

QUESTION BANK FOR V SEMESTER (Term: Aug-Dec 2020)
Computer Networks Laboratory (CSL58/CSL59)
I.A. Marks : 50
Credits: 0:0:1
Exam Hours: 03
Exam Marks: 50

1.	<p>A. Write a program for error detection using CRC-CCITT (16-bits).</p> <p>B. Trace Packets using Wireshark for DNS and Answer the following Questions URL: http://www.ietf.org</p> <ul style="list-style-type: none"> 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? Use ipconfig to determine the IP address of your local DNS server. 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? <p>Use nslookup -type=NS mit.edu and answer the following</p> <ul style="list-style-type: none"> 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”? <p>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?</p>
2.	<p>A. Write a program to generate Hamming Code for error detection and correction.</p> <p>B. Trace Packets using Wireshark for Dynamic Host Configuration Protocol (DHCP) and Answer the following Questions:</p> <p style="text-align: center;">Use dhclient -r for releasing ip address, dhclient <eth0> for renewing ipaddress</p> <ul style="list-style-type: none"> a) Are DHCP messages sent over UDP or TCP? b) What is the link-layer (e.g., Ethernet) address of your host? c) What values in the DHCP discover message differentiate this message from the DHCP request message?

	<p>d) What is the value of the Transaction-ID in each of the first four discover/Offer/Request/ACK) DHCP messages? What is the purpose of the Transaction-ID field?</p> <p>e) 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.</p> <p>f) What is the IP address of your DHCP server?</p> <p>g) 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.</p> <p>h) 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?</p> <p>i) Explain the purpose of the lease time. How long is the lease time in your experiment?</p> <p>j) What is the purpose of the DHCP release message? Does the DHCP server issue an acknowledgment of receipt of the client's DHCP request?</p>
3.	<p>A. Simulate a three nodes point-to-point network with duplex links between them using NS3. Set the queue size vary the bandwidth and find the number of packets dropped.</p> <p>B. Trace Hypertext Transfer Protocol.</p> <p>The Basic HTTP GET/response interaction URL: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html</p> <p>a) Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?</p> <p>b) What languages does your browser indicate that it can accept from the server?</p> <p>c) What is the status code returned from the server to your browser?</p> <p>d) When was the HTML file, that you are retrieving last modified at the server?</p> <p>e) How many bytes of content are being returned to your browser?</p> <p>The HTTP CONDITIONAL GET/response interaction URL : http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html</p> <p>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?</p> <p>b. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?</p> <p>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?</p> <p>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.</p>
4.	<p>A. Write a program to implement traffic policing using Leaky bucket algorithm.</p> <p>B. Trace Hypertext Transfer Protocol</p> <p>Retrieving Long Documents URL: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html</p> <p>a. How many HTTP GET request messages were sent by your browser?</p> <p>b. How many data-containing TCP segments were needed to carry the single HTTP Response?</p> <p>c. What is the status code and phrase associated with the response to the HTTP GET</p>

	<p>Request?</p> <p>HTML Documents with Embedded Objects</p> <p>URL: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html</p> <ol style="list-style-type: none"> How many HTTP GET request messages were sent by your browser? To which Internet addresses were these GET requests sent? Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain. <p>HTTP Authentication</p> <p>URL: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html</p> <p>username: wireshark-students</p> <p>password: network</p> <ol style="list-style-type: none"> What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser? When your browser sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?
5.	<p>A. Simulate using NS3 a transmission of ping message over a network topology consisting of 6 nodes and find the number of packets dropped due to congestion.</p> <p>B. Trace Packets using Wireshark for DNS and Answer the following Questions</p> <p>URL: http://www.ietf.org</p> <ol style="list-style-type: none"> Locate the DNS query and response messages. Are they sent over UDP or TCP? What is the destination port for the DNS query message? What is the source port of DNS response message? To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same? Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"? Examine the DNS response message. How many "answers" are provided? What does each of these answers contain? 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? This web page contains images. Before retrieving each image, does your host issue new DNS queries? <p>Use nslookup -type=NS mit.edu and answer the following</p> <ol style="list-style-type: none"> To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"? 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?
6.	<p>A. Write a program for error detection using CRC-CCITT (16-bits).</p> <p>B. Trace Packets using Wireshark for Dynamic Host Configuration Protocol (DHCP) and Answer the following Questions:</p>

