

Router setup checklist

Presented for the Personal Computer Club of Charlotte, October 2018.

Note: This is not expected to be a comprehensive list of all the items to be configured in a consumer internet router.

Every router is different in the interface and features. You need to be creative to find critical settings and appropriate options.

Online resources and additional support are in the “geeky detail” appendix at end.

Configuration	Setting	Verification / comment
	Getting started	
<p><i>Follow along with the illustrated “representative router configuration” linked from the “geeky detail” appendix. Changing any settings may require you to reconfigure devices already working on your network. Be sure you record all of the modifications you make from a previously functioning network.</i></p>		
1) Connect router	<ul style="list-style-type: none"> • Connect computer with Ethernet to a numbered port. • Connect internet modem to “Internet” or “WAN” port (usually marked with yellow). <ul style="list-style-type: none"> ◦ If you don’t know login credentials, do a hardware reset; usually by holding a recessed button. A reset is different from rebooting (see your manual). 	You should see lights on the panel of the router and near the Ethernet jacks.
2) Login to router	<ul style="list-style-type: none"> • Connect to router. <ul style="list-style-type: none"> ◦ Reboot your computer. ◦ See your manual for a “manual” login. (we do not recommend installing the router software) ◦ If you do not see a login screen, see “geeky detail” appendix. • Enter the known or default credentials. 	<p>You see the first configuration screen.</p> <p><i>If your router is in use, you may want to back up current settings before you start.</i></p>
	Critical settings	
3) Internet setup Heading might be “Internet” or “WAN” settings.	<p>Probably default for most ISPs. If not, keep reading ...</p> <ul style="list-style-type: none"> • Look for instructions from your ISP. If none ... <ul style="list-style-type: none"> ◦ Select automatic or DHCP. ◦ Reboot router (<i>not</i> a hardware reset). ◦ <i>You may need to reboot your computer. You may also need to reboot your modem.</i> <p>Most routers will display their public IP address. It will look like 204.133.75.51. The numbers may be displayed differently. If it starts with 198, 172, or 10; there is another router between it and the internet.</p>	<p>Browse to the internet from your connected computer. Choose a web page that is not cached such as news or weather.</p>
4) Local network setup Heading might be “LAN” or “DHCP”.	<p>The default should be appropriate for most networks. <i>If you have multiple routers, you may need alternate settings from the defaults.</i></p> <p><i>If settings changed, you may need adjust manual settings on connected devices such as printers or TV boxes.</i></p>	You can connect to the router and other devices on your network.

5) Change default password	Find the screen with “login credentials” or “router password.” <u>Change it</u> . (There may be an additional user name to change the password for also.)	<i>Test now!</i> Log in with new password. If you can’t, try the default or reset the router and start over.
6) Remote access	<u>Disable it!</u> If offered, this could allow malicious internet users total access to your network. If possible, in addition to turning it off, assign a unique long password such as found at https://www.grc.com/passwords.htm .	
	Wireless settings	
<i>For detailed instructions, follow along on the illustrated “representative router configuration” linked from the “geeky detail” appendix.</i>		
7) SSID	Change to something you’ll recognize rather than “ISP23976”	
8) Security	Choose any flavor of WPA that works with your devices. Choose a password that won’t be easily guessed, but is easily entered from a phone.	Test your new settings from a wireless only device while you can still tweak them.
9) Guest access	If offered, enable it. You can use it for IoT devices, guests, kids, and anyone else you don’t want to see into your critical network. Use a different password and, if possible, different network settings from your primary network.	
10) WPS	If you see a setting and don’t need it, disable if possible. <i>This is a scheme to simplify connecting to your network; but the codes can be cracked in minutes.</i>	
	Things you may have to search for	
<i>Disabling or configuring is desirable if your router allows it. The settings may be listed under various headings.</i>		
11) UPnP	Also “Universal Plug and Play”. Disable it. You may find some devices require it to communicate with others on the internet (for example, multi-player games). Be sure you really want to let strangers into your system.	
12) Port forwarding	This manually does the same as UPnP. If you need to configure this manually, it may require significant experimentation between computer, router, and outside device. Every environment is different.	
13) DMZ	Disable it. This puts one device naked on the internet and exposed to anything the “Russians” or the kid next door care to throw at it. Once one computer is exposed, malware can jump to any other device on the network.	
14) Test it	Go to https://www.grc.com/shieldsup to see if your network is exposed. <i>This only tests the router connected directly to the internet. If your modem contains a router, the test will not be valid.</i>	

The “geeky detail” appendix

The “*representative router configuration*” is annotated screenshots of