**Chapter 7 Problems and Exercises Tips**

**1) Testing Wi-Fi Connection Speeds**

Several free Wi-Fi connection speed tests are available on the public Internet that enable you to determine the robustness of your Wi-Fi connection from different locations of your residence. Most of these tests work by receiving a fixed-sized download and sending a fix-sized upload to a single Internet server and using the duration of the download and upload as a measure of connection speeds. It is important to note that the broadband connection between your Wi-Fi router and ISP is typically the main bottleneck that limits the total possible connection speed for your network. This means that most Wi-Fi speed tests produce results showing connection speeds that are likely to be significantly lower than the maximum speeds that ISPs advertise.

This exercise illustrates the use of the Wi-Fi Speed Test at Optimum.com, so it starts by using your device (smartphone, tablet, laptop) and using your browser to navigate to the Optimum.com web page (<https://www.optimum.com/internet/wifi/speed-test>). Optimum has partnered with Ookla for Wi-Fi testing. Ookla uses secure third-party test servers for measuring data transfer rates and latencies. You can access Ookla’s testing platform at <https://www.speedtest.net/>.

When testing your Wi-Fi speed, it is important to remember that many factors can impact your test results, including device distance from the Wi-Fi router; the total number of devices connected to the Wi-Fi router; the type of device you use to do the tests; and the Wi-Fi router’s age and ability to support the later Wi-Fi generations’ capabilities.

To directly test the speed of the link from the Wi-Fi router to your ISP, you can use an Ethernet cable to connect your laptop to one of the router’s RJ45 ports. Running this test first enables you to determine the maximum connection speed that is possible for your network.

To test your Wi-Fi performance, you should use a portable device (e.g., a laptop, tablet, or smartphone) that is connected to your Wi-Fi network. To illustrate concepts from this chapter, you should run your Wi-Fi speed test multiple times from different locations in and around your residence. You should also repeat your sequence of tests using both the 2.4 GHz and 5 GHz connection options, if they appear as distinct options in your list of available Wi-Fi networks.

To get a clear picture of your device’s Wi-Fi connection and performance, you should disconnect all other devices on your WLAN while doing the Wi-Fi speed test. If this is not possible (e.g., you may not want to turn off Wi-Fi connected IoT sensors), do your best to ensure that they are currently inactive or are using no data.

**Testing Instructions**

1. Create ideal test conditions by disconnecting other wireless devices from your WLAN. Connect your device to the network, ideally using the 5 GHz connection option if it is available. Get as close as you can to your Wi-Fi router (ideally within five feet), launch your device’s browser, navigate to the Wi-Fi test page (<https://www.optimum.com/internet/wifi/speed-test>), and click the GO button to perform the test. Record your test results. (An example of a table for recording test results is provided below.)

2. Move as far away as you can from the Wi-Fi router while still in the same room. Repeat the Wi-Fi speed test and record your results.

3. Move to a room that is adjacent to the room with the Wi-Fi router, repeat the speed test, and record the results.

4. Move to a room that is farthest from the room with the Wi-Fi router, repeat the speed test and record the results.

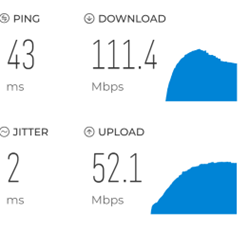
5. Move to a location that is outside your residence but in an area where you can still connect to the network. Repeat the speed test and record your results.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Device** | **Wi-Fi Band** | **Location** | **Ping (ms)** | **Jitter (ms)** | **Upload (Mbps)** | **Download (Mbps)** |
| *(e.g., laptop)* | *(e.g., 5 GHz)* | Next to router |  |  |  |  |
|  |  | Same room |  |  |  |  |
|  |  | Adjacent room |  |  |  |  |
|  |  | Distant room |  |  |  |  |
|  |  | Outside residence |  |  |  |  |

6. Identify and describe the patterns that you observe in your test results.

* Does the distance between the device and the Wi-Fi router make a difference?
* Do walls make a difference in test results?

**Tips for Success:** Be sure to complete the entire table. You are encouraged to do a screen or snip capture for each test; your instructor may require that you do this to verify that the entries in your table are correct. An example of a test result snip is provided below.



Be sure to provide answers to part 6 questions and be sure that they are consistent with your test results.

