Exercise 1: Web Browsing (DNS, TCP, HTTP)

Objective

In this exercise we analyze the layered structure of network protocols using a web browsing example. We examine the header structure of the PDUs at the Data Link, IP, Transport, and Application layers. In particular we observe how addresses and port numbers work together to enable end-to-end applications.

Protocols Examined

- Ethernet and IP addressing
- DNS Query and Response
- TCP three-way handshake, sequence and ACK numbering
- HTTP GET and Response messages

Background Material

Refere correspondig chaper of your Textbook

Prerequisite

The student knows how to capture packets using Ethereal.

See Ethereal Lab Exercises for more information.

Procedure

1. Start Ethereal..
2. Start a web browser and enter the URL of a website of your choice but do *not* press ENTER.
3. Start Ethereal packet capture.
4. Access the website by pressing ENTER in the browser web page.
5. Once page is loaded, stop capture. Save the capture file.
6. Save the displayed web page for later reference.

Protocol Analysis Questions

To answer the following questions, start Ethereal and open the packet capture file created above.

1. Protocols Captured

- Examine the protocol column in the top pane of the Ethereal window. Confirm that you have captured DNS, TCP, and HTTP packets.

2. Ethernet frame, IP packet, and UDP datagram

- Examine the frame for the first DNS packet sent by the client.
  a. Identify the Ethernet and IP address of the client.
  b. What is the content of the type field in the Ethernet frame?
  c. What are the destination Ethernet and IP addresses and to which machines do these addresses correspond? Explain how this depends on how your machine is connected to the Internet.
- Examine the IP header for the first DNS packet sent by the client.
  a. What is the header length? What is the total packet length?

b. Identify the protocol type field. What is the number and type of the protocol in the payload?

- Examine the UDP header of the first DNS packet sent by the client.
  a. Identify the client ephemeral port number and the server well-known port number. What type of application layer protocol is in the payload?
  b. Confirm that the length field in the UDP header is consistent with the IP header length information.
- Sketch the protocol stack from the data link layer up to the application layer at the client and server sides and explain how the contents in the various PDUs enable end-to-end communication between application layer processes.

3. ***DNS***

- Examine the DNS query message in the DNS packet sent by the client.
  a. What field indicates whether the message is a query or a response?
  b. What information is carried in the body of the query?
  c. What is the query transaction ID?
  d. Identify the fields that carry the type and class of the query.
- Now consider the packet that carries the DNS response to the above query.
  a. What should the Ethernet and IP addresses for this packet be? Verify that these addresses are as expected.
  b. What is the size of the IP packet and UDP datagram that carry the response? Is it longer than the query?
  c. Confirm that the transaction ID in the response message is correct.
  d. How many answers are provided in the response message? Compare the answers and their time-to-live values.

4. TCP three-way handshake

- Identify the frame that carries the first TCP segment in the three-way handshake that sets up the connection between the http client and server.
  a. What source Ethernet and IP addresses do you expect in this segment? What protocol and type fields do you expect in the first segment? Confirm that these addresses are as expected.
  b. Explain the values in the destination Ethernet and IP addresses in the first segment? To what machine(s) do these addresses correspond?
  c. Identify the ephemeral port number used by the client and confirm that the well-known port number is the correct value for HTTP.
  d. What is the length of the TCP segment?
  e. What is the initial sequence number for the segments from the client to the server? What is the initial window size? What is the maximum segment size?
  f. Find the hex character that contains the SYN flag bit.
- Identify the frame that carries the second segment in the three-way handshake.
  a. How much time elapsed between the capture of the first and second segments?
  b. Before examining the captured packets, specify the values for the following fields in this frame:
     - Source and destination addresses and type field in Ethernet frame.
     - Source and destination IP addresses and port numbers in IP packet.

- Acknowledgement number in TCP segment.
- Values of flag bits.
- Confirm that the frame contains the expected values.

c. What is the length of the TCP segment?

d. What is the initial sequence number for the connection from the server to the client? What is the maximum segment size?

- Identify the frame that carries the last segment in the three-way handshake.
  a. How much time elapsed between the capture of the second and last segment? Compare to the elapsed time between the first and second segments and explain the difference.
  b. Specify the following values in the TCP segment:
     - Acknowledgement and sequence numbers.
     - Flag bits and window size.
     - Confirm that the segment contains the expected values
  c. What is the length of the third TCP segment?

5. HTTP GET

- Identify the frame that carries the HTTP "GET" message.
  a. Confirm that the sequence and acknowledgement values in the TCP header are as expected.
  b. Examine the flag bits in the TCP header. Can you explain why the two flag bits are set?
  c. What are the lengths of the TCP segment and payload?
- Now consider the contents of the "GET" message.
  a. Scroll down the third pane in the Ethereal window and compare the decoded text with the contents of the HTTP message in the second window.
  b. Count the number of octets in the message and verify that this number is consistent with the length information in the TCP header.
  c. What is the next sequence number that is expected in the next segment from the server?

6. HTTP Response

- How much time elapses between the capture of the GET message and the capture of the corresponding Response message?
- Determine whether the server responds with an HTTP response message or simply with a TCP ACK segment. Verify that the sequence number in the segment from the server is as expected.
- Now consider the segment that contains the HTTP response message.
  a. What is the length of the payload in the TCP segment?
  b. Examine whether any of the flags are set and explain why they are set.
  c. What acknowledgement number is expected in the next segment from the client?
- Now consider the HTTP response message.
  a. What is the result code in the response message?

b. Highlight the “data” section of the HTTP response message. Scroll down the third pane in the Ethereal window and compare the decoded text with the contents of the web page that was displayed on your screen.