

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.