

College of Engineering

Computer Engineering Department

Computer Network Lab

**Exp. No.6**

(Wireshark Lab: TCP)

**Prepared by:**

**Assist. Lecturer Basheer H. Ali**

**2018-2019**

**Introduction**

TCP is a unicast **connection-oriented** protocol. Before either end can send data to the other, a connection must be established between them. TCP detects and repairs essentially all the data transfer problems that may be introduced by packet loss, duplication, or errors at the IP layer (or below).

Because of its management of **connection state** (information about the connection kept by both endpoints), TCP is a considerably more complicated protocol than UDP. UDP is a connectionless protocol that involves no connection establishment or termination. One of the major differences between the two is the amount of detail required to handle the various TCP states properly: when connections are created, terminated normally, and reset without warning.

During connection establishment, several options can be exchanged between the two endpoints regarding the parameters of the connection. Some options are allowed to be sent only when the connection is established, and others can be sent later. The TCP header has a limited space for holding options (40 bytes).

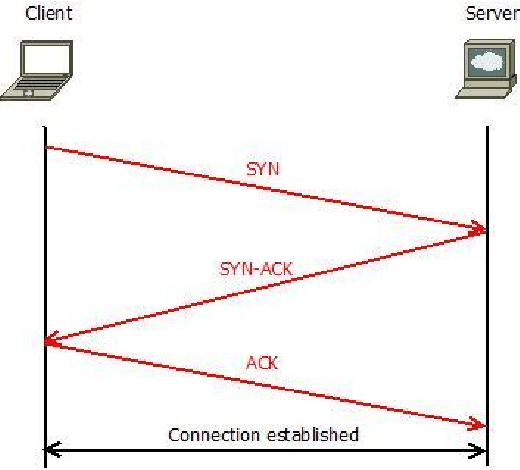
### TCP Connection Establishment and Termination:

A TCP connection is defined to be a 4-tuple consisting of two IP addresses and two port numbers. It is a pair of **endpoints** or **sockets** where each endpoint is identified by an (IP address, port number) pair.

A connection typically goes through three phases:

1. Setup (see figure#1)
2. Data transfer (called established)
3. Teardown (closing)

Some of the difficulty in creating a robust TCP implementation is handling all of the transitions between and among these phases correctly. A typical TCP connection establishment and close (without any data transfer).



…….

Data Transfer

……..



Figure #1: TCP Three Way Handshaking

## Activity 1 - Capture TCP Traffic

To capture TCP traffic:

1. [Start a Wireshark capture](https://en.m.wikiversity.org/wiki/Wireshark/Start).
2. [Open a command prompt](https://en.m.wikiversity.org/wiki/Command_Prompt/Open).
3. Type telnet www.google.com 80 and press Enter.
4. Close the command prompt to close the TCP connection.
5. [Stop the Wireshark capture](https://en.m.wikiversity.org/wiki/Wireshark/Stop)

## Activity 2 - Analyze TCP SYN Traffic

To analyze TCP SYN traffic:

1. Observe the traffic captured in the top Wireshark packet list pane. To view only TCP traffic related to the web server connection, type **tcp.port == 80** (lower case) in the Filter box and press **Enter.**
2. Select the first TCP packet, labeled **http [SYN]**.
3. Observe the packet details in the middle Wireshark packet details pane. Notice that it is an Ethernet II / Internet Protocol Version 4 / Transmission Control Protocol frame.
4. Expand Ethernet II to view Ethernet details.
5. Observe the Destination and Source fields. The destination should be your default gateway's MAC address and the source should be your MAC address. You can use [ipconfig /all](https://en.m.wikiversity.org/wiki/Ipconfig/All) to confirm.
6. Expand Internet Protocol Version 4 to view IP details.
7. Observe the Source address. Notice that the source address is your IP address.
8. Observe the Destination address. Notice that the destination address is the IP address of one of Google's web servers.
9. Expand Transmission Control Protocol to view TCP details.
10. Observe the Source port. Notice that it is a dynamic port selected for this connection.
11. Observe the Destination port. Notice that it is http (80).
12. Observe the Sequence number. Notice that it is 0 (relative sequence number). To see the actual sequence number, select Sequence number to highlight the sequence number in the bottom Wireshark bytes pane.
13. Expand Flags to view flag details.
14. Observe the flag settings. Notice that SYN is set, indicating the first segment in the TCP three-way handshake.

