Hands-on Project 9-7: Working with DNS Tools in Windows 10
Time Required: 15 minutes
objective: Use ipconfig and nslookup to work with DNS.
Required Tools and equipment: Your Windows 10 computer
Description: In this project, you use ipconfig to display and delete your DNS cache and then view your hosts file. You also use nslookup to query your DNS server.

1. If necessary, log on to your computer and open a command prompt window. Start a Web browser and navigate to a Web site, such as www.cengage.com. This step loads some records in the DNS resolver cache. Exit your browser.

2. To see the DNS resolver cache, type ipconfig /displaydns and press enter. To delete the entries, type ipconfig /flushdns and press enter. Display the DNS resolver cache again. Unless there are entries in your hosts file, there is no output.

Tip
At the command prompt, you can press the up and down arrow keys to access recent commands you have entered.

3. To perform a DNS lookup, type ping www.cengage.com and press enter. Display the DNS cache again. You should see a DNS record for www.cengage.com that includes the IP address and other information. Another field in the DNS cache is a TTL value. This DNS TTL value is sent by the DNS server maintaining the www.cengage.com record. It's measured in seconds and tells your DNS client how long to cache the DNS record as a safeguard against clients holding on to DNS records whose IP addresses might have changed.

4. To open your computer's hosts file, type Notepad in the search box and press enter. From the Notepad menu, click File and then click open. In the Open dialog box, navigate to C:\Windows\System32\drivers\etc. In the File type drop-down list at the lower-right side of the window, click All Files. Double-click the hosts file to open it.

5. After the last line in the file, type 67.210.126.125 books. Save the file by clicking File and then Save As. Click desktop in the left pane, and in the File name text box, type "hosts". (You must include the quotation marks so that Notepad doesn't save the file with the .txt extension.) Exit Notepad.

6. Open File Explorer, navigate to the desktop, and copy the hosts file you just saved. Then navigate to C:\Windows\System32\drivers\etc and paste the file there. When prompted to confirm, click Replace the file in the destination. When prompted, click Continue. Close File Explorer.

7. At the command prompt, type ipconfig /displaydns and press enter to see that the entry is in your DNS cache. Type ping books and press enter. Delete the DNS resolver cache (see Step 2)

and then display it again. Notice that the books entry remains in the cache because the hosts file data always stays in the cache.

8. Type nslookup www.cengage.com and press enter. Your DNS server's name and IP address are displayed along with the name and IP addresses of www.cengage.com. You use nslookup to look up a host's IP address without actually communicating with it.

9. Type nslookup and press enter. You enter interactive mode. Type www.yahoo.com and press enter. You might see more than one address along with one or more aliases (other names that www.yahoo.com goes by). Type www.yahoo.com again (or press the up arrow to repeat the last line you typed) and press enter. You should see the IP addresses returned in a different order. (If you don't, keep trying, and the order will change.) The www.yahoo.com page can be reached by a number of different IP addresses, and the addresses are returned in a different order so that a different server is used each time, which is called "round-robin load balancing."

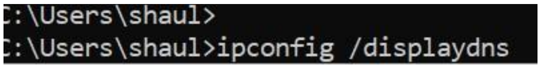
10. Type 198.60.125.150 and press enter. Nslookup is also used to do reverse lookups, in which the IP address is given and the host name is returned.

11. You can change the DNS server that nslookup uses. Type server 8.8.8.8 and press enter to change the DNS server to a server run by Google. Type www.microsoft.com and press enter. If you're ever concerned that your DNS server isn't working correctly, you can test it with nslookup and compare the results of your DNS server with the results from another server, such as Google's.

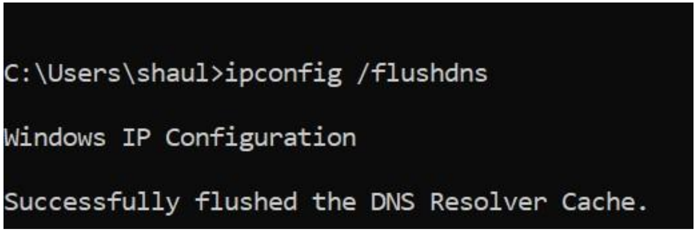
12. Close all windows and shut down your Windows 10 computer.

