**Chapter 5 Problems and Exercises Tips**

**1)** **At a Windows computer command line, type: ipconfig /all. *Note:* On a Windows computer, the command prompt is included in the Windows System folder. The results will resemble the following:**

**A screenshot of a computer

Description automatically generated**

**Note: On a Windows 11 computer, you can find comparable information by navigating to the Network and internet setting screen, selecting Advanced network settings, and selecting Hardware and connection properties. The results obtained will resemble the following:**

**A screenshot of a computer

Description automatically generated**

**A) Create a Word document and insert a screenshot or snip of the configuration of your computer’s active network adapter. Beneath your screenshot or snip, provide your answers for Item B.**

**B) Using the section of your results for your active adapter (Ethernet or Wi-Fi):**

1. **Identify the adapter’s MAC address(es).**
2. **Identify your device’s logical Network layer address.**
3. **Identify the value that would be included in the Source Address field of IPv4 packets created by your computer.**
4. **Identify the value that would be included in the Source Address field of the Data Link layer frames created by your computer.**
5. **Identify the device in the list that your computer would contact when its lease expires.**
6. **Identify the device in the list that your computer would contact to identify the IP address of the network that includes a host with which you want to communicate.**
7. **Identify the device in the list that your computer would contact to send packets to computers in other networks.**

**Tips for Success**: This is hands-on exercise that illustrates numerous concepts Chapter 5 including the differences between IP and MAC addresses, DHCP, DNS, and routers. It is easiest to complete on a Windows computer. The exercise can help you connect some of the dots between device configurations and addressing and routing concepts and services. Because the configurations of devices in TCP/IP networks differ, you should complete all parts of this exercise on the same machine.

It is easy for an instructor to detect cheating on this assignment because computers have different MAC and IP addresses. If your instructor encounters identical screenshots or answers, they will know that cheating has occurred.

For part a, it is important to understand that a MAC address is also called a Physical address. For part b, Section 5.4.1 is relevant. Figure 5-17 is relevant to part c. Section 4.4.4 is relevant to part d. Sections 5.1.3 and 5.1.4 are relevant to parts e and f. Section 5.4.2 is relevant to part g.

**2)** **Ping is a tool that can be used to identify the reachability of computers in your network or other networks attached to the Internet. It can also be used to identify the amount of time it takes to get a response from the other host. Ping sends a small packet to the other computer. Like *ipconfig*, ping is used at the command prompt. Due to security concerns, not all networks support ping, since it can be used to identify IP addresses associated with URLs and determine whether another host is active and reachable. Such networks will not respond to ping requests.**

**A) At the command prompt, type *ping* followed by the IP address for your network’s Default Gateway—the router that serves your local network. *Note*: To identify the IP address for your Default Gateway, refer to Exercise 1. Your results should resemble the following:**

**A screen shot of a computer

Description automatically generated**

**Document the completion of this step by adding a screenshot or snip of your results for pinging your network’s router to a Word document.**

**B) At the command prompt, type ping followed by amazon.com. Note that the round-trip time is more than that obtained when you pinged your local router because amazon.com is on a different network. Also note that your ping results identify the Amazon.com IP address. To verify your completion of this step, add a screenshot or snip of your ping results to your Word document.**

**C) At the command prompt, type ping followed by unsw.edu.au (the domain name for the University of New South Wales in Sydney, Australia). Include a screenshot or snip in your Word document to verify the completion of this part of this exercise. Students in the United States should note that the round-trip time is higher than those for their previous pings because the university’s network is on a different continent.**

**Tips for Success**: This hands-on exercise features ICMP’s Ping utility. Be sure to include two screenshots and an explanation for why the round-trip time to a distant network is higher than that for the local network. The local router is called the Default Gateway in the response to the ipconfig /all command for your Windows computer.

For the round-trip distance differences explanation, explain why in your own words and don’t use those from online or AI sources.

**3)** **You can use *nslookup* at the command prompt to issue a DNS request to identify the IP address of a network that includes a particular domain name. For example, typing nslookup followed by the domain name for Home Depot (homedepot.com) produces the following results:**

**A black background with white text

Description automatically generated**

**A) Use nslookup at the command prompt to identify the IP address for Slack.com and another website of your choice. Note that your DNS request may return more than one IP address. To verify completion of this exercise, include screenshots or snips of your nslookup results in a Word document.**

**Tips for Success**: This hands-on exercise enables you to see firsthand that a DNS name server associates IP addresses and website/network/domain names. Be sure to provide two screenshots for the responses to your two nslookup commands at the command prompt, including one for Slack.com.

