ISLAMIC UNIVERSITY OF TECHNOLOGY

Organization of Islamic Cooperation

Board Bazar, Gazipur

Laboratory Report 02

CSE 4512

**Title**: Understanding the basics of OSI Model

**Objective**:

* Examine HTTP Web Traffic.
* Display Elements of the TCP/IP Protocol Suite

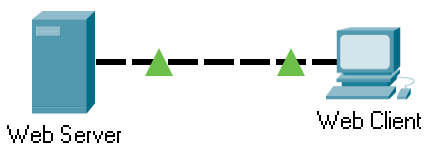
**Devices/Software Used**: Cisco Packet Tracer

**Working Procedure**:

Following steps are taken to complete the Experiment:

1. It was ensured that we are in Simulation mode and that only HTTP events are being tracked.
2. The browser of the Web Client was used to navigate to the URL ‘www.osi.local’.
3. In the Simulation window, the forward button was clicked four times to go through all four events.
4. It was ensured that the website had loaded in the Web Client’s browser.
5. For each event, the OSI Model and Outbound PDU Details were examined. The details are provided below.
6. Next, we moved to the section for displaying elements of the TCP/IP Protocol suites. All the event types were shown. The additional event types include DNS, ARP and TCP.
7. The OSI Model and Outbound PDU Details for the first DNS event were analyzed. In the DNS Query section of the Outbound PDU Details, the name was ‘www.osi.local’.
8. The last DNS event was analysed. In the OSI Model, it was said to be at device Web Client. In the DNS Answer section of the Inbound PDU Details no ADDRESS label could be found.
9. The first TCP event after the first HTTP event was analysed. In layer 4 of the In Layers section of the OSI Model of this event, it was seen that the TCP connection was successful and the device set the connection state to ESTABLISHED.
10. The last TCP event was analyzed. This event closed the connection after all other activities were complete.
11. The port numbers for HTTP requests and DNS requests were examined. The Web Server was listening for HTTP requests on port 80 and for DNS requests on port 53.

**Diagram of the experiment**:



**Observation**:

At the time of exploring the contents of HTTP packets from the event list, I observed there are four HTTP events taking place. I found notable findings in each of the event and explanation of the findings are listed below:

1st HTTP Event:

In layer 7, the actual HTTP request was made. There was no text next to the label for this layer. The text beneath was given as:

The HTTP client sends a HTTP request to the server.

In layer 4, segmentation information was added. The source and destination ports were also identified. The destination port was 80.

In layer 3, the source and destination IP addresses were identified. It was detected that the destination was within the same subnet, so the next hop was set to the destination directly. The destination IP value was 192.168.1.254.

In layer 2, the ARP protocol was used to find the MAC address of the destination using its IP address. The PDU was also encapsulated into an ethernet frame.

Moving to the IP packet, the source and destination IPs were also seen here. This packet was created in layer 3.

In the TCP packet, the source and destination ports, the sequence number and the ACK number were given. This packet was created in layer 4.

In the HTTP section, the host was ‘www.osi.local’. This information came from layer 7.

2nd HTTP Event:

During the previous event, the frame was buffered in layer 1 since the fastEthernet0 port was busy. In this event, the port became free, so the frame was finally sent.

3rd HTTP Event:

The third event dealt with what happened at the server.

The frame was received by the first layer. Layer 2 ensured that the destination MAC address was an acceptable one and then decapsulated the frame. Layer 3 checked that the destination IP address was an acceptable one and then decapsulated the packet. Layer 4 collected the segments, reassembled them and passed them to the upper layer. Layer 7 received the HTTP request.

Next, layer 7 sent an HTTP reply. In Layer 4, segmentation information was added. The source and destination ports were also identified. The destination port was 1025. In Layer 3, the source and destination IP addresses were added. The destination was identified as being within the same subnet, so the next hop was set directly to the destination. The destination IP value was 192.168.1.1. In Layer 2, the ARP protocol was used to identify the MAC address of the destination using its IP address. The PDU was encapsulated into an ethernet frame. In layer 1, the frame was sent out.

The major differences between the In Layers and the Out Layers was in the In Layers, all the addresses such as MAC addresses and IP addresses were being checked to ensure this device was the intended destination while in the Out Layers, this information was being added. Additionally, decapsulation took place in the In Layers while encapsulation took place in the Out Layers.

In the HTTP section of the Outbound PDU Details, the first line was ‘HTTP Data: Connection: close’.

4th HTTP Event:

In this event, the response from the server reached the client. The OSI Model tab gave information about the different layers, while the Incoming PDU Details tab gave information about the different packets. The Outgoing PDU Details tab was missing since nothing was being sent out in this event. The information for the In Layers section of the OSI Model was the same as that in the previous event.

**Challenges**:

There were no major challenges completing this activity. The only challenges faced were minor, such as initially figuring out how the different parts of the UI were laid out and what I needed to look at to find the answers.