Lab 9: Application and Transport Layer Protocols

Or: HTTP and TCP in action

Overview

In tasks 1 and 2 you will explore the many functions of the Transport Layer TCP protocol that contribute to a reliable and successful communication between two communicating entities.

What you will do:

1. Capture, inspect, and understand the basic operation of TCP.

Things that you will need to know or learn:

1. TCP Port numbers for the HTTP application.
2. How to use Wireshark to capture & **filter** interesting network traffic
3. How to identify key fields in a Wireshark capture: IP addresses, port numbers, transport layer header values, and application layer header and data fields. (Skill exercised by lab)
4. TCP header fields: Acknowledgement number, Sequence number, Flags, Source port, Destination port, Header length, Checksum, Options, Urgent
5. TCP three way handshake, connection tear down.

What you need to submit and when:

1. Complete the in-lab part of the exercise (see below), **during** your scheduled lab period.
2. Complete the "Lab 9 – Postlab Quiz" on Blackboard, **before** the due time.

References and Resources:

- Chapter 9 from the CISCO's online curriculum
- Week 9 lecture

Task 0: Setup

Step 1:
Preparation tasks:

- Download this document to your laptop.
- Disable your wireless network adapter.
- Connect your laptop to the lab's Eagle Network (red RJ45 jack).
- Make sure you have a valid IP address from the red network (172.16.0.0/16).

Task 1: Capture HTTP communication between client and server (using Wireshark)

Step 1. Open a Command Prompt as administrator and enter these commands

a. arp -d * Clear your Arp cache
b. Ipconfig /flushdns Clear your DNS cache

Step 2. Open Wireshark BUT do not start the capture yet.

Step 3. Set the Wireshark's Ethernet interface capture buffer size to 200 Mbytes. Here's how: Select Capture →Options; double click the **Ethernet** interface; increase buffer size to 200 Mbytes. Click **Start** to start a Wirehark capture.

Step 4. Open a web browser and connect to http://eagle-server.example.com

Step 5. Stop the Wireshark capture. **Save your wireshark capture** as "Lab9". DO NOT PROCEED to Task 2 until you have validated your Wireshark capture.

Wireshark Capture Validation: **Filter** the output to only display frames corresponding to the above client to server communication:

Filter: (http || tcp) && ((ip.src == c.c.c.c && ip.dst == s.s.s.s) || (ip.dst == c.c.c.c && ip.src == s.s.s.s))

Replace c.c.c.c with your client IP address and s.s.s.s with the Eagle Server address.

Task 2: HTTP/TCP Communication Analysis

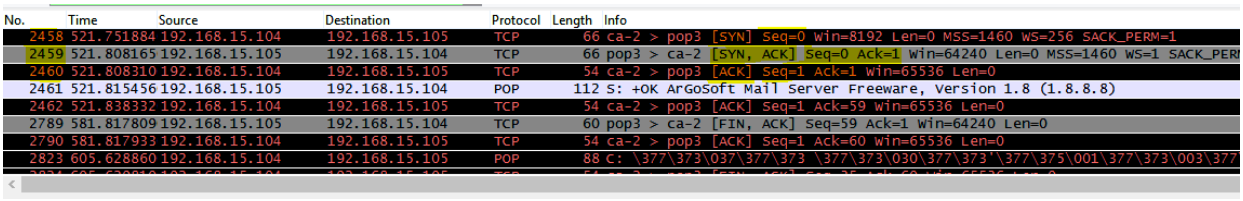
Step 1. Examine and analyse the frames to answer the following questions:

Three-Way Handshake

Locate the three frame numbers corresponding to the TCP session establishment between the client and server. The session establishment is known as the Three-Way Handshake. Frames 2458, 2459 and 2460 in the figure below are an example of a Three-Way Handshake with the TCP flag sequence:

[SYN]
[SYN, ACK]
[ACK]

*****Note that the IPs and TCP ports values remain UNCHANGED for all frames of the same communication session. Segments with different port values belong to different sessions! In this section and all subsequent sections, it is important that you identify TCP segments belonging to the same session!**