## Activity 3 - Analyze TCP SYN, ACK Traffic

To analyze TCP SYN, ACK traffic:

1. In the top Wireshark packet list pane, select the second TCP packet, labeled **SYN, ACK**.
2. Observe the packet details in the middle Wireshark packet details pane. Notice that it is an Ethernet II / Internet Protocol Version 4 / Transmission Control Protocol frame.
3. Expand Ethernet II to view Ethernet details.
4. Observe the Destination and Source fields. The destination should be your MAC address and the source should be your default gateway MAC address.
5. Expand Internet Protocol Version 4 to view IP details.
6. Observe the Source address. Notice that the source address is the Google web server IP address.
7. Observe the Destination address. Notice that the destination address is your IP address.
8. Expand Transmission Control Protocol to view TCP details.
9. Observe the Source port. Notice that it is http (80).
10. Observe the Destination port. Notice that it is the same dynamic port selected for this connection.
11. Observe the Sequence number. Notice that it is 0 (relative sequence number). To see the actual sequence number, select Sequence number to highlight the sequence number in the bottom Wireshark bytes pane.
12. Observe the Acknowledgement number. Notice that it is 1 (relative ack number). To see the actual acknowledgement number, select Acknowledgement number to highlight the acknowledgement number in the bottom pane. Notice that the actual acknowledgement number is one greater than the sequence number in the previous segment.
13. Expand Flags to view flag details.
14. Observe the flag settings. Notice that SYN and ACK are set, indicating the second segment in the TCP three-way handshake.

## Activity 4 - Analyze TCP ACK Traffic

To analyze TCP ACK traffic:

1. In the top Wireshark packet list pane, select the third TCP packet, labeled **http ACK**.
2. Observe the packet details in the middle Wireshark packet details pane. Notice that it is an Ethernet II / Internet Protocol Version 4 / Transmission Control Protocol frame.
3. Expand Ethernet II to view Ethernet details.
4. Observe the Destination and Source fields. The destination should be your default gateway MAC address and the source should be your MAC address.
5. Expand Internet Protocol Version 4 to view IP details.
6. Observe the Source address. Notice that the source address is your IP address.
7. Observe the Destination address. Notice that the destination address is the Google web server IP address.
8. Expand Transmission Control Protocol to view TCP details.
9. Observe the Source port. Notice that it is the same dynamic port selected for this connection.
10. Observe the Destination port. Notice that it is http (80).
11. Observe the Sequence number. Notice that it is 1 (relative sequence number). To see the actual sequence number, select Sequence number to highlight the sequence number in the bottom Wireshark bytes pane.
12. Observe the Acknowledgement number. Notice that it is 1 (relative ack number). To see the actual acknowledgement number, select Acknowledgement number to highlight the acknowledgement number in the bottom pane.
13. Expand Flags to view flag details.
14. Observe the flag settings. Notice that ACK is set, indicating the third segment in the TCP three-way handshake. The client has established a TCP connection with the server.

## Activity 5 - Analyze TCP FIN ACK Traffic

To analyze TCP FIN ACK traffic:

