ECSE 308:
Introduction to
Communication Systems and Networks

L5: TCP & UDP

Part 1: TCP
Part 2: UDP

CEAB Data – Engineering tools

- The following engineering tools are used in this laboratory:
  - Wireshark network analyser
  - TCP protocol
  - UDP protocol
  - DNS

Part 1: TCP

Objectives: Use Wireshark to collect TCP traces and investigate the TCP protocol functions:

- TCP connection establishment phase
- TCP flow control
- TCP termination phase

Transmission Control Protocol (TCP): Overview

- TCP is a connection-oriented protocol meaning that it establishes an end-to-end connection before any data is sent.
- Typically, TCP connections go through three phases: connection establishment, data transfer and termination. These phases in TCP segments are identified by flags.
- TCP uses an end-to-end flow control protocol to avoid having the sender send data too fast for the TCP receiver to receive and process it reliably.
- It applies a sliding window flow control protocol. In each TCP segment, the receiver specifies in the receive window field the amount of additionally received data (in bytes) that it is willing to buffer for the connection. The sending host can send only up to that amount of data before it must wait for an acknowledgment and window update from the receiving host.

TCP & congestion control: Overview

- TCP applies congestion control mechanisms which control the rate of data entering the network, keeping the data flow below a rate that would trigger collapse.
- For each connection, TCP maintains a congestion window, limiting the total number of unacknowledged packets that may be in transit end-to-end.
- This is somewhat analogous to TCP's sliding window used for flow control.
- TCP uses a mechanism called slow start to increase the congestion window after a connection is initialized or after a timeout.
- It starts with a window of two times the maximum segment size (MSS) Although the initial rate is low, the rate of increase is very rapid; for every packet acknowledged, the congestion window increases by 1 MSS so that the congestion window effectively doubles for every round-trip time (RTT).

TCP: Instruction

- Find the IP address of www.httpforever.com
- Start up your web browser and clear the browser's cache memory.
- Open up the Wireshark and start packet capture.
- Go to the "http://www.httpforever.com"
- Stop Wireshark packet capture.
- In the filter filed, type "tcp" to see only the TCP packets. Press Apply.

Questions - TCP connection establishment phase

1. How many TCP datagrams are exchanged between your computer and the server to establish the TCP connection? Why each of these segments is needed to setup the TCP connection?

- You may need to include the IP address of “http://open-up.eu ” (or any other “HTTP” website, note that HTTPS websites are not shown in wireshark as HTTP)in your filtering (use & to filter for multiple filters: “ip.addr == xxx.xxx.xxx.xxx && tcp”)

2. Which end point started the TCP Connection-Establishment phase?
3. What flags are set in each of these TCP datagrams?
4. What is the initial value of the sequence number on the client’s side?
5. What is the initial value of the sequence number on the server’s side?
6. What is the value of the Acknowledgement field in the SYN ACK datagram? How did the server determine that value?
7. For the TCP SYN datagram, determine the following
   - the source port number
   - the destination port number
   - the size of the window
   - the header length
8. For the TCP SYN ACK datagram, determine the following
   - the source port number
   - the destination port number
   - the size of the window
   - the header length

Questions - TCP Flow Control

9. What is the usage of the window field in the TCP segments?
10. Consider the TCP segment containing the HTTP GET as the first segment in the TCP connection. For the first three TCP segments, answer the following questions:
    - When was each segment sent?
    - At what time 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 three segments?
    - What is the Estimated RTT value after the receipt of each ACK?

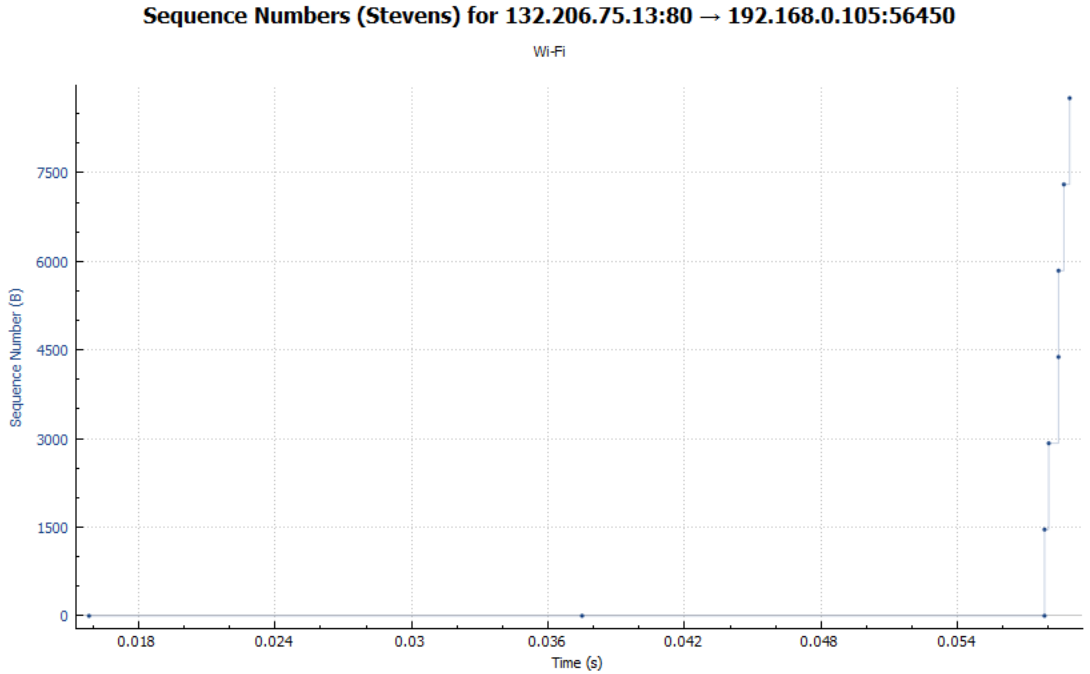
    - Note: Wireshark has a nice feature that allows you to plot the RTT for each of the TCP segments sent. Select a TCP segment in the "listing of captured packets" window that is being sent from the client to the server. Then select: Statistics->TCP Stream Graph>Round Trip Time Graph.
        - What is the length of each of the first three TCP segments?
11. Are the client's port number and the server's port number the same in the entire trace? What is the usage of the port number?
12. 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?

Questions - TCP Termination Phase

13. Are there any retransmitted segments in the trace file? What did you check for (in the trace) in order to answer this question?
14. How much data does the receiver typically acknowledge in an ACK? Can you identify cases where the receiver is ACKing every other received segment.
15. Calculate the throughput (bytes transferred per unit time) for the TCP connection? Explain how you obtained this value.
16. How many TCP datagrams are exchanged for the termination phase?
17. Which end point started the Connection Termination phase?
18. What flags are set in each of segments used for connection termination?

TCP congestion controlTCP congestion control

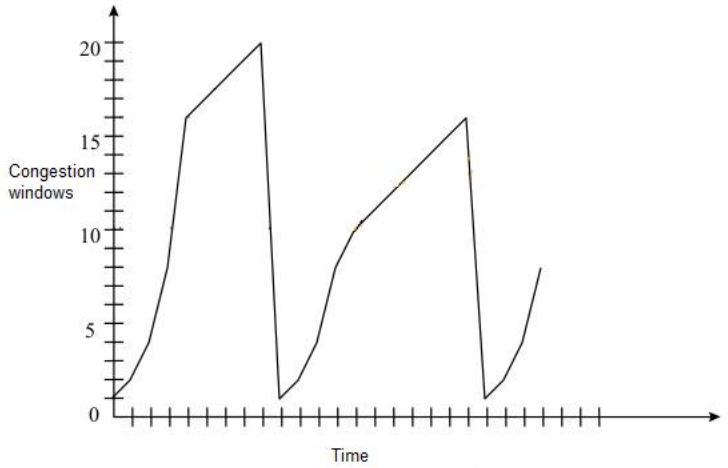
- Select a TCP segment in the Wireshark's "listing of captured-packets" window.
- Select the menu : Statistics->TCP Stream Graph-> Time-SequenceGraph(Stevens).



Questions - TCP Congestion Control

19. 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 server. Can you identify where TCP's slow start phase begins and ends, and where congestion avoidance takes over? Explain your answer.

20. Locate the different phases of the congestion control mechanism on the below graph. Also describe the congestion control algorithm.

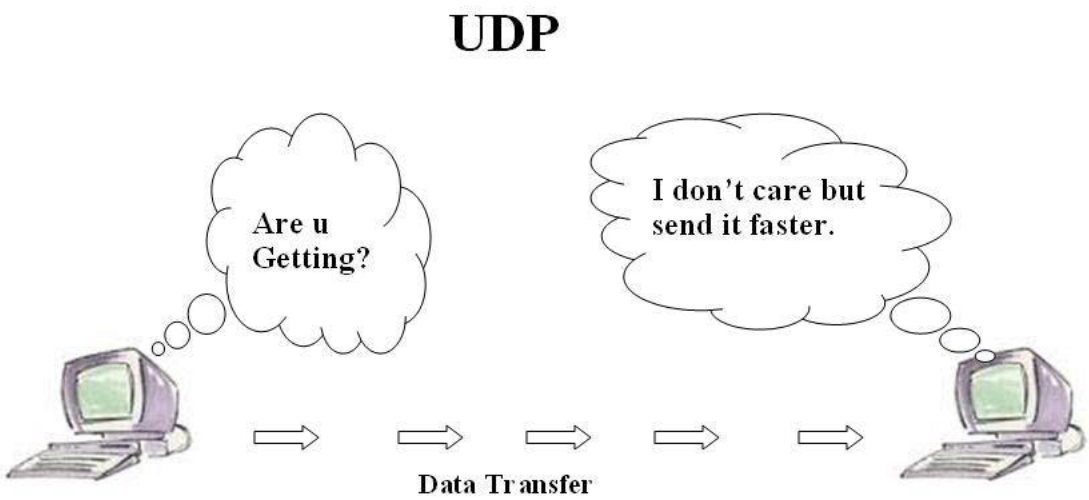


Part 2: User Datagram Protocol (UDP)

Objectives: Use Wireshark to investigate the UDP structure and protocol properties.

UDP

- Use In this experiment, we will focus on the UDP, which is one of the transport level protocol of the TCP/IP model. UDP is a connection-less protocol meaning that no connection-establishment and connection-terminations are used in this protocol. To analyze UDP headers, we need to run an application that uses the UDP service. A good candidate is DNS.



UDP/DNS: Instructions

- Use “ipconfig /flushdns” command in windows terminal to clear the DNS cache in your host.
- If you are using mac or linux look for the right command to clear the DNS chache
- Open your browser and clear your browser cache.
- Use ipconfig to obtain your IP address.
- Open up the Wireshark and enter “ip.addr == your_IP_address” into the filter. This filter removes all packets that neither originate nor are destined to your host.
- Open up the Wireshark and start packet capture.
- With your browser, visit the Web page: http://ieeexplore.ieee.org/
- Stop packet capture.

UDP/DNS: Questions (1/2)

1. What transport layer protocol is used to transfer the DNS query and the response message?
2. To setup the connection, how many UDP datagrams are exchanged between your computer and the server? Explain your answer.
3. Select the first DNS packet in your trace. From this packet, determine the header fields of UDP.
4. By consulting the displayed information in Wireshark's packet content field for the first DNS message, determine the length (in bytes) of each of the UDP header fields.
5. The value in the Length field indicates the length of what? Verify your claim with your captured UDP packet.
6. What is the maximum number of bytes that can be included in a UDP payload? (Hint: the answer to this question can be determined by your previous answer)
7. What is the largest possible source port number?

UDP/DNS: Questions (2/2)

8. Determine whether a checksum is provided for the first DNS message or not. What is the usage of this field?
9. Determine the destination port number for the DNS query message and the source port number of the DNS response. What is the relationship between the two? Which port number is a well-known port number?
10. List two other well-known port numbers used by UDP.
11. Determine the IP address of your local DNS server (use ipconfig). Is it the same as destination IP address of the DNS query?
12. Examine the DNS response message. How many “answers” are provided in this message? What do each of these answers contain?
13. By checking the trace, determine whether UDP is a reliable protocol or not. Explain your answer.
14. Why does DNS use UDP services?