Lab 2: Packet Analysis and Network Simulation

This lab is about simulation. In other words, how packets of different protocols move from one device to another device, and what are the fields present in the headers of these packets will be shown in this lab. Also, we will see how we can create some particular event by ourselves to observe the flow of packets. So, let's dive into the introduction of each task.

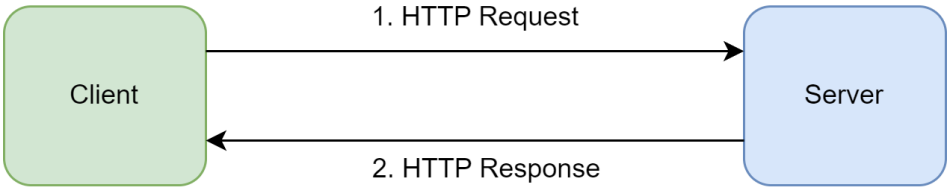
Packet Tracer Simulation

At the end of lab 1, after completing the configuration, we were asked to check the connectivity between the devices. For that, we had to ping one device from another. This means a packet has to traverse from the source to the destination. Today we are going to observe these packets but for web browsing and sending emails.

Web Browsing (HTTP Protocol)

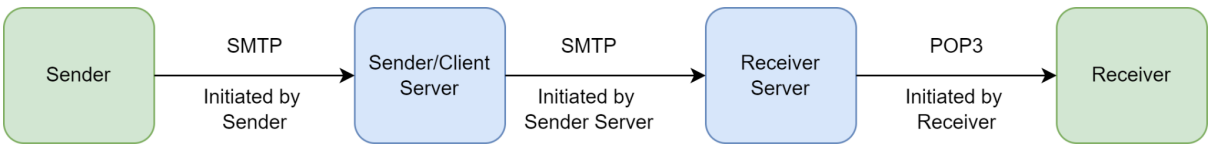
You may recall that protocols are the set of rules that govern the communication. To browse or surf the internet, we have to follow certain rules that are specifically mentioned in the HTTP protocol. If we go through a real-life example, suppose you have gone to the Information Desk of our university to get some information and the person sitting there has provided you with your desired information. Two things happened here, one is that you have requested and the other is that the person has responded to your request. HTTP works in the same way. Every time we want to browse any website, we send a request to the server where that webpage is hosted. After acknowledging the request, the server sends a response. Here, our browsers through which we visit the webpage work as clients while the web servers work as servers. Today we will see what are the fields of HTTP request and response messages, what the source and destination IP addresses are and what the source and destination

port addresses are. You may recall that we use port addresses to identify the processes/applications of a device.



Emailing (SMTP, POP3)

Unlike web browsing, we need to use multiple protocols for sending and receiving emails. In our case, we are going to observe the SMTP protocol to send email and the POP3 protocol to receive email. It might seem that when we send an email it directly goes to the other user/device. However, this is not the case. Let's think the person who is sending the mail is the sender, the person who is receiving the mail is the receiver. Between them, there exist one or multiple servers. Suppose the sender is using @yahoo.com domain while the receiver is using @gmail.com. For these two domains, there will be two different servers. When the sender sends the email, it first goes to the sender's mail server. In our case yahoo server. Then the yahoo server will send the mail to the Gmail server. In these two steps, the SMTP protocol is used. Once the mail reaches the receiver's mail server, the receiver must fetch the email to see it. Again, the receiver's server will not send the email to the receiver by itself. So, the receiver will fetch the email from its server (in our case the Gmail server) using the POP3 protocol. We will be seeing one example involving both of these protocols in our lab.



DNS Protocol

You may recall that while pinging, we used the IP address of the destination device because the IP address is like the postal address of any device. Without it, we can't locate a device. Now, when we browse any website, we provide the URL or even while

sending emails we just write the sender's and the receiver's email addresses. Does it come to mind how the packets reach their destination without us specifically defining the destination IP addresses? There comes DNS protocol or in other words, the directory system of the Internet. DNS helps us to find the IP address of a server if we happen to know the URL of that web page. When we write www.bracu.ac.bd in the URL bar, first of all, our browser asks the DNS resolver to find out the IP address of the server where this page is hosted. Then the DNS resolver gets the IP address from the DNS server and provides it to the browser. After that, we establish a TCP connection and then send the HTTP request message. For this lab, we will not focus on how the TCP connection is established but we will see how DNS and HTTP work.

Wireshark Simulation

In the case of packet tracer, we have worked in a dummy environment. Let's see how things actually work in a real-life scenario. Using Wireshark we will capture HTTP packets that we send and receive from the computer that you are using to read this document. Wireshark can also be used to capture any type of packet. If you like playing around with different protocol header fields and how they change, this is the perfect tool for you.

NS3 Simulation

In our previous two tasks, we have observed how different protocols work. These protocols have some predefined rules that were already implemented in the devices. How about, creating the nodes/devices and establishing connections and installing the protocols in them by ourselves? In other words, simulating the system that will be built from scratch by ourselves. There comes NS3. Using NS3, we will assign IP addresses, and port addresses to our client and the server, we will define how many packets will be sent each time after how much delay, we will install the protocols for each layer and see the simulation of how packets are moving using another software name netAnim.

Note: The description of Wireshark Simulation and NS3 Simulation has been kept shorter here, as they have been elaborately discussed in the Task file. If you want to know more about NS3, you may learn from here.