CS3205 - Introduction to Computer Networks
Even Sem. 2019, Dr. Manikantan Srinivasan
Assignment 1 (Mini): Wireshark - Ping, Nslookup, Traceroute
Individual Assignment
Due date: Jan 28, 2020, 11PM, On Moodle

Extension: 15 % penalty for each 24-hr period; Max. of 48-hrs past the original deadline

Jan 21, 2020

The purpose of this assignment is to 1) Gain familiarity with the use of Wireshark 2) Use of few networking tools/programs commonly used by communication networking engineers - Ping, Nslookup, Traceroute.

1 Tools / Methods

1.1 Wireshark

Wireshark is a versatile packet sniffer that helps a network designer/engineer in many day to day networking activities. The methods to use and work with the wireshark has been demonstrated with a hands-on in the class. You should be quite familiar with enabling wireshark, initiating capture on a specific interface - i.e., Wi-Fi, or Ethernet (RJ45), stop capture, apply a filter, save the captured packets to a file, open a saved file.

1.2 PING

Ping utility helps to understand/determine the reachability to a particular domain name / IP address. PING utility utilizes the ICMP (Internet Control Message Protocol). ICMP is defined in RFC 792. PING utility uses ICMP Echo request and Echo reply messages, reflected by the differing ”Type of message” and ”code” values in the ICMP header. The Ping results indicate the number of routers (hops) that is present between the source and destination, which can be determined from the TTL (Time To Live) value, and the explicit round trip delay (milliseconds) will be available.

1.3 Nslookup

Nslookup utility enables a user to query any specified DNS server/default DNS server for a DNS record. DNS stands for Domain Name Service, the protocol will be discussed in upcoming class. DNS does the mapping of a domain name to a specific IP address. Nslookup sends a DNS query to the specified DNS server/Default server, receives a DNS reply from that same DNS server, and displays the result.

For example by executing ”nslookup www.cse.iitm.ac.in”, one can get the IP address associated with the web server that hosts the IITM CSE department web site.

1.4 traceroute/tracert

tracerouet/tracert tool allows a user to determine the exact path which a packet takes to reach a destination. This is typically achieved with the help of ICMP echo request/reply messages having specfic TTL values, i.e., value increased from 1, 2, .. etc., until the destination is reached. Traceroute utility checks each router (hop) along the path to the destination thrice. One can co-relate the TTL value in a PING response with the Traceroute/Tracert output. i.e, the output of tracert will a) n output items/lines, mapping to the n hops to reach the destination, b) each output line will provide the time it took for each of the packet to reach the hop (router id), along with the router id (i.e., a distinct IP address assigned to a router), or it can be a domain name too.

At times different packets to the same destination can travel via different paths.

1.5 Note

The utilities are implemented slightly differently in the different OSs. i.e. behavior in Windows / Linux / MAC might slightly differ w.r.to the way the output(s) is/are generated.

2 Action items

1. You are to choose atleast Five (5) different (distinct) domains. Please show your creativity i.e., it HAS TO be a domain in India, Asia, Europe, American continent (north/ south), Pacific (Australia/NewZealand). You can choose an university or a well known business organization.
2. For each of the chosen domain perform "Ping <domain name>" such that you capture atleast 10 ping requests. (By default in windows it sends only 3 packets. By default in linux, it continuously sends packets. Ping has an option to specify the number of packets to send and check).
3. For each of the chosen domain perform "nslookup <domain name>". Note down the IP address returned along with the Name of the domain you choose with the IP address. This must be the destination IP address of the ICMP echo requests sent in the Ping check you performed earlier.
4. For each of the chosen domain perform "traceroute/tracert <domain name>". Perform this thrice. Check / observe the IP addresses of the hops/routers via which the packet has traversed. The number of hops must match the TTL value seen in the Ping check you performed earlier.

3 What to Submit

The directory **"Assignment1"** should contain the following files:

1. A brief report as - a Word doc / PDF. The report should serves as a README for the directory, as well as it should contain the following details.
   - Your system's unique IP address and MAC address (wifi interface) using which the data exchange would have been acheived.. (By executing the system command ipconfig in windows, ifconfig in linux, you can obtain the IP address and MAC address associated with your system's interfaces.
   - Command prompt / Terminal output screen shots for each of the command execution. ifconfig/ipconfig, Ping, Nslookup, Traceroute for each of the domains.
   - For each Ping to a domain, your observation, i.e. what did you infer
   - For each Nslookup what did you infer/observed

    - For each trace route what was your observation. Did you notice any interesting results, and if so, give your interpretation.
    - Please note, a well highlighted interpretation gets better credits.

2. Wireshark capture files (after applying filter) for the Ping and Traceroute.

3. Wireshark capture files for the ping response should have minimum of 20 packets, (10 request, and its corresponding replies) - you can apply filter, and save only the filtered packets.

4. Wireshark capture files for the traceroute should have all the packets that form part of the trace route, i.e. 3 icmp echo requests, along with time exceeded error messages for each hop, and final successful result.

5. Name the files intuitively to reflect what it is associated with - i.e. Ping-dn1.pcap, Ping-dn2.pcap, ... trace-dn1.pcap

Submit a tar(zip) file of the directory. Name the tar file as <ROLL Number>CS3205Assignment1.tar(zip)

4 Grading

- Report - with screen captures: 25 points. (5 Pings - 5 points, 5 nslookup - 5 points, 5x3 traceroute - 15 points)
- Wireshark files: 20 points (there will be 10 files) - one for Ping and one of the trace route trial capture. (Sufficient you share one of the trace route capture file)
- Viva Voce: 5 points

5 Help

1. Ask questions EARLY and start your work NOW. Take advantage of the help of the TAs and the instructor.
2. Submissions uploaded to Moodle within the deadline will be graded. No submission via emails.
3. Demonstration of command execution, explanation of behavior to the TAs MUST be done using the files uploaded on Moodle.
4. Execute the commands / perform the study using your individual laptops or distinct workstations in the labs.
5. The wireshark captures will need to be distinct. If two submissions have same source IP / MAC, it will be treated as copy and will receive “Zero” credits.
6. Try to be creative as much as possible.