Lab 9: Application and Transport Layer Protocols

*Or*: FTP 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 FTP 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 BrightSpace, **before** the due time.

References and Resources:

* Chapter 9 from the CISCO’s online curriculum
* Lecture on chapter 9

Task 0: Setup

Step 1:

Preparation tasks:

* Download this document to your laptop.
* Connect to the Internet.

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

1. Open Wireshark BUT do not start the capture yet.
2. Choose the proper network interface on Wireshark and set the capture buffer size to 200 Mbytes. Here’s how: Select Capture 🡪Options; double click the proper interface; increase buffer size to 200 Mbytes. Click **Start** to start a Wirehark capture.
3. Open a Command Prompt as administrator and enter these commands
   1. arp -d \* Clear your Arp cache
   2. ipconfig /flushdns Clear your DNS cache
4. Open a Command Prompt and login to the FTP server by the following command:

ftp ftp.cdc.gov

Use “anonymous” as user, no password needed. When you logged into the FTP server, you can execute and FTP commands on the Server.

Type the command “**quit**” to logout from the FTP server.

1. Stop the Wireshark capture. **Save your wireshark capture** as “Lab9\_task1”. 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: (ftp || 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 FTP address.

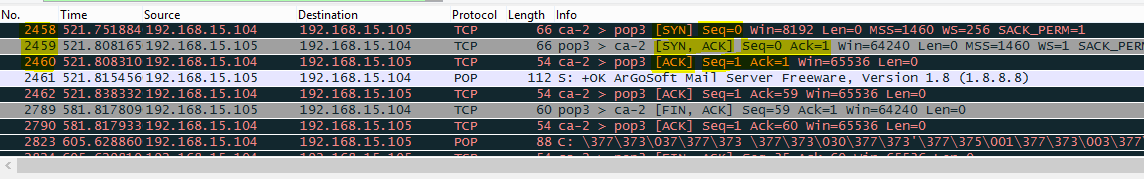
Task 2: FTP/TCP Communication Analysis

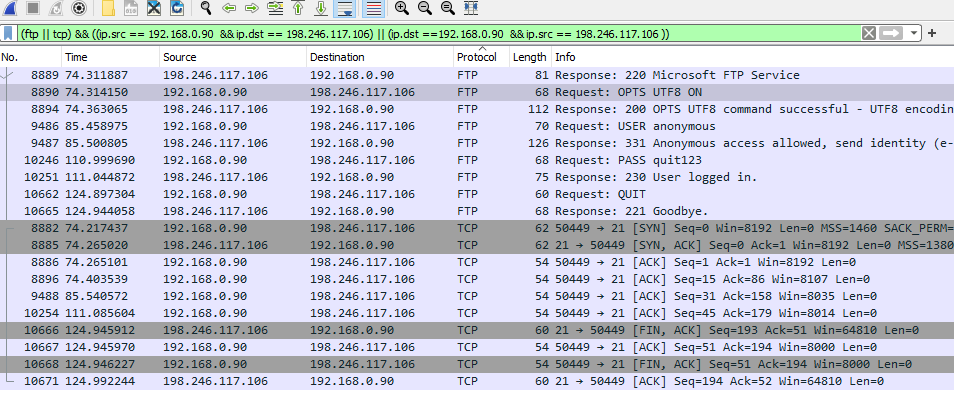
1. Examine and analyse the frames to answer the following questions:

**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!**



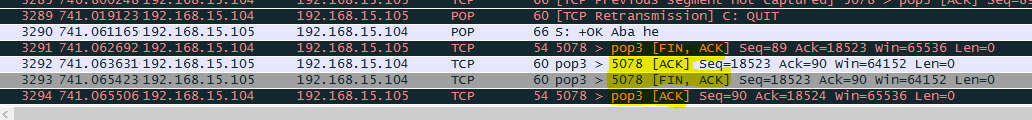


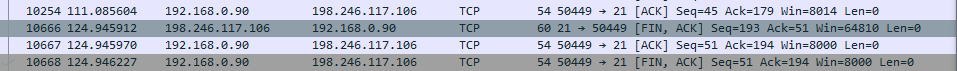
1. Locate the three frames in your Wireshark capture corresponding to your client to server Three-Way Handshake.
2. What TCP port number has been assigned at the client end?  
    50449
3. What are the values of Seq, Ack and Window Size in the last segment of the three-way handshake?  
    SEQ =194  
     
    ACK = 52  
     
    Window = 64810  
     
     
    *(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. Take a screen capture of the located frames and save as “Lab9\_task3”.

Task 4: Clean up, BrightSpace Lab Quiz

1. Submit your saved results “Lab9\_task1”, “Lab9\_task3” and this doc with questions answered to BrightSpace.
2. Complete “Lab 9 – Postlab Quiz” before the due time.