No.	Time	Source	Destination	Protocol	Length	Info
2458	521.751884	192.168.15.104	192.168.15.105	TCP	66	ca-2 > pop3 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
2459	521.808165	192.168.15.105	192.168.15.104	TCP	66	pop3 > ca-2 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 WS=1 SACK_PERM
2460	521.808310	192.168.15.104	192.168.15.105	TCP	54	ca-2 > pop3 [ACK] Seq=1 Ack=1 Win=65536 Len=0
2461	521.815456	192.168.15.105	192.168.15.104	POP	112	S: +OK ArGoSoft Mail Server Freeware, Version 1.8 (1.8.8.8)
2462	521.838332	192.168.15.104	192.168.15.105	TCP	54	ca-2 > pop3 [ACK] Seq=1 Ack=59 Win=65536 Len=0
2789	581.817809	192.168.15.105	192.168.15.104	TCP	60	pop3 > ca-2 [FIN, ACK] Seq=59 Ack=1 Win=64240 Len=0
2790	581.817933	192.168.15.104	192.168.15.105	TCP	54	ca-2 > pop3 [ACK] Seq=1 Ack=60 Win=65536 Len=0
2823	605.628860	192.168.15.104	192.168.15.105	POP	88	C: \377\373\037\377\373 \377\373\030\377\373'\377\375\001\377\373\003\377

1. Locate the three frames in your Wireshark capture corresponding to your client to server Three-Way Handshake.
2. What TCP port number has been assigned at the client end?

   _____

3. What are the values of Seq, Ack and Window Size in the last segment of the three-way handshake?

   SEQ _____

   ACK _____

   Window _____

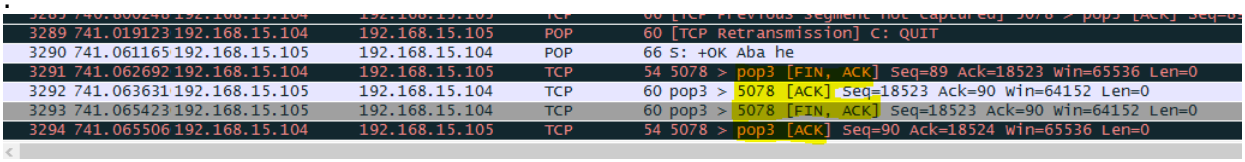
(Note: the Ack value is a different animal from the [ACK] flag.
In the middle pane, pop open the [+] Transmision_Control … and [+] Flags: …
to see the difference between: Ack Acknowledgement_number:
and Flags: (ACK) ...1 .. Acknowledgement:: (flag) Set

TCP Connection Tear-down

You will locate the four frames corresponding to the client to server TCP connection Tear-Down. Please refer to frames 3291, 3292, 3293 and 3294 in the figure below for sample frames with the TCP flag sequence:

[FIN, ACK]
[ACK]
[FIN, ACK]
[ACK]

.



Note: All TCP segments belonging to the same communication, including segments for the 3-way handshake, data transfer and connection tear-down are uniquely identified via the combination called a socket:

- Client IP/ TCP Port;
- Server IP/ TCP Port.

Using the Sequence (Seq) and Acknowledgment (Ack) number values in the last frame of the connection teardown (shown above), you can tell how much application layer data (bytes) was transferred in each direction (client to server and server to client).

For example, in the communication represented by the example above, the Sequence number is 90 bytes and the Acknowledgement number is 18524. Since the frame originates at the client end:
Seq = 90 indicates that 90 bytes of DATA was transferred from the client to the server.
Ack=18524 indicates that (18524 -1) = 18523 bytes of data was acknowledged and received from the server.

Task 3: DNS Communication Analysis

1. Locate the frames in your Wireshark capture corresponding to the DNS query and response. You will need to modify your display filter.

2. Show your lab instructor the DNS frames. _____

Task 4: Clean up, Blackboard Lab Quiz

Step 1. Make sure you have saved all the results you got during this lab period.
Step 2. Re-enable Firewalls, Anti-virus, Wireless, etc.
Step 3. Complete “Lab 9 – Postlab Quiz” before the due time.