【2021 Advanced Computer Networks Homework 1】

Rules

1. 依題目要求回答問題，並且截圖 (print screen) 說明答案，繳交電子檔。

2. 請將作業輸出成 PDF，並命名為 TCPIP_HW1.pdf，上傳至中山網路大學 http://cu.nsysu.edu.tw/
3. TAs email: net_ta@net.nsysu.edu.tw
4. Lab: Network & System Laboratory - EC5018 (11:00a.m. - 5:00p.m.)
5. Deadline: 電子檔請於 2021/10/13 9:10 前上傳至網路大學。

Part 1: Web Browsing (DNS, TCP)

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

Procedure.

1. Install and start Wireshark
2. Start a web browser and type the URL of a website: http://cse.nsysu.edu.tw but do not press ENTER.
3. Start Wireshark 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

Other example for how to use Wireshark：
https://www.howtogeek.com/104278/how-to-use-wireshark-to-capture-filter-and-inspect-packets/

Protocol Analysis Questions

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

1. Find the first DNS request packet sent by the client. (Request for cse.nsysu.edu.tw) You can find a record like below on Wireshark. And you can answer the question.

(1) Examine the Ethernet

a. What is the Ethernet address of the source and destination?

b. What is the content of the type field in the Ethernet frame?

(2) Examine the Internet Protocol

a. What is the IP address of the source and destination?

b. What is the header length? What is the total packet length?

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

(3) Examine the User Datagram Protocol

a. Identify the client ephemeral port number and the server well-known port number.

b. What type of application layer protocol is in the payload?

(4) Examine the Domain Name System (query)

a. What field indicates whether the message is a query or a response?

b. What is the query transaction ID?

c. Identify the fields that carry the type and class of the query.

2. Find the DNS response packet which is response to the DNS request packet from the above question. You can find a record like below on Wireshark. And you can answer the question. (cse.nsysu.edu.tw == 140.117.13.244)

(1) Examine the Ethernet

a. What is the Ethernet address of the source and destination?

b. What is the content of the type field in the Ethernet frame?

(2) Examine the Internet Protocol & Domain Name System (response)

a. What is the IP address of the source and destination?

b. What is the header length? What is the total packet length? Is it longer

than the query?

c. How many answers are provided in the response message? Compare the answers and their time-to-live values.

3. Find the first TCP packet sent by client. (The destination IP address is response from above question.) You can find three record like below on Wireshark. It's TCP three-way handshake

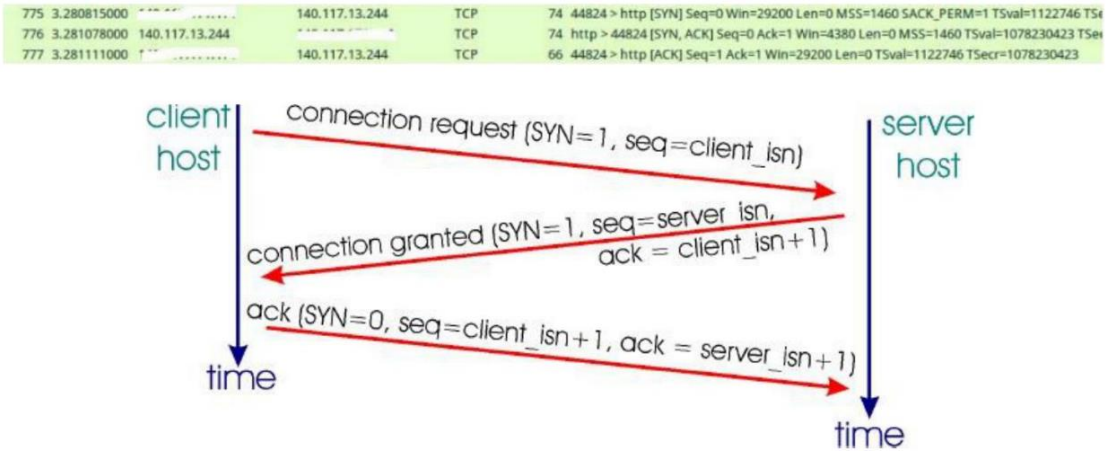

Figure: TCP three-way handshake (1)

