RAMAIAH Institute of Technology

Department of Computer Science & Engineering

QUESTION BANK FOR Fourth Semester (Term: April-July 2024)

Data Communication and Networking Laboratory (CSL47)

Develop the following programs using C/C++/Java/Wireshark/NS3

Exercise Number		Problem Statements
1)	A.	Trace Domain Name Server using packet sniffer and packet analyser.
	B.	Design and simulate a wired network with duplex links between 'n' nodes with CDR over UDP. Set the queue size vary the bandwidth and find the number of packets dropped.
2)	A.	Trace Hypertext Transfer Protocol using packet sniffer and packet analyser.
	B.	Simulate a four node point-to-point network, and connect the links as follows: n0-n2, n1-n2 and n2-n3. Apply TCP agent between n0-n3 and UDP agent between n1-n3. Apply relevant applications over TCP and UDP agents by changing the parameters and determine the number of packets sent by TCP/UDP.
3)	A.	Trace Internet Protocol and Internet Control Message Protocol using packet sniffer and packet analyser.
	B.	Design and simulate simple Extended Service Set with transmitting nodes in wireless LAN and determine the performance with respect to transmission of packets.
4)	A.	Write a program to find the shortest path between vertices using Bellman-Ford algorithm.
	B.	Design and simulate infrastructure less network, generate two traffic flows between nodes and analyse its performance.
5)	A.	Write a program for congestion control using leaky bucket algorithm.
	B.	Design and simulate a wired network with duplex links between 'n' nodes with CDR over UDP. Set the queue size vary the bandwidth and find the number of packets dropped.
6)	A.	Write a client-server program using TCP/IP sockets in which client requests for a file by sending the file name to the server, and the server sends back the contents of the requested file if present.
	B.	Simulate a four node point-to-point network, and connect the links as follows: n0-n2, n1-n2 and n2-n3. Apply TCP agent between n0-n3 and UDP agent between n1-n3. Apply relevant applications over TCP and UDP agents by changing the parameters and determine the number of packets sent by TCP/UDP.
7)	A.	Trace Domain Name Server using packet sniffer and packet analyser.
	B.	Design and simulate simple Extended Service Set with transmitting nodes in wireless LAN and determine the performance with respect to transmission of packets.
8)	A.	Trace Internet Protocol and Internet Control Message Protocol using packet sniffer and packet analyser.

	B.	Design and simulate infrastructure less network, generate two traffic flows between nodes and analyse its performance.
9)	A.	Write a program for congestion control using leaky bucket algorithm.
	B.	Design and simulate simple Extended Service Set with transmitting nodes in wireless LAN and determine the performance with respect to transmission of packets.

10)	A	Trace Hypertext Transfer Protocol using packet sniffer and packet analyser.
	B	Design and simulate infrastructure less network, generate two traffic flows between nodes and analyse its performance.

Note:

- **Student is required to solve one of the above 10-exercise statements. Each exercise problem statement consists of one PART-A and one PART-B problem statement as given above. The questions are allotted based on lots.**
- **Marks Distribution is as follows**

Conduction and Result	**Write-up (8)**	**Execution (35)**	**Viva/ Demo**	**Change of Program**	**Total**
Part-A	4	15	7	-10 Marks	50 Marks
Part-B	4	20			

RAMAIAH Institute of Technology

Department of Computer Science & Engineering

Wireshark Detailed Questions to be answered:

1.	Trace Hypertext Transfer Protocol. (Part A) **The Basic HTTP GET/response interaction** URL: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html a) Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running? b) What languages does your browser indicate that it can accept from the server? c) What is the status code returned from the server to your browser? d) When was the HTML file, that you are retrieving last modified at the server? e) How many bytes of content are being returned to your browser? **The HTTP CONDITIONAL GET/response interaction** URL : http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html f) 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? g) Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell? h) 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? i) 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.
2.	Trace Hypertext Transfer Protocol (Part B) **Retrieving Long Documents** URL: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html a) How many HTTP GET request messages were sent by your browser? b) How many data-containing TCP segments were needed to carry the single HTTP Response? c) What is the status code and phrase associated with the response to the HTTP GET Request? **HTML Documents with Embedded Objects** http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html d) How many HTTP GET request messages were sent by your browser? To which Internet addresses were these GET requests sent? e) Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain. **HTTP Authentication** URL: http://gaia.cs.umass.edu/wireshark-labs/**protected**_pages/HTTP-wireshark-file5.html username: wireshark-students password: network f) What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser? g) When your browser sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