1. In the top Wireshark packet list pane, select the fourth TCP packet, labeled **http FIN, ACK**.
2. Observe the packet details in the middle Wireshark packet details pane. Notice that it is an Ethernet II / Internet Protocol Version 4 / Transmission Control Protocol frame.
3. Expand Ethernet II to view Ethernet details.
4. Observe the Destination and Source fields. The destination should be your default gateway MAC address and the source should be your MAC address.
5. Expand Internet Protocol Version 4 to view IP details.
6. Observe the Source address. Notice that the source address is your IP address.
7. Observe the Destination address. Notice that the destination address is the Google web server IP address.
8. Expand Transmission Control Protocol to view TCP details.
9. Observe the Source port. Notice that it is the same dynamic port selected for this connection.
10. Observe the Destination port. Notice that it is http (80).
11. Observe the Sequence number. Notice that it is 1 (relative sequence number).
12. Observe the Acknowledgement number. Notice that it is 1 (relative ack number).
13. Expand Flags to view flag details.
14. Observe the flag settings. Notice that FIN and ACK are set, indicating the first segment in the TCP teardown handshake. The client has indicated it is closing the TCP connection with the server.

## Activity 6 - Analyze TCP FIN ACK Traffic

To analyze TCP FIN ACK traffic:

1. In the top Wireshark packet list pane, select the fifth TCP packet, labeled **FIN, ACK**.
2. Observe the packet details in the middle Wireshark packet details pane. Notice that it is an Ethernet II / Internet Protocol Version 4 / Transmission Control Protocol frame.
3. Expand Ethernet II to view Ethernet details.
4. Observe the Destination and Source fields. The destination should be your MAC address and the source should be your default gateway MAC address.
5. Expand Internet Protocol Version 4 to view IP details.
6. Observe the Source address. Notice that the source address is the Google web server IP address.
7. Observe the Destination address. Notice that the destination address is your IP address.
8. Expand Transmission Control Protocol to view TCP details.
9. Observe the Source port. Notice that it is http (80).
10. Observe the Destination port. Notice that it is the same dynamic port selected for this connection.
11. Observe the Sequence number. Notice that it is 1 (relative sequence number).
12. Observe the Acknowledgement number. Notice that it is 2 (relative ack number).
13. Expand Flags to view flag details.
14. Observe the flag settings. Notice that FIN and ACK are set, indicating the second segment in the TCP three-way handshake. The server has indicated it is closing the TCP connection with the client.

## Activity 7 - Analyze TCP ACK Traffic

To analyze TCP ACK traffic:

1. In the top Wireshark packet list pane, select the sixth TCP packet, labeled **http ACK**.
2. Observe the packet details in the middle Wireshark packet details pane. Notice that it is an Ethernet II / Internet Protocol Version 4 / Transmission Control Protocol frame.
3. Expand Ethernet II to view Ethernet details.
4. Observe the Destination and Source fields. The destination should be your default gateway MAC address and the source should be your MAC address.
5. Expand Internet Protocol Version 4 to view IP details.
6. Observe the Source address. Notice that the source address is your IP address.
7. Observe the Destination address. Notice that the destination address is the Google web server IP address.
8. Expand Transmission Control Protocol to view TCP details.
9. Observe the Source port. Notice that it is the same dynamic port selected for this connection.
10. Observe the Destination port. Notice that it is http (80).
11. Observe the Sequence number. Notice that it is 2 (relative sequence number).
12. Observe the Acknowledgement number. Notice that it is 2 (relative ack number).
13. Expand Flags to view flag details.
14. Observe the flag settings. Notice that ACK is set, indicating the third segment in the TCP teardown handshake. The client has acknowledged the server closing the TCP connection.

**Homework:**

Download this packet trace http://packetlife.net/captures/HTTP.cap and answer the following questions: (provide screenshot for your answer).

1. What is the IP address of the client (the initiator of this TCP connection), and what is the server's IP address? From which port the client initiates the connection, and what is the port number used for this connection on the server side?

2. During the handshaking of this connection, what is the length of the TCP header? Is this TCP header the basic one? If not, what is the optional field(s) in the TCP header.

3. Answer 3 after the handshaking stage. What is the length of maximum TCP payload of a packet after this tcp connection is established?

4. What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and server? What is it in the segment that identifies the segment as a SYN segment?

5. What is the sequence number of the SYNACK segment sent by the server to the client computer in reply to the SYN? What is the value of the ACKnowledgement field in the SYNACK segment? How did the server determine that value? What is it in the segment that identifies the segment as a SYNACK segment?