**Additional Tests (Optional)**

Disconnect your device from the 5 GHz band, connect to the 2.4 GHz band, and repeat the sequence of Wi-Fi speed tests specified in the instructions above. Record your results.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Device** | **Wi-Fi Band** | **Location** | **Ping (ms)** | **Jitter (ms)** | **Upload (Mbps)** | **Download (Mbps)** |
| *(e.g., laptop)* | *(e.g., 2.4 GHz)* | Next to router |  |  |  |  |
|  |  | Same room |  |  |  |  |
|  |  | Adjacent room |  |  |  |  |
|  |  | Distant room |  |  |  |  |
|  |  | Outside residence |  |  |  |  |

7. Identify and describe the patterns that you observe in your test results.

* Does the Wi-Fi band (2.4 GHz versus 5 GHz) make a difference?
* Does the distance between the device and the Wi-Fi router make a difference?
* Do walls make a difference in test results?

Disconnect and power off the device used for the first round of results. Connect to the network using a different device, repeat the Wi-Fi speed tests, and record your results.

8. Identify and describe the patterns that you observe in your test results.

* Does the type of device used for the tests make a difference?
* Does the Wi-Fi band (2.4 GHz versus 5 GHz) make a difference?
* Does the distance between the device and the Wi-Fi router make a difference?
* Do walls make a difference in test results?

**Additional Tests Tips for Success:** The answers that you provide for items 6, 7, and 8 should be consistent with the data in the tables and any screenshots or snips that you are required to submit. You should avoid only yes or no answers and you should focus on identifiable patterns in the tables.

Your instructor may use a grading rubric like the following to evaluate your work.

|  |  |
| --- | --- |
| **Grading Dimension** | **Points** |
| Submitted on time? | 10 |
| Are table rows complete? | 10 |
| Are Item 6 questions answered? | 10 |
| Are Item 6 answers based on data patterns in the table? | 10 |
| Are Item 7 questions answered? | 15 |
| Are Item 7 answers based on data patterns in the table(s)? | 15 |
| Are Item 8 questions answered? | 10 |
| Are Item 8 answers based on data patterns in the tables? | 10 |
| Are Items 6-8 answers free of spelling errors and other grammatical shortcomings | 10 |
| **Total points** | **100** |

**2) Configuring Wi-Fi Router Security Settings**

***Overview***: For this exercise, you will use an online Wi-Fi simulator that will enable you to modify the settings of a simulated Wi-Fi router. As you complete this exercise, you will (a) be saving screenshots/snips for the Wi-Fi router setting changes and (b) be providing explanations/descriptions of how the setting changes will affect how the Wi-Fi router works and its security. This exercise illustrates multiple concepts discussed in Chapter 7, especially those associated with Wi-Fi security.

***Instructions:***

Open a Web browser and go to: <https://ui.linksys.com/WRT54GS2/1.0.00/Basic.htm> (or an alternative router simulation specified by your instructor).

**Part A:**

1. Click the Wireless navigation link. Then click the Manual configuration option.
2. Change the Wireless Network Name (SSID) to Yourname’s Network (where Yourname is your first and last name).
3. *Briefly describe what will happen* to your device’s list of available networks when the network’s SSID is changed to Yourname’s Network.
4. Change the Wireless SSID Broadcast status from Enable to Disable.
5. *Briefly describe what will happen* to your device’s list of available networks when the SSID Broadcast Status is changed to Disable.
6. Change the Channel number from its default setting (6) to one of the other nonoverlapping channel numbers for the 2.4 GHz Wi-Fi band.
7. Take a **screenshot** (or snip) displaying the new nonoverlapping channel number and other setting changes made in steps 2–6 to verify/document your setting changes.

**Part A Tips for Success**: This part of the exercise illustrates several basic characteristics of Wi-Fi networks. Sections 7.1.2 and 7.3.1 are especially relevant. Be sure to provide answers for items 3 and 5; there is no need to overthink how to answer these and it is best to avoid the inclusion of technical details from online sources. Non-overlapping channels are identified in Section 7.3.1. Be sure that your step 7 screenshot(s)/snip(s) illustrate the changes that you implemented in steps 2 through 6.

**Part B:** Click Wireless Security (next to Basic Wireless Settings on the menu bar).

1. Change the Security Mode from Disabled to that for the *most secure* wireless security mode that is available.
2. Capture a **screenshot/snip** of the setting change made in Part B, step 1 (showing the most secure wireless security mode).
3. *Briefly describe* how the security setting change will affect what new users will have to do when they log onto the Wi-Fi network for the first time and the security of the frames that are transferred between their device and the Wi-Fi router.
4. Click the Wireless MAC Filter on the Wireless menu bar.
5. Click the Enable radio button, click the Permit only radio button, and take a **screenshot/snip** of the changes specified in this step.
6. Click the Edit MAC Filter List button. For MAC 01: add the Physical Address for your Wi-Fi adapter (or use: 08:C7:29:12:6B:10).
7. For MAC 02: and MAC 03: add the physical addresses (MAC addresses) of two other wireless devices (or use: 00:0D:83:B1:C0:8E and 34:31:8F:75:24:B1).
8. Capture a **screenshot/snip** of the Wireless MAC Filter list screen after making the changes specified in Part B, steps 6 and 7.
9. *Briefly explain* the impact of making the changes specified in Part B, steps 6 and 7.

