School of Electrical and Electronic of Enginnering
eee 4474-01 : Experiments on Communication Networks
2조 2016142096 **조윤신**, 2017142043 **김재민**

Result Report Week 2

wireshark(2) : TCP UDP IP protocols

1 Experiment 1 : TCP

1.a A first look at the captured trace

Problems

Problem 1: What is the IP address and TCP port number used by the client computer (source) that is transferring the file to gaia.cs.umass.edu? To answer this question, it's probably easiest to select an HTTP message and explore the details of the TCP packet used to carry this HTTP message, using the "details of the selected packet header window"
Answer

Problem 2: What is the IP address of gaia.cs.umass.edu? On what port number is it sending and receiving TCP segments for this connection?
Answer

1.b TCP Basics

Problems

Problem 3: What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu? What is it in the segment that identifies the segment as a SYN segment?
Answer

Problem 4: What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN? What is the value of the Acknowledgement field in the SYNACK segment? How did gaia.cs.umass.edu determine that value? What is it in the segment that identifies the segment as a SYNACK segment?
Answer

Problem 5: What is the sequence number of the TCP segment containing the HTTP POST command? Note that in order to find the POST command, you'll need to dig into the packet content field at the bottom of the Wireshark window, looking for a segment with a "POST" within its DATA field.
Answer

Problem 6: Consider the TCP segment containing the HTTP POST as the first segment in the TCP connection. What are the sequence numbers of the first six segments in the TCP connection (including the segment containing the HTTP POST)? At what time was each segment sent? When was the ACK for each segment received? Given the difference between when each TCP segment was sent, and when its acknowledgement was received, what is the RTT value for each of the six segments?
What is the EstimatedRTT value after the receipt of each ACK?
Assume that the value of the EstimatedRTT is equal to the measured RTT for the first segment, and then is computed using the EstimatedRTT equation below for all subsequent segments.

$$\text{Estimated RTT} = 0.875 \times \text{Estimated RTT} + 0.125 \times \text{Sample RTT}$$

Answer

Problem 7: What is the length of each of the first six TCP segments?
Answer

Problem 8: What is the minimum amount of available buffer space advertised at the received for the entire trace? Does the lack of receiver buffer space ever throttle the sender?
Answer

Problem 9: Are there any retransmitted segments in the trace file? What did you check for (in the trace) in order to answer this question?
Answer

Problem 10: How much data does the receiver typically acknowledge in an ACK? Can you identify cases where the receiver is ACKing every other received segment.
Answer

Problem 11: What is the throughput for the TCP connection? Explain how you calculated this value.
Answer

1.c TCP congestion control in action

Problems

Problem 12: Use the Time-Sequence-Graph(Stevens) plotting tool to view the sequence number versus time plot of segments being sent from the client to the gaia.cs.umass.edu server. Can you identify where TCP's slow-start phase begins and ends, and where congestion avoidance takes over? Comment on ways in which the measured data differs from the idealized behavior of TCP that we've studied in the text.
Answer

2 Experiment 2: UDP

Problems

Problem 1: Select one UDP packet from you r trace . From this packet, determine how many fields there are in the UDP header.
Answer

Problem 2: By consulting the displayed information in Wireshark's this packet packet content field for ,determine the length (in bytes) of each of the UDP header fields.
Answer

Problem 3: The value in the Length field is the length of what? this answer
Answer

Problem 4: What is the maximum number of bytes that c
Answer

Problem 5: What is the largest possible source port number?
Answer

Problem 6: What is the protocol number for UDP? Give your answer in both hex decimal notation. To answer this question, you'll need to loo adecimal and k into the field of the IP datagram containing this UDP segment.
Answer

3 Experiment 3 : IP

3.a Capturing packets from an execution of traceroute

Problems

Problem 1: 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?
Answer

Problem 2: Within the IP packet header, what is the value in the upper layer protocol field?
Answer

Problem 3: How many bytes are in the IP header?
Answer

Problem 4: How many bytes are in the payload of the IP datagram? Explain how you determined the number of payload bytes.
Answer

Problem 5: Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.
Answer

3.b Basic IPv4

Problem 6: Which fields in the IP datagram always change from one datagram to the next within this series of UDP segments sent by your computer destined to 128.119.245.12, via traceroute? Why?
Answer

Problem 7: Which fields in this sequence of IP datagrams (containing UDP segments) stay constant? Why?
Answer

Problem 8: Describe the pattern you see in the values in the Identification field of the IP datagrams being sent by your computer.
Answer

3.c Fragmentation

Problems

Problem 9: Find the first IP datagram containing the first part of the segment sent to 128.119.245.12 sent by your computer via the traceroute command to gaia.cs.umass.edu, after you specified that the traceroute packet length should be 3000. Has that segment been fragmented across more than one IP datagram?
Answer

Problem 10: What information in the IP header indicates that this datagram been fragmented?
Answer

Problem 11: What information in the IP header for this packet indicates whether this is the first fragment versus a latter fragment?
Answer

Problem 12: How many bytes are there in is this IP datagram (header plus payload)?
Answer

Problem 13: Now inspect the datagram containing the second fragment of the fragmented UDP segment. What information in the IP header indicates that this is not the first datagram fragment?
Answer

Problem 14: What fields change in the IP header between the first and second fragment?
Answer