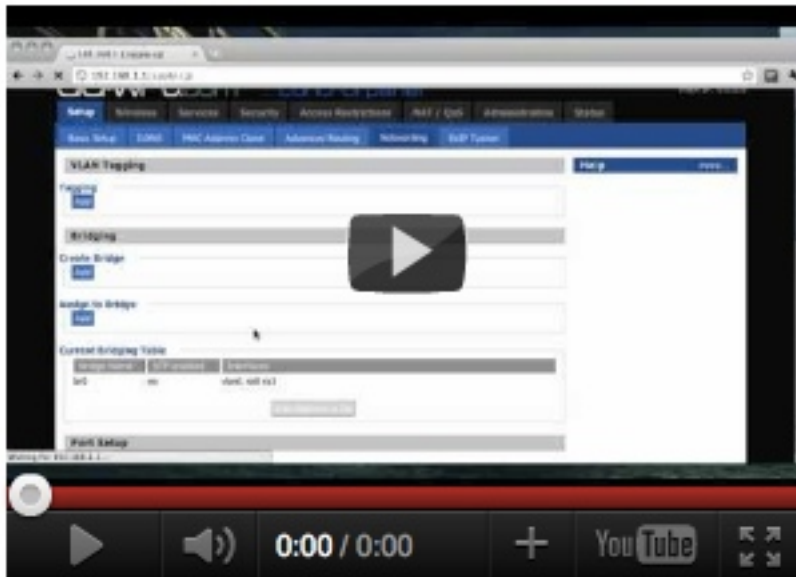
Bridge mode can work in two different ways, and what type of router you have will determine if you can use only one of these ways or both. More commonly you'll have the ability to connect the bridged router via ethernet and then use it only to broadcast a wireless signal. Less commonly, the bridged router can do the same thing but connect over Wi-Fi. This comes with the disadvantage of slightly degraded performance. If you have a bunch of routers in your home you also run the risk of added interference. That said, this can be an effective way to ensure you actually get a signal where you need it.

So how do you activate bridge mode? This varies a lot from router to router. The easiest routers to work with are Apple routers, as you just have to run through the setup options and choose "Connect to my current wireless network" (rather than create a new one). Then choose "Extend the range of my wireless network." That's pretty much all you have to do, aside from choosing another network. On other routers it

gets more detailed and pretty specific, so here are a few tutorials you can use for these popular brands:

- 1 [Belkin](#)
- 2 [DD-WRT](#) (custom firmware compatible with many Linksys routers and more)
- 3 [Netgear](#)

Guest Networks



You have your primary wireless network, of course, but if you want to separate guests you can set up a guest network. This will give them a separate [SSID](#) to choose when connecting and keep them from accessing

anything locally. It's not a bad idea for security and privacy purposes. You'll find the guest networks feature on custom firmware DD-WRT and some other routers as well. To see how to set it up with DD-WRT, [watch this video](#). If you want to enable guest networks on your non-DD-WRT router, first make sure you have the feature. It's more common with higher-end routers, but still not a feature every router will have. In most cases the setup will be very simple and you'll simply need to turn guest networks on.

For Cisco/Linksys E-series routers, you'll need to use the Cisco Connect software included with your router to enable a guest network. It will not be on the router admin page. Once you run the software, just click "Change" in the Guest Account area and it will create a guest username and password. When a guest connects to the guest network's SSID, that username and password will be necessary in order for them to use it.

Belkin routers with this feature will have the option [on the admin page in the Guest Access section](#). The same goes for D-Link routers, but the area is called [Guest Zone](#). Some Netgear routers should have a similar option as well. If you're using a newer Apple router, [MacLife has a great setup guide](#).

For more information on guest networks, [check out our guide](#).

Further Resources

- 1 We've mainly talked about routers in these lessons, but there's more networking hardware to learn about. The Petri IT Knowledgebase has [an article the differences between routers, switches, and hardware firewalls](#) you might want to read to learn more.
- 2 If you run into trouble down the line, DV Hardware has a handy [router troubleshooting guide](#). eHow also has a [variety of troubleshooting articles](#), some specific to certain kinds of routers.
- 3 We've already talked about how to do a lot of practical things with your home network, but it doesn't hurt to know exactly what's actually making all of that stuff work behind the scenes. HowStuffWorks has a [good explainer on the subject](#).

- 4 One of the most valuable sources for information about your router is the user guide. It's probably a little dry, yes, but it still contains lots of good things you'll want to know. If you need to ease yourself into learning about everything, look at your router's admin pages and see if there are any tool tips or sidebar help blurbs. Often times router admin pages include more information right where you'll need it most.
 - 5 Lastly, About.com [recommends several home networking books](#) if you really want to read quite a bit more. We don't have much experience with home networking how-to literature, and encourage you to explore and learn on your own, but if you like the comfort of a book you might find what you need on that list.
-

You can follow Adam Dachis, the author of this post, on [Twitter](#), [Google+](#), and [Facebook](#). Twitter's the best way to contact him, too.