Examine the Transmission Control Protocol

a. What are the ephemeral port number used by the client and the well-known port number used by the server?

b. What is the length of the TCP segment?

c. What is the initial sequence number for the segments from the client to the server?

d. What is the initial window size?

e. What is the maximum segment size?

f. Find the hex character that contains the SYN flag bit

Part 2 Probing the Internet (ICMP, PING, Traceroute)

Objective

In this exercise we investigate two applications of the Internet Control Message Protocol (ICMP):

1. PING uses ICMP to determine whether a host is reachable

2. Traceroute uses ICMP to allow users to determine the route that an IP packet takes from a local host to a remote host

Protocols Examined

-ICMP: Echo, Echo Reply, Time Exceeded messages

-IP Time-to-Live
-PING application
-Traceroute application

Background Material
PING, Traceroute commands: Consult your system documentation for information on using these commands. (In Ubuntu: man ping or man traceroute)

Procedure
PING
1. Prepare Wireshark for a packet capture.
2. Open a Command Prompt window.
3. Type "ping 8.8.8.8"; Do NOT press ENTER.
4. Start Wireshark packet capture.
5. Press ENTER in Command Prompt window.
6. Stop packet capture when Command Prompt returns.

Traceroute
1. Prepare Wireshark for a packet capture. .
2. Open a Command Prompt window.
3. Type "sudo traceroute –q 1 –I 8.8.8.8"; Do NOT press ENTER.
4. Start Wireshark packet capture.
5. Press ENTER in Command Prompt window.
6. Stop packet capture when Command Prompt returns.

Protocol Analysis Questions
To answer the following questions, start Wireshark and open the packet capture file created above.
1. Ping Captured.
(1) Find the first ICMP Echo Request packet.
a. First, examine the Internet Protocol. What is the Time-to-Live?
b. Next examine the Internet Control Message Protocol. What is the ICMP message type?
c. What is the message identifier and sequence number?
(2) Find the first ICMP Echo Reply packet.
a. Now examine the Internet Control Message Protocol. What is the ICMP message type?

2. Traceroute Captured.

(1) Find the first ICMP Echo Request packet.

a. Examine the Internet Protocol. What are the source and destination addresses?

b. What are the protocol type and the Time-to-Live in the IP packet?

c. Next, examine the Internet Control Message Protocol. What is the ICMP message type? What are the message identifier and sequence number?

(2) Find an ICMP Time-to-live exceeded packet.

a. Examine the Internet Protocol. What are the source and destination addresses?

b. Next, examine the Internet Control Message Protocol. What is the ICMP message type?

Part 3 Measuring Network Bandwidth

Objective

In this part, we measure our network bandwidth via iperf.

Install with command line: (64-bit for example)

1. sudo apt-get remove iperf3 libiperf0
2. wget https://iperf.fr/download/ubuntu/iperf3_3.1.3-1_amd64.deb
3. wget https://iperf.fr/download/ubuntu/libiperf0_3.1.3-1_amd64.deb
4. sudo dpkg -i libiperf0_3.1.3-1_amd64.deb iperf3_3.1.3-1_amd64.deb
5. rm libiperf0_3.1.3-1_amd64.deb iperf3_3.1.3-1_amd64.deb

or directly download from https://iperf.fr/iperf-download.php

Server IP : 140.117.171.208

1. Measure the bandwidth for Transmission Control Protocol Type “iperf3 -c 140.117.171.208 -t 10 -i 2”
2. Adjust the window size for Transmission Control Protocol. See what’s different. Type “iperf3 -c 140.117.171.208 -w 2000 -t 10 -i 2”
3. Measure the bandwidth for User Datagram Protocol Type “iperf3 -c 140.117.171.208 -u -t 10 -i 2”
4. Adjust the bandwidth for User Datagram Protocol. Measure the package lost rate or any else happened. Type “iperf3 -c 140.117.171.208 -u -t 10 -i 2 -b 512G”