	<p>Use <code>dhclient -r</code> for releasing ip address, <code>dhclient <eth0></code> for renewing ipaddress</p> <p>Are DHCP messages sent over UDP or TCP?</p> <ol style="list-style-type: none"> What is the link-layer (e.g., Ethernet) address of your host? What values in the DHCP discover message differentiate this message from the DHCP request message? What is the value of the Transaction-ID in each of the first four discover/Offer/Request/ACK) DHCP messages? What is the purpose of the Transaction-ID field? 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. What is the IP address of your DHCP server? 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. 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? Explain the purpose of the lease time. How long is the lease time in your experiment? What is the purpose of the DHCP release message? Does the DHCP server issue an acknowledgment of receipt of the client's DHCP request?
7.	<p>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.</p> <p>B. Trace Internet Protocol and Internet Control Message Protocol using Wireshark.</p> <ol style="list-style-type: none"> 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 of your computer? Within the IP packet header, what is the value in the upper layer protocol field? 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. Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented. Which fields in the IP datagram always change from one datagram to the next within this series of ICMP messages sent by your computer? Which fields stay constant? Find the first ICMP Echo Request message that was sent by your computer after you changed the Packet Size to 2000 (Use command <code>ping -s 2000 www.msrit.edu</code> to change the MTU of the packet). Has that message been fragmented across more than one IP datagram? 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? 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 header between the first and second fragment?

8.	<p>A. Write a program to implement traffic policing using Leaky bucket algorithm.</p> <p>B. Trace FTP using Wireshark. URL: ftp://ftp.cdc.gov</p> <ol style="list-style-type: none"> Identify the protocol that is used by transport layer for establishing FTP connection. What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and ftp.cdc.gov? What is the sequence number of the TCP SYN ACK segment that is used to initiate the TCP connection between the ftp.cdc.gov and client computer? List the values of all the fields in TCP ACK segment. Identify the FTP commands and response codes during the FTP session. What is the username and password used to access FTP server? Type this in filter “tcp and ip.addr==198.246.117.106” (hint: nslookup ftp.cdc.gov) and Identify the flags that are set to 1 on successful login. Identify the phrase and code of the Retrieve and command response.
9.	<p>A. Simulate simple Extended Service Set with transmitting nodes in wireless LAN using NS3 and determine the performance with respect to transmission of packets.</p> <p>B. Trace Internet Protocol and Internet Control Message Protocol using Wireshark.</p> <ol style="list-style-type: none"> 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 of your computer? Within the IP packet header, what is the value in the upper layer protocol field? How many bytes are in the IP header? How many bytes are in the payload of <i>the IP datagram</i>? Explain how you determined the number of payload bytes. Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented. Which fields in the IP datagram <i>always</i> change from one datagram to the next within this series of ICMP messages sent by your computer? Which fields stay constant? Find the first ICMP Echo Request message that was sent by your computer after you changed the <i>Packet Size</i> 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 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? 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 header between the first and second fragment?
10.	<p>A. Write a program to generate Hamming Code for error detection and correction.</p> <p>B Trace Hypertext Transfer Protocol. The Basic HTTP GET/response interaction URL: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html</p>

	<p>f) Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?</p> <p>g) What languages does your browser indicate that it can accept from the server?</p> <p>h) What is the status code returned from the server to your browser?</p> <p>i) When was the HTML file, that you are retrieving last modified at the server?</p> <p>j) How many bytes of content are being returned to your browser?</p> <p>The HTTP CONDITIONAL GET/response interaction</p> <p>URL : http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html</p> <p>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?</p> <p>b) Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?</p> <p>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?</p> <p>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.</p>
11.	<p>A. Write a program to generate Hamming Code for error detection and correction.</p> <p>B. A. Trace FTP using Wireshark. URL: ftp://ftp.cdc.gov</p> <p>a) Identify the protocol that is used by transport layer for establishing FTP connection.</p> <p>b) What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and ftp.cdc.gov?</p> <p>c) What is the sequence number of the TCP SYN ACK segment that is used to initiate the TCP connection between the ftp.cdc.gov and client computer?</p> <p>d) List the values of all the fields in TCP ACK segment.</p> <p>e) Identify the FTP commands and response codes during the FTP session.</p> <p>f) What is the username and password used to access FTP server?</p> <p>g) Type this in filter “tcp and ip.addr==198.246.117.106” (hint: nslookup ftp.cdc.gov) and Identify the flags that are set to 1 on successful login.</p> <p>h) Identify the phrase and code of the Retrieve command and response.</p>
12.	<p>A. Write a program to implement traffic policing using Leaky bucket algorithm</p> <p>B. Trace Hypertext Transfer Protocol</p> <p>Retrieving Long Documents</p> <p>URL: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html</p> <p>a) How many HTTP GET request messages were sent by your browser?</p> <p>b) How many data-containing TCP segments were needed to carry the single HTTP Response ?</p> <p>c) What is the status code and phrase associated with the response to the HTTP GET Request ?</p> <p>HTML Documents with Embedded Objects</p> <p>URL: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html</p> <p>a) How many HTTP GET request messages were sent by your browser? To which Internet addresses were these GET requests sent?</p> <p>b) Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.</p>

	HTTP Authentication URL: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html username: wireshark-students password: network a) What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser? b) When your browser sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?
--	---

Note:

Conduction and Result (both (a) & (b)	: 35 Marks (a: 15 Marks, b: 20 Marks)
Write-up	: 7 Marks
Viva	: 8 Marks
COP	: -5 Marks