**Part B Tips for Success**: Wi-Fi security protocols are identified in section 7.4.3. Be sure that you make the correct selection and that your selection is illustrated in the required screenshot for step 2 of this part. Be sure to provide a description for step 3, but this does not have to be overly detailed; it should indicate that device and AP will authenticate themselves and that data passed between them will be encrypted. Be sure to provide the specified screenshot/snip for step 5. Steps 6, 7, and 8 can be completed most easily using the specified MAC addresses, but if you were configuring a real (not-simulated) Wi-Fi router, you would have to specify the MAC addresses of the devices that connect to it. Be sure to provide an answer for step 9; essentially it should indicate that only devices with MAC addresses on the list will be able to connect to the network.

**Part C:** Click Access Restrictions on the menu bar to open the Internet Access Policy screen.

1. Change the Status to Enable.
2. For Enter Policy Name: enter Yourname’s Workweek Policy (where yourname = your first and last name)
3. Click the Edit List of PCs button and add the MAC addresses used in Part B, steps 6 and 7; set the IP Range from 192.168.1.1 to 192.168.1.100 in the Enter the IP Range of the PCs section near the bottom of the List of PCs window, then click the Save Settings button.
4. Return to the Policy screen, and for Days uncheck Everyday then uncheck Sun. and Sat.: leave M, T, W, Th, and F checked.
5. For Times, change the settings to from 06:00 AM to 06:00 PM.
6. In the Blocked Services section of the policy screen, click the first NONE button and select ping from the list. Click the second NONE button and select ftp.
7. In the Website Blocking by URL Address section of the policy screen, add [www.facebook.com](http://www.facebook.com), [www.twitter.com](http://www.twitter.com), [www.instagram.com](http://www.instagram.com), and [www.tiktok.com](http://www.tiktok.com).
8. *Briefly describe* the consequences of making the changes specified in Part C, steps 1–7.
9. Take a **screenshot/snip** that displays the settings specified in Part C, steps 1–2 and 4–7.

**Part C Tips for Success:** This part of the exercise illustrates how security and use policies can be created and configured to determine when and how the Wi-Fi network can be used by devices that are allowed to connect to it. For step 8, be sure to provide a complete and accurate description of the policy changes that identify when the network can be used, which devices can use the network, which services and websites are blocked during the times that the policy is in effect; it is better to say more rather than less in this description. Also, be sure to provide the specified screenshot/snip for step 9 because this will verify that you made the changes specified in steps 2, 4, 5, 6, and 7.

**Part D:** Click Administration on the menu bar.

1. Change the router default password.
2. For Access Server, make sure that both options are checked and enable Wireless Access.
3. Change Remote Management to Enable; check the Use https checkbox.
4. Take a **screenshot/snip** displaying the changes specified in Part D, steps 1–3.
5. *Briefly explain* the consequences of making the settings changes specified in Part D, steps 1–3.

**Part D Tips for Success**: Be sure to provide the screenshot/snip specified for step 4. This will verify completion of steps 1-3. Be sure to provide a complete and accurate description of the consequences of the configuration changes. This should indicate that changing the default password will make the router more difficult to hack; it should also indicate that enabling remote management will make it possible for the administrator to connect remotely to the router to make configuration changes even if he/she is connected to a wireless network and the https option ensure that any configuration changes specified by the administrator will be encrypted.

**Additional Tips for Success:** Your instructor may use a grading rubric like the following to evaluate your work.

|  |  |
| --- | --- |
| **Assignment Component** | **Points** |
| Submitted on or before due date. | 10 |
| Part A, step 3: SSID change explanation | 5 |
| Part A, step 5: SSID disable explanation | 10 |
| Part A, step 7, screenshot | 5 |
| Part B, step 2: WPA settings changes screenshot | 5 |
| Part B, step 3, WPA settings explanation | 10 |
| Part B, step 5, MAC & PC filter enable screenshot | 5 |
| Part B, step 8, screenshot | 5 |
| Part B, step 9 explanation | 10 |
| Part C, step 8, policy settings explanation | 15 |
| Part C, step 9, policy settings screenshot | 5 |
| Part D, step 4 administration screenshot | 5 |
| Part D, step 5 admin access & security explanation | 10 |
| **Total Points** | **100** |