COL374/672 Computer Networks: 2022-23 Semester I

Assignment 1

Networking Tools

This part is aimed to make you familiar with basic networking tools. Read the man pages of the tools *ifconfig* (ipconfig), *ping*, *traceroute* (tracert), and *nslookup*.

1. Find the IP address of your machine. Try connecting to different service providers and notice the changes, if any, in the IP address of your machine.
2. Find the IP address associated with www.google.com and www.facebook.com using *nslookup*. Change the DNS server (look for open DNS servers on the web) to use in the command and see how IP address of the above domains change.
3. Ping the IP address of www.google.com .Send the *ping* packets with different packet sizes, TTL values, etc.
4. Run *traceroute* via two or more service providers for www.iitd.ac.in. If your ISP blocks packets on the path to www.iitd.ac.in then try with a different destination like www.google.com, or www.facebook.com, etc. Report your observations, like if some paths default to IPv6 then how you can force traceroute to use IPv4, any private IP addresses(10.*.*.* or 192.168.*.*), routers that do not reply to requests, etc. What changes can you make to the traceroute request for some of the missing routers to reply?

Report your observations in the submission PDF along with the appropriate screenshots.

Packet Analysis

This part of the assignment is to make you familiar with the packet analyzer tool, Wireshark. Wireshark is free and open-source. It is used for network troubleshooting, analysis, software and communications protocol development, and education.

1. DNS Task

Use wireshark to grab all packets on your wireless interface, while visiting the website http://www.cse.iitd.ac.in from your browser. Do an ipconfig /flushdns1 before you do this activity to clear your local DNS cache. Report the following:

1. Locate the DNS query and response messages. Are then sent over UDP or TCP?
2. How many DNS queries are sent from your browser (host machine) to DNS Server(s)?
3. How many DNS servers are involved?
4. Which DNS Server replies with actual IP Address(es).
5. Do all DNS servers respond?
6. Clearly list the resource records involved in resolving the IP address of the site, mentioning, Name, value, type, TTL appropriately in the complete resolving process of this DNS conversation including query/queries and response/answer(s).

Provide appropriate screenshot from terminal and wireshark to answer the above questions in your report.

2. Iperf Task

- Start the Wireshark packet sniffer and start capturing.
- Open a terminal
- Start iperf3 in client with reverse mode destined to ping.online.net as **iperf3 -u -t 10 -c ping.online.net -p 5208 -R**
- Once the iperf3 communication is complete stop the Wireshark packet capture

Answer the following questions:

1. How many UDP packets are exchanged in this communication between iperf3 client and remote server?
2. Who is sending bulk data to whom? What is the average size of the packet sent?
3. Calculate the throughput (bytes transferred per unit time) for this UDP conversation using UDP's length field. Explain how you calculated this value using Wireshark capture in this experiment along with relevant screenshots. Verify your calculation with the one done by Wireshark using "Capture File properties" as well with the one displayed by iperf3 terminal. If you observe the major difference in your calculation and with the other two listed here, comment why and how?

In the saved file used for analysis, export only those IP packets involved in either direction (in communication) using appropriate Wireshark display filters and save it to another file to upload during submission.

3. HTTP Task

Analyse the attached HTTP/2 packet (http2-h2c.pcap) capture using Wireshark to answer the following (Hint : Use Statistics->HTTP, HTTP2 windows).

1. How many HTTP/2 and HTTP/1.1 packets are present? 10 and 2
2. How many HTTP/2 packets are exchanged between client and server here before the first object is fetched? 4 packets are exchanged
3. What main difference do you observe in headers of HTTP/2 packets displayed here, compared to the headers of HTTP/1.1 packets ? see screenshot Screenshot from 2022-08-27 16-31-58.png

4. PING Task

- Start the Wireshark packet sniffer and start capturing.
- Open a terminal. Execute **ping -s 3500 ping-ams1.online.net -c 5**
- Stop the wireshark capture and save the file for further analysis.

Answer the following questions:

1. How many total IP packets are exchanged in the communication between your host and the remote server representing ping-ams1.online.net ? 5 packets 10 request and reply
2. What is the size of each ping request sent from your host to remote server? 1008 bytes
3. Make a table for each ping request packet sent from your host to remote, the respective field indicating it, if the request packet is fragmented or not. If packet is fragmented (add details on number of IP fragments and on each fragment), Time of sending each individual fragment/packet, length of the individual fragment/packet), time of receiving ping response, the respective field indicating if response packet is fragmented or not, if response packet is fragmented, include the number of IP fragments, total actual length of data carried by the respective fragment in respective ping request and response.

see from screenshot timestamp from icmp data

actual length is 992 from ss

In the saved file used for analysis, export only those IP packets involved in either direction (in communication) using appropriate Wireshark display filters and save it to another file to upload during submission.

5. TRACEROUTE Task

- You will require traceroute software to execute this experiment.
- Start the Wireshark packet sniffer and start capturing. Open a terminal.
- Execute **traceroute -q 5 ping-ams1.online.net 3500**.
- Stop the wireshark capture and save the file for further analysis.

Answer the following questions:

1. How many hops are involved in finding the route to this ping-ams1.online.net
2. How many total IP packets are exchanged in the communication to get the final traceroute output of ping-ams1.online.net? How many of them are sent from client to remote machine (server/router) ? How many of them are sent from the remote machine (hop/server/router) to the local client ? Tabulate this with an entry for a router/server and the client too.
3. Which fields in the IP datagram always change from one datagram to the next within this series of IP packets sent by your host/client ? Which fields stay constant? Which of the fields must stay constant? Which fields must change? Why?

In the saved file used for analysis, export only those IP packets involved in either direction (in communication) using appropriate Wireshark display filters and save it to another file to upload during submission.

SUBMISSION INSTRUCTIONS

Prepare a detailed observation and analysis report, and the appropriate screenshots from the wireshark and terminal for listed questions with specific details asked in individual tasks along with respective wireshark trace files (for what is being mentioned only in the IPERF TASK, PING TASK and TRACEROUTE TASK; Please don't upload the entire trace file captured). Submit your report in PDF format with name as <ENTRY NO.>.pdf. Submit your wireshark traces named as <ENTRY NO.>_iperf.pcap, <ENTRY NO.>_ping.pcap and <ENTRY NO.>_traceroute.pcap .

Zip all these files into a single zip file <ENTRY NO.>.zip and submit on moodle.