HOD, Dept. of CSE

3.	Trace Packets using Wireshark for DNS and Answer the following Questions URL: http://www.ietf.org a) Locate the DNS query and response messages. Are they sent over UDP or TCP? b) What is the destination port for the DNS query message? What is the source port of DNS response message? c) To what IP address is the DNS query message sent? Determine the IP address of your local DNS server (*Hint: nmcli*). Are these two IP addresses the same? d) Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"? e) Examine the DNS response message. How many "answers" are provided? What does each of these answers contain? f) Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message? g) This web page contains images. Before retrieving each image, does your host issue new DNS queries? **Use *nslookup –type=NS mit.edu*** and answer the following h) To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? i) Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"? j) Examine the DNS response message. What MIT name servers does the response message provide? Does this response message also provide the IP addresses of the MIT name servers?
4.	Trace Internet Protocol and Internet Control Message Protocol using Wireshark. a) Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol part of the packet in the packet details window. What is the IP address ofyour computer? b) Within the IP packet header, what is the value in the upper layer protocol field? c) How many bytes are in the IP header? How many bytes are in the payload *of the IP datagram*? Explain how you determined the number of payload bytes. d) Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented. e) Which fields in the IP datagram *always* change from one datagram to the next within this series of ICMP messages sent by your computer? f) Which fields stay constant? g) Find the first ICMP Echo Request message that was sent by your computer after you changed the *Packet Size* to 2000 (Use command *ping –s 2000 www.msrit.edu* to change the MTU of the packet). Has that message been fragmented across more than one IP datagram h) Write down the first fragment of the fragmented IP datagram. What information in the IP

	header indicates that the datagram been fragmented? What information in the IP header indicates whether this is the first fragment versus a latter fragment? How long is this IP datagram? i) What information in the IP header indicates that this is not the first datagram fragment? Are there more fragments? How can you tell? What fields change in the IP headerbetween the first and second fragment?
5.	Trace Packets using Wireshark for Dynamic Host Configuration Protocol (DHCP) and Answer the following Questions: **Use *dhclient –r* for releasing ip address, *dhclient <eth0>* for renewing ipaddress** Are DHCP messages sent over UDP or TCP? a) What is the link-layer (e.g., Ethernet) address of your host? b) What values in the DHCP discover message differentiate this message from the DHCP request message? c) What is the value of the Transaction-ID in each of the first four discover/Offer/Request/ACK) DHCP messages? What are the values of the Transaction- ID in the second set (Request/ACK) set of DHCP messages? What is the purpose of the Transaction-ID field? d) A host uses DHCP to obtain an IP address, among other things. But a host's IP address is not confirmed until the end of the four-message exchange! If the IP address is not set until the end of the four-message exchange, then what values are used in the IP datagrams in the four-message exchange? For each of the four DHCP messages (Discover/Offer/Request/ACK DHCP), indicate the source and destination IP addresses that are carried in the encapsulating IP datagram. e) What is the IP address of your DHCP server? f) What IP address is the DHCP server offering to your host in the DHCP Offer message? Indicate which DHCP message contains the offered DHCP address. g) In the example screenshot in this assignment, there is no relay agent between the host and the DHCP server. What values in the trace indicate the absence of a relay agent? Is there a relay agent in your experiment? If so what is the IP address of the agent? h) Explain the purpose of the lease time. How long is the lease time in your experiment? i) What is the purpose of the DHCP release message? Does the DHCP server issue an acknowledgment of receipt of the client's DHCP request?