Activity 2.1.3c Protocols and Bandwidth

Part V: Use the domain name system to look up IP addresses

17. Use `nslookup` to find the IP address for the web server of your favorite web page. Simply type `nslookup` followed by the domain name of your favorite website.

    ```
    c9username:~/workspace $ nslookup www.coolsite.com
    ```

    Record your information here. URL of favorite website:

    _____

    IP address of favorite web server:

    _____

18. To see the work of the authoritative DNS servers, use the `dig` (domain information groper) program with the `+trace` option as shown below.

    ```
    c9username:~/workspace $ dig www.example.org +trace
    ```

    …lots of output and finally the output:

    ```
    www.example.org.  4697    IN   A    93.184.216.119
    ```

    There is much more output from the dig program than shown here. First, the recursive DNS server reports the domain name of one or more root servers. The recursive server asks one of the root servers for the IP address of `www.example.org`. That root DNS server responds with the domain names (and IP addresses, though not shown in the output) for the `.org` name servers. The `NS` records refer to other name servers, while the `A` record shown above finally gives the address.

    How many separate machines are serving DNS for the top-level `.org` domain?

Part VI: Measure latency and bandwidth

The `ping` command is another commonly used tool to see behind the curtain in a computer network, on both Windows and UNIX-like systems. The command uses a simple protocol: one host sends a packet asking for an echo, and the target host responds. The ping command repeats the process for many iterations. It reports how long the round trips took and whether any packets were dropped. Use Ctrl-c to **kill** the `ping` **process**. A process is a program or distinct thread of a program. Killing a process tells the operating system to stop executing it.

19. Execute the command with your own choice of domain name in place of `www.example.org`. The last line of output is shown below.

    ```
    c9username:~/workspace $ ping www.example.org
    rtt min/avg/max/mdev = 17.385/17.439/17.585/0.108 ms
    ```

    This output shows that the packets traveled round trip from `pltwcs.org` to `www.example.org` in `17.439 ms`, on average. A signal can travel one million feet of copper wire in `1 ms`!

    Try a few domains; what is the fastest response you can find?

23. Given the download speed you measured, calculate how long it would take to download a 450 kb file. Show your work.

Part VII: Observe that IP packets travel multiple paths

24. Use `whatsmyip.org` in a new browser tab to identify the IP address of your computer. (This might be your school's router's IP address. ipconfig would find your computer's IP address, but it might be only internal to the school network. We'll ignore these complications.)

    Record the IP address from the top of the page.

    To find the paths from the Cloud9 server to the computer that you are using, you need the tracepath utility.

25. First, install tracepath on the Cloud9 machine using the following command.

    ```
    c9username:~/workspace $ sudo apt-get install iputils-tracepath
    ```

    The `sudo` command lets you execute any other command as the "superuser" with unlimited rights. The `apt-get` program is the advanced packaging tool, and it takes two arguments: a command like `install` and a package like `iputils-tracepath`.

    You should see lots of output.

26. Now, execute the `tracepath` command on the server, followed by your computer's IP address. Ctrl-c will stop the tracepath program early if desired. Use your IP address instead of `63.152.11.159` as in the example below.

    Packets contain the maximum number of hops that can be sent, known as the time-to-live (TTL). When an Internet host forwards a packet, it **decrements** the TTL. If the TTL reaches 0, the packet is dropped and an error message is sent back to the sender's IP. The tracepath program sends IP packets that will survive only one hop, two hops, or three hops, and so on, so it can receive error messages from the machines along the way to the destination, revealing their IP addresses. Some machines won't send back an error message if they get a packet that has run out of hops, resulting in "no reply".

    How many hops does it take to reach you? As an example, one line of output is shown below, indicating that a packet sent to `63.152.11.159` that was set to expire after five hops had reacher of hop #5 is shown below.

```
c9username:~/workspace $ tracepath 63.152.11.159
mi
rtt
5:  PR01.LAX03.google.com (206.223.123.21) 17.827ms
```