Hands-On Project 9-7

1. I’m logged into my Windows 10 computer. I open the command prompt and load a website.
2. *I* type in *ipconfig /displaydns* to see the DNS resolver cache, and then I type in *ipconfig /flushdns* to delete.



```
:\Users\shaul>
:\Users\shaul>ipconfig /displaydns
```

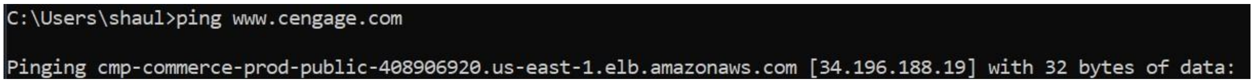


```
C:\Users\shaul>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.
```

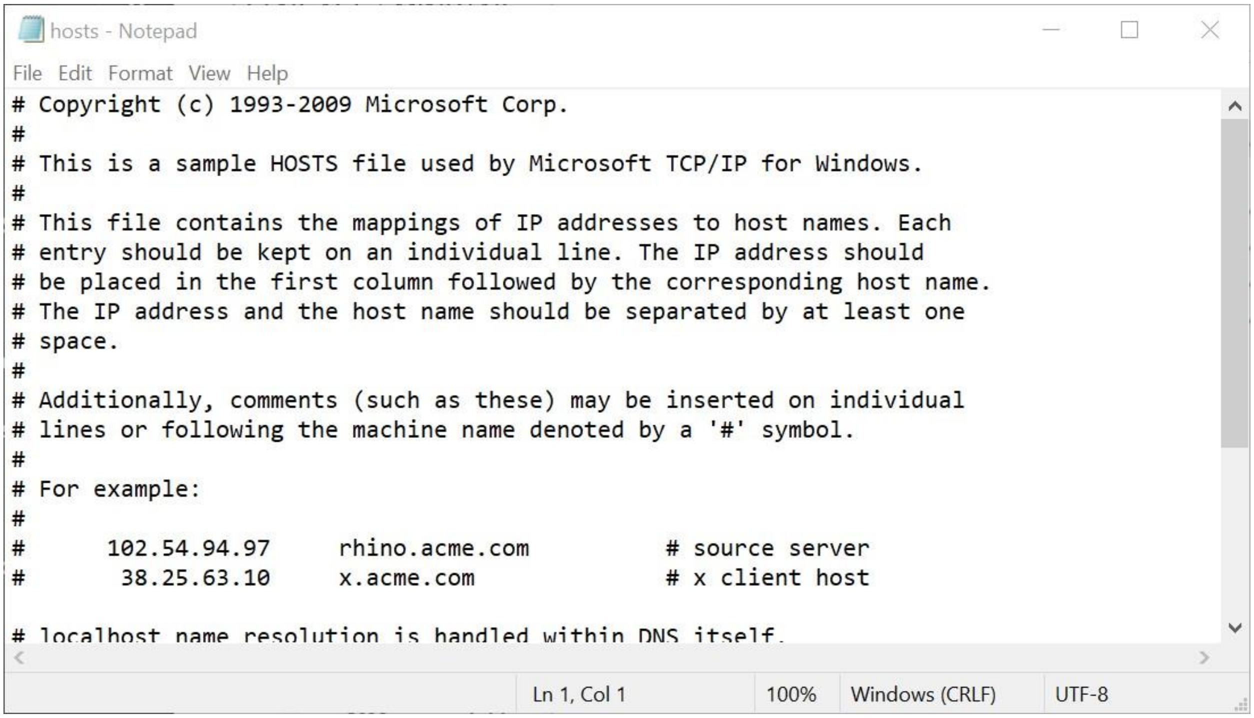
3. I perform a DNS lookup for Cengage’s website.



```
C:\Users\shaul>ping www.cengage.com

Pinging cmp-commerce-prod-public-408906920.us-east-1.elb.amazonaws.com [34.196.188.19] with 32 bytes of data:
```

