CS301: Computer Networks

Assignment 1: Basic Networking Tools and Application Layer Protocols (HTTP & DNS)

Deadline: 2nd September 2023, 11:59 PM

Goals of the Assignment:
1. Study and use various network diagnostic tools.
2. Study and understand application layer protocols (HTTP, DNS) using packet analyzer and other tools.

Part 1: Basic Networking Tools

Instruction: Perform the experiments on a Unix/Linux-based computer.

Q1. Answer the following questions related to the ***ifconfig*** command. **[3 Points]**

(1) Run the ifconfig command and briefly describe its output (important attribute). **[1.5]**

(2) What options can be provided with the ifconfig command? Mention and explain at least four options. **[1.5]**

Q2. Answer the following questions related to the ***netstat*** command. **[5 Points]**

(1) What is the use of the netstat command? **[1]**

(2) Find all the active TCP port on your system. Identify the ports and PIDs of your web browser. Can you identify the port number and PID of specific TAB in your browser? Find out if any of the services running in your system uses the standard ports of HTTP, DHCP, DNS, SMTP, and FTP. **[3]**

(3) What option of *netstat* can be used to show the statistics of all UDP connections? Run the command on your computer and show the output. **[1]**

Q3. Answer the following questions related to the ***ping*** command. **[4 Points]**

(1) What is the use of the ping command? **[1]**

(2) Select three hosts of your choice on the Internet and experiment with pinging each host 10 times at three different hours of the day. You can use the following online tool or some other tool for this experiment.

Link: https://subnetonline.com/pages/network-tools/online-ping-ipv4.php

(a) List out the average RTT for each host in tabular form and explain whether RTT has a correlation with the geographical distance of the destinations from the source. **[1]**

(b) Pick one of the above-used hosts and repeat the experiment with different packet sizes ranging from 64 bytes to 2048 bytes. Plot average RTT vs packet size. **[1]**

(c) Explain how the change in packet size, and time of the day impact RTT. **[1]**

Q4. Answer the following questions related to the ***traceroute***. **[8 Points]**

(1) What is the use of traceroute tool? **[1]**

(2) Inspect the cases when the traceroute does not find complete paths to some hosts and explain the reasons. **[2]**

(3) Is it possible to find the route to certain hosts which fail to respond with the ping experiment? Give reasoning. **[2]**

(4) Use the traceroute program to find the route to three of your favorite sites on the Internet. Draw a graph of your results, labeling each node with the IP address of the hops between your location and the destinations. The links between them should be marked with the measured delays between each link. **[3]**

Part 2: HTTP

Instruction: Start packet capture just before opening https://www.iitbhilai.ac.in website and stop the packet capture once the complete page is loaded (or you can wait for 2 minutes and then stop the packet capture). Save the pcap file and answer the following questions by analyzing the packet traces.

1. When you browse IIT Bhilai main page (https://www.iitbhilai.ac.in) how many get request is sent (how many of the GET request are for embedded content and how many get request for the text)? Plot the IO graph for packets sent to iitbhilai.ac.in and packets received from iitbhilai.ac.in **[3]**

2. For each HTTP GET request as you see above, find out (i) the total amount of data being received in the corresponding HTTP response message. **[2]**
3. For the response to your HTTP GET request, get the image reconstructed by hex editor. **[2]**

4. **HTTP Conditional GET:** Answer the following questions. **[4]**
   a. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE" line in the HTTP GET?
   b. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?
   c. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE:" line in the HTTP GET? If so, what information follows the "IF-MODIFIED-SINCE:" header?
   d. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.
5. Surf a website (other than google.com) of your choice and discuss the end-to-end process of web page loading using Wireshark. How much time did it take to load the page? Find out how many connections are used to download this page. Are these connections persistent or non-persistent? How many objects

have been transferred on these connections? Which object took the longest time to download? **[5]**

Part 3: DNS

1. The root servers on the Internet are in the domain root-servers.net. You can see the list of all root servers using ***dig*** *[DNS lookup utility] or any tool/command.* **[6]**

   Use dig to ask the root server the address of www.iitbhilai.ac.in, without recursion. Go through the hierarchy from the root without recursion, following the referrals manually until you have found the address of www.iitbhilai.ac.in

   List all the name servers involved to find out the IP address of the www.iitbhilai.ac.in.

   Do the same exercise for 2 more websites with different top-level domains (.com, .edu, .org, etc.)

Deliverables in a tar ball on GC:

- Submission Guidelines: Upload the Assignment Report, pcap in GC as a tar ball with file name as <your roll no>_<your name>.tar
- Readable Report [2 Points for report quality] enumerating steps followed with screenshots for each of the important steps.
  - Pcap trace collected and mention the command/tool used.
  - Put the screenshots (**mandatory**) to validate your answers in the report.
  - Clear and concise writing.

Check Web sources for more information.