**4) You can use *ipconfig*/*displaydns* at the command prompt to show the contents of your computer’s DNS cache. The DNS cache is basically a list of the Internet domains and their associated IPv4 or IPV6 addresses that your computer consults prior to sending a request to the DNS for an IP address. When you visit a new website, your DNS cache is typically updated. The results returned when this command is used resemble the following but may be quite lengthy, depending on your recent online activity:**

A screen shot of a computer

Description automatically generated

**A) Type *ipconfig*/*displaydns* at the command prompt to view the contents of your computer’s DNS cache. Include one or more screenshots or snips of your results in a Word document to verify completion of this exercise.**

**Tips for Success**: This exercise shows that your computer has a DNS cache that includes the names and IP addresses of recently used/visited networks/websites/services. The exercise illustrates that a device has a DNS cache that it consults prior to step 1 in Figure 5-7 and Table 5-3. If the needed information is not in the local cache, the machine contacts the local DNS server for assistance. Be sure to include one or more screenshots or snips of the contents of your computer’s DNS cache.

**5)** **You can use the *tracert* command at the command prompt to identify the number of routers (hops) involved with transferring a tracert packet to another network attached to the Internet. Because tracert information can be used maliciously by attackers, numerous networks do not respond to tracert packets for security reasons. The following displays the results from typing tracert unsw.edu.au, (the domain name for the University of New South Wales in Sydney, Australia) at the command prompt:**

**A computer screen shot of a computer program

Description automatically generated**

**These results show that 21 routers were involved in transferring the tracert request from a host in the United States to the UNSW network.**

**A) At the command prompt, type *tracert facebook.com*. To verify completion of this activity, include a screenshot/snip of your tracert results in a Word document.**

**B) Use *tracert* to identify the number of hops to another Internet domain of your choosing and include a screenshot/snip of your results in your Word document. Note: You may have to try this for several domains to get results—mit.edu is a domain that typically returns tracert results**.

**Tips for Success**: This exercise provides hands-on experience with ICMP’s tracert utility and it illustrates that multiple routers (hops) are usually involved in transferring a packet between different networks. Like Ping, not all networks/websites support tracert. Be sure to include a screenshot/snip for each response to the tracert commands.

**6) You can use Wireshark to view your computer’s interactions with the DNS to identify the IP address for a website. Completing this exercise will demonstrate that your computer will issue a DNS request for the IP address of a website that is not in its DNS cache. Wireshark and its use were introduced in the exercises for Chapter 4.**

**A) Some preliminary activities are necessary before using Wireshark:**

**1) Use *ipconfig /All* at the command prompt to identify the IP addresses for your computer and your network’s DNS server.**

* 1. **What is your computer’s IP address?**
  2. **What is the IP address of your network’s DNS server?**

**2) Type *ipconfig /flushdns* at the command prompt to empty your computer’s DNS cache.**

**B) Next, open Wireshark and type “ip.addr==your IP address” (e.g., ip.addr==192.168.0.111) in the filter in the upper left hand corner of the screen, as shown below.**

**A screenshot of a computer

Description automatically generated**

**This will limit your capture to the packets coming from or going to your device.**

**Then double-click your active adapter (Ethernet or Wi-Fi) and begin to capture packets.**

**C) Use your web browser to visit** [**www.icann.org**](http://www.icann.org)**, and stop your packet capture after the web page has loaded.**

**D) Locate the DNS query and response messages for** [**www.icann.org**](http://www.icann.org) **in your packet list.**

1. **What Transport layer protocol was used for the DNS query?**
2. **What Transport layer protocol was used for the DNS response?**
3. **What source and destination ports are specified in the DNS query?**
4. **What source and destination ports are specified in the DNS response?**
5. **What IP address for icann.org is specified in the DNS response message?**
6. **What destination IP address is specified in the DNS query?**
7. **What destination IP address is specified in the DNS response?**

**E) Locate the HTTP GET message for** [**www.icann.org**](http://www.icann.org) **in your packet list.**

1. **What is the source IP address?**
2. **What is the destination IP address?**

**Tips for Success**: This hands-on exercise helps to illustrate the use of layered communications in TCP/IP networks.

If you have not used Wireshark, you should consider completing the Wireshark tutorials identified in Exercise 4-2 in Chapter 4 to increase your comfort level with Wireshark.

In Part A, it is important to clear your computer’s DNS cache to force it to consult the local DNS name server to help identify the IP address of the specified site.

For Part B, stop capturing packets before typing the IP address filter in the filter box.

For Part C, you can stop capturing packets in Wireshark immediately after the website loads in your browser window.

In Part D, you need to explode the layers of the DNS request and response messages. These messages can be isolated by clicking the Protocol column and scrolling down; this will sort the protocols in alphabetical order. When you explode the messages, you can see that frames carrying DNS messages include IP packets and (typically), UDP datagrams. Be sure that you provide responses for each Part D question (questions a-f),

For Part E, if you sorted the protocol list for Part D, it should not be hard to find the frames that include HTTP messages.

Your instructor may require you to provide screenshots/snips to verify your completion of each step.