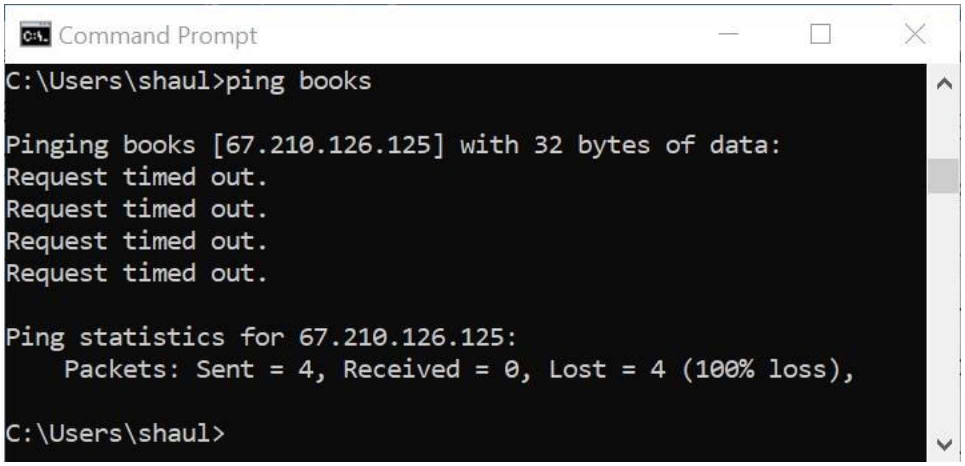
4. I open the *hosts* file using Notepad.



```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
```

5. I add “67.210.126.125 books” to the end of the file and save a copy of it to my desktop.
6. I copy the new file to folder of the original.
7. I display my cache, use ping on books, delete the cache, and display it again. I notice that the books entry remains.



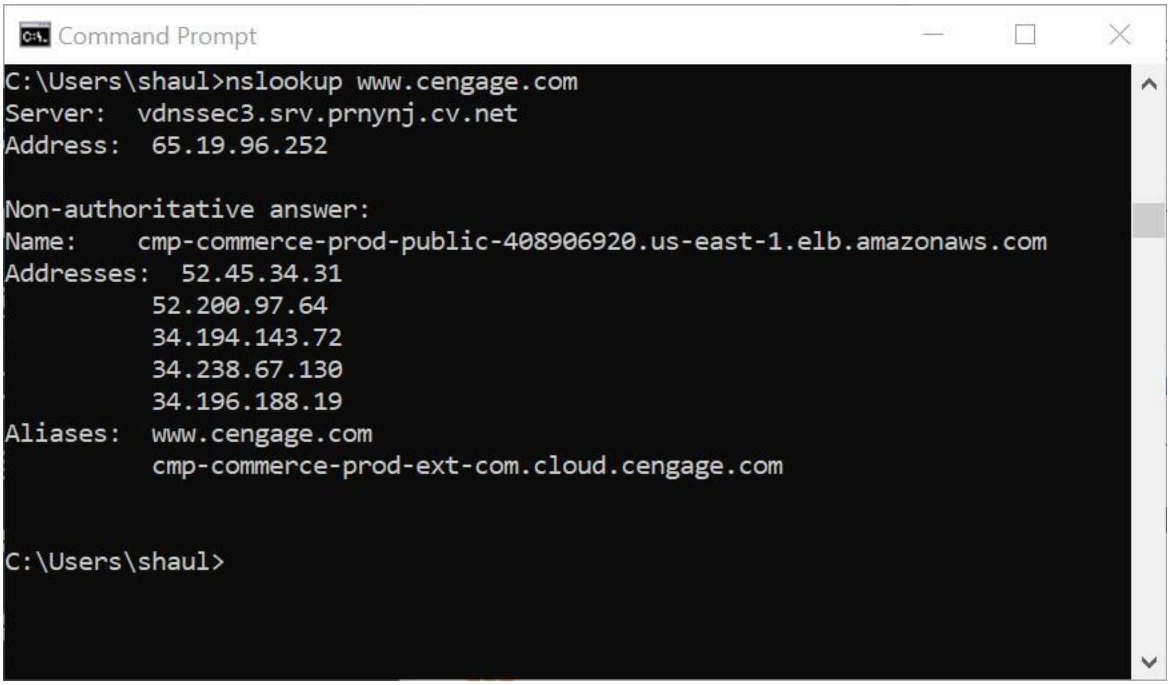
```
C:\Users\shaul>ping books

Pinging books [67.210.126.125] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 67.210.126.125:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\shaul>
```

