CS 39006: Networks Lab

Assignment 2: Use Wireshark for Understanding Different Fields at Protocol Headers

Date: 31st January, 2017

Objective:

The objective of this assignment is to understand the TCP/IP protocol stack and the headers associated with different layers of the protocol stack.

Submission Instructions:

You need to prepare a report that will contain the followings.

