**Malaviya National Institute of Technology Jaipur**
**Computer Networks**
**Lab Tasks#3**

---

## Problem 1:

Start up your web browser. Then start up the wireshark (i.e. ethereal) packet sniffer and then begin ethereal packet capture. Next, enter into your browser http://www.ezinemart.com .Open one more browser window and open http://*www.mnit.ac.in*. Wait for some time before you stop the capture. Specify filter “dns” in display-filter-specification window, so that only captured DNS messages will be displayed later in the packet-listing window. Find out the answer of following questions by observations:

**i)** Locate the DNS query and response messages. What field indicates whether the message is a query or a response? Are they sent over UDP or TCP?

**ii)** What is the destination port for the DNS query message? What is the source port of DNS response message?

**iii)** To what IP address is the DNS query message sent? Use appropriate command to determine the IP address of your local DNS server. Are these two IP addresses the same?

**iv)** What is the canonical name for www.ezinemart.com and www.mnit.ac.in?

**v)** Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

**vi)** Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?

**vii)** These web pages contain images. Before retrieving each image, does your host issue new DNS queries?

**viii)** Can you identify from the captured packets whether the IP address of mnit.ac.in is taken from local DNS server or some authoritative DNS server(s)? If yes then How?

## Problem 2:

Start up your web browser. Then start up the wireshark (i.e. ethereal) packet sniffer and then begin ethereal packet capture. Next, enter into your browser http://www.ezinemart.com. Open one more browser window and open http://*www.mnit.ac.in*. Wait for some time before you stop the capture. Specify filter “dns” in display-filter-specification window, so that only captured DNS messages will be displayed later in the packet-listing window. Find out the answer of following questions by observations:

Use the same capture as used in ***Problem 1*** above and now specify filter “http” in display-filter-specification window, so that only captured HTTP packets will be displayed later in the packet-listing window. Now answer the following questions:

**a)** What is the server's response (write status code and phrase) in response to the initial HTTP GET message from your browser?

**b)** Can you identify how many connections have been established to get the entire first page of *ww*w.mnit.ac.in ? Which attribute of the http protocol decides it?

**c)** How many HTTP GET request messages were sent by your browser? To which Internet addresses were these GET requests sent?

**d)** Did you find IF-MODIFIED-SINCE line in any of the http GET? If yes then what is the response for that from server side and what does it mean?

**e)** Have you observed any SET-COOKIE header in any of the request and response header? (If not; you try after browsing some E-Commerce websites).

**f)** What kind of server is running over www.ezinemart.com *and ww*w.mnit.ac.in ?

**Problem 3:** This problem is related to the transport layer protocol i.e. TCP. Capture data packets in promiscuous mode by using Ethereal from the URLs (e.g. http://www.bits-pilani.ac.in, http://www.rediff.com, http://www.yahoo.com etc.). Apply appropriate filter to visualize only the TCP segments in your capture. Answer the following questions:

***Note: Capture some decent amount of packets by clicking various links on the index pages of the URLs to observe the results effectively.***

**a)** What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and www.rediff.com? What is it in the segment that identifies the segment as a SYN segment?

**b)** What is the sequence number of the SYNACK segment sent by www.bits-pilani.ac.in to the client computer in reply to the SYN? What is the value of the Acknowledgement field in the SYNACK segment? How did www.bits-pilani.ac.in determine that value? What is it in the segment that identifies the segment as a SYNACK segment?

**c)** The sequence numbers that you observed so far in your trace are the actual sequence numbers? Is it overruling the things which you read in the text? Don't be confused. Are you really wanted to know the actual things? Follow Edit->preferences->protocols->tcp and unmark the Relative Sequence Number and Window Scaling. Now check the sequence numbers in your trace. Did you observe any change? Explain the reason.

**d)** What is the length of each of the first three TCP segments for www.yahoo.com?

**e)** Are there any retransmitted segments in the trace file? What did you check for (in the trace) in order to answer this question?

**Problem 4:** Trace-route is the program that shows you the route over the network between two systems, listing all the intermediate routers. Open the URL www.traceroute.org in your browser. Trace the internet path (route) from ISP server within India to www.google.com. Answer the following after observing the outputs:

Note: Include the trace output in your solutions for reference.

**a)** How many intermediate routers did you find between them? Is this number is always fixed for this source destination combination? Yes/No. Why?
Note: Run the trace for same pair in different times.

**b)** Did you observe any tier-1 ISP router in your trace? If yes, name the ISP.

**c)** In your trace most of the output lines having three time values? What are these values? Some output lines don't have three time values. What does it mean?

**d)** Examine these time values and try to find out at which link the network may congest?