8. I use the *nslookup* command on Cengage's website.

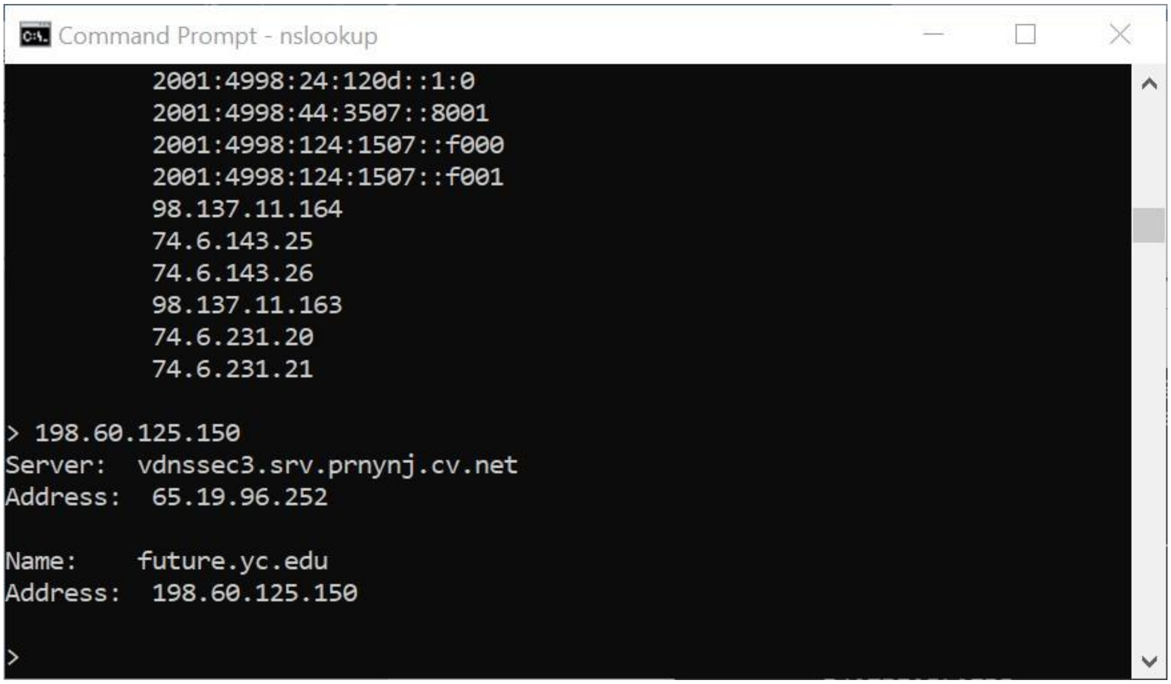


```
C:\Users\shaul>nslookup www.cengage.com
Server:  vdnssec3.srv.prnynj.cv.net
Address:  65.19.96.252

Non-authoritative answer:
Name:    cmp-commerce-prod-public-408906920.us-east-1.elb.amazonaws.com
Addresses:  52.45.34.31
          52.200.97.64
          34.194.143.72
          34.238.67.130
          34.196.188.19
Aliases:  www.cengage.com
          cmp-commerce-prod-ext-com.cloud.cengage.com


C:\Users\shaul>
```

9. I use the *nslookup* command and try Yahoo's website a few times. The IP addresses come up in different orders each time I try.
10. I type in the following IP address: 198.60.125.150. The host name of the website is returned.



```
          2001:4998:24:120d::1:0
          2001:4998:44:3507::8001
          2001:4998:124:1507::f000
          2001:4998:124:1507::f001
          98.137.11.164
          74.6.143.25
          74.6.143.26
          98.137.11.163
          74.6.231.20
          74.6.231.21

> 198.60.125.150
Server:  vdnssec3.srv.prnynj.cv.net
Address:  65.19.96.252

Name:    future.yc.edu
Address:  198.60.125.150

>
```

11. I have also learned that I can change the server used by *nslookup*. For example, I can type in server 8.8.8.8 to use a server run by Google.