ECSE 308:
Introduction to
Communication Systems and Networks

L4N1: IP & TCP

Part 1: Internet Protocol (IP)

Part 2: 802.11 frames

Part 3: TCP

L4N1: IP & TCP

Part 1: Internet Protocol (IP)

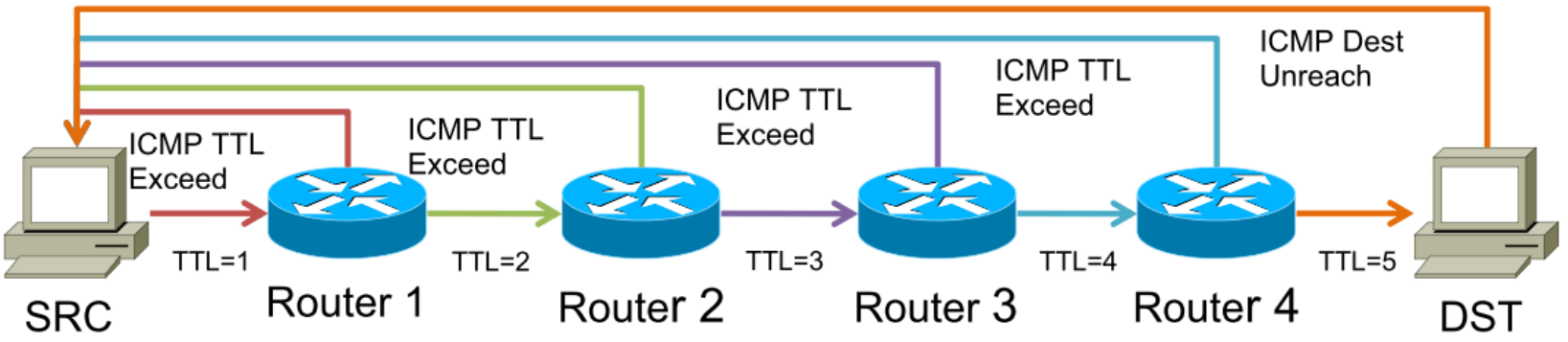
Objectives: Use of the tracert utility to trace the routing path of Internet Protocol (IP) packets sent from your computer to the destination.

Internet Protocol (IP): Overview

- The Internet Protocol (IP), is used to route packets from source to destination based on logical (IP) addresses.
- One of the tools that can be used to get better understanding of how this protocol works is *tracert*.

Tracert

- The *tracert* utility in Windows is a client-server program that sends ICMP echo messages encapsulated in IP packets with TTL values 1,2,3, and so on.
- When a router receives one of these packets, it decrements the value of TTL field by one and if this value reaches zeros, it transmits an ICMP message (type 11 – TTL-exceeded) to the sending host.
- Thus, the packet with TTL i leads the router on i hop away from the host to transmit an ICMP message back to the sender.
- As a result, by receiving these ICMP messages, the tracert learns the identities of the routers between the host and the destination.
- The *tracert* procedure is shown in the following figure (from http://www.keyboardbanger.com/understanding-the-traceroute-command/)



IP *tracert*: Instructions

- Open up the Wireshark.
- Start Packet Capture.
- Run Command Prompt and type:

  tracert –d www.acm.org

  The –d option prevents *tracert* from resolving the IP addresses to their names.
- Go back to the Wireshark and stop packet capture.
- In the filter field, type *icmp* and click apply.

IP *tracert*: Questions

1. How many ICMP packets are in the list plane?
2. How many probe packets are sent from the source to the destination for each TTL?
3. The last few echo-request ICMP packets are followed by the echo-reply ICMP packets. Compare one of them with the corresponding reply. Determine which fields are similar and which fields are different? Explain the reason.
4. What are the TTL values for these last few packets? Determine the number of routers between the source and destination based on these TTL values.
5. Examine the IP packet header of the last echo-request ICMP packet, what is the value in the "Protocol" field? What does this field indicate?
6. How many bytes are in this IP header? How many bytes are in the payload of this IP packet? Explain how you determined the number of payload bytes.
7. Has this IP packet been fragmented? Explain how you determined whether or not the packet has been fragmented.
8. How the IP address of www.acm.org can be found? Determine the packet and the filed in the packet that contains this information.

L4N1: IP & TCP

Part 2: 802.11 frames

Objectives: To investigate 802.11 frames:

- Information in beacon,
- frames used for association and disassociation.

802.11 frames

- In the second part of this lab, we will focus on 802.11 networks, which use different types of frames:
  - Beacon frames, transmitted by the APs to advertise their existence.
  - Furthermore, in these networks, a host must first associate with an access point before sending data. Association in 802.11 is performed using the ASSOCIATE REQUEST frame (sent from host to AP, with a frame type 0 and subtype 0) and the ASSOCIATE RESPONSE frame (sent by the AP to a host with a frame type 0 and subtype of 1, in response to a received ASSOCIATE REQUEST).
- Since 802.11 is a wireless link-layer protocol, we will be capturing frames "in the air." Unfortunately, many device drivers for wireless 802.11 NICs don't provide the hooks to capture/copy received 802.11 frames for use in Wireshark. Thus, in this lab, we will provide a trace of captured 802.11 frames for you to analyze.

802.11: Instructions

- Start your web browser and go this address:
- http://www.info308a.ece.mcgill.ca/wpa-Induction.pcap, download the file on your computer.
- Open up the Wireshark.
- Open the trace file that you just download.

Questions - Beacon Frames

9. What is the SSID of the access point that is issuing the beacon frame?
10. What are the time intervals between transmissions of beacon frames? Does the beacon frame contain this information?
11. What is the source MAC address in the beacon frame?
12. What is the destination MAC address in the beacon frame? What does this address mean?
13. How many data rates can the access point support?
14. Examine the beacon frame, what frequency does the advertised network use?

Questions - Association

15. By looking at the list plane, indicate what type of packets have the smallest size? What type has the largest size?
16. Before sending data to Apple_82:36:3a, what frames are exchanged between this device and the access point?
17. Examine the Authentication frame sent by Apple_82:36:3a, does the host want the authentication to require a key or be open?
18. Examine the response Authentication frame sent by the AP to Apple_82:36:3a. What is the Association ID for this host? What is the usage of this ID?
19. What transmission rates is the host willing to use? The AP? To answer this question, you will need to look into the parameters fields of the 802.11 wireless LAN management frame.
20. Examine the Disassociation frame sent by Apple_82:36:3a to the AP. What is the reason that this user sent Disassociation frame?

L4N1: IP & TCP

Part 3: TCP

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

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

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

- 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.info308a.ece.mcgill.ca/Lab1Ex2.html.
- Stop Wireshark packet capture.
- In the filter filed, type "tcp" to see only the TCP packets. Press Apply.

Questions - TCP connection establishment phase

21. 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?
22. Which end point started the TCP Connection-Establishment phase?
23. What flags are set in each of these TCP datagrams?
24. What is the initial value of the sequence number on the client's side?
25. What is the initial value of the sequence number on the server's side?
26. What is the value of the Acknowledgement field in the SYN ACK datagram? How did the server determine that value?
27. For the TCP SYN datagram, determine the following
    a. the source port number
    b. the destination port number
    c. the size of the window
    d. the header length
28. For the TCP SYN ACK datagram, determine the following
    a. the source port number
    b. the destination port number
    c. the size of the window
    d. the header length

Questions - TCP Flow Control

29. What is the usage of the window field in the TCP segments?
30. 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:
    a. When was each segment sent?
    b. At what time was the ACK for each segment received?
    c. 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?
    d. 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.

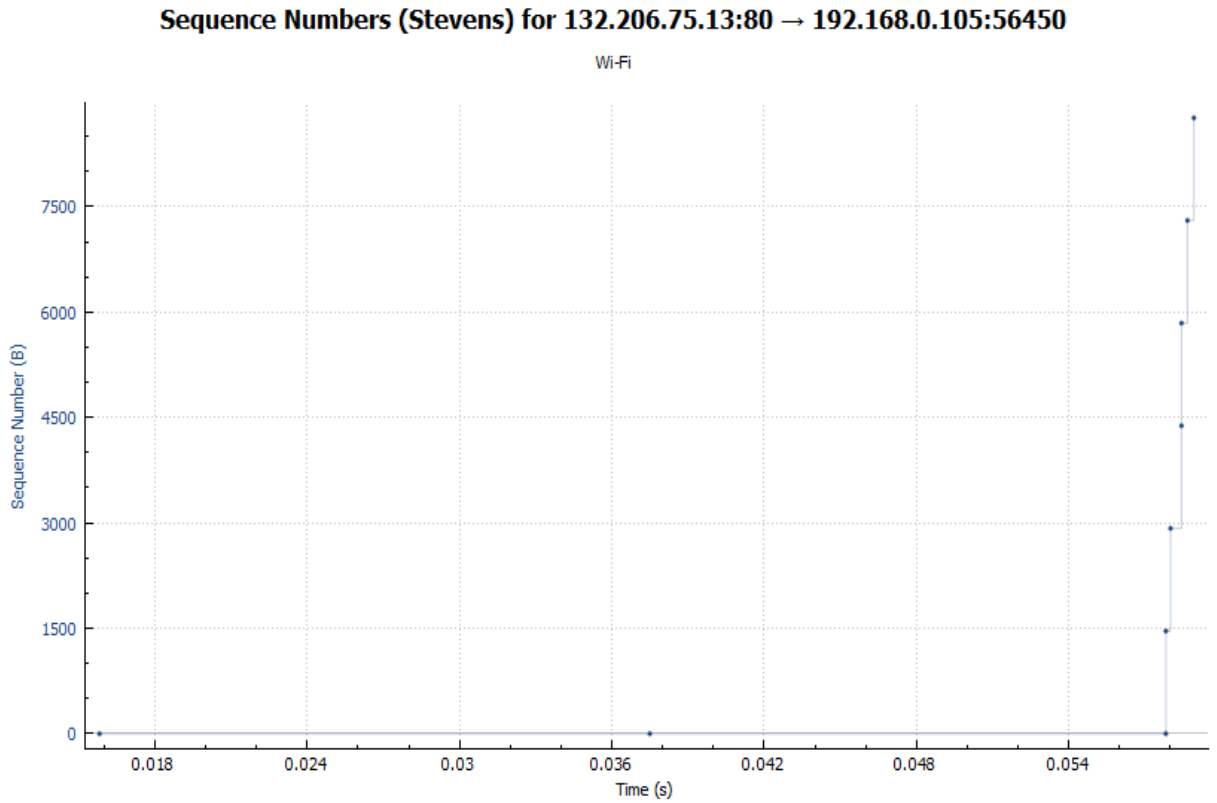
    e. What is the length of each of the first three TCP segments?
31. Are the client's port number and the server's port number the same in the entire trace? What is the usage of the port number?
32. What is the minimum amount of available buffer space advertised at the received for the entire trace? Does the lack of receiver buffer space ever throttle the sender?
33. Are there any retransmitted segments in the trace file? What did you check for (in the trace) in order to answer this question?
34. How much data does the receiver typically acknowledge in an ACK? Can you identify cases where the receiver is ACKing every other received segment.
35. Calculate the throughput (bytes transferred per unit time) for the TCP connection? Explain how you obtained this value.

Questions - TCP Termination Phase

36. How many TCP datagrams are exchanged for the termination phase?
37. Which end point started the Connection Termination phase?
38. What flags are set in each of segments used for connection termination?

TCP 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

39. 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.
40. Locate the different phases of the congestion control mechanism on the below graph. Also describe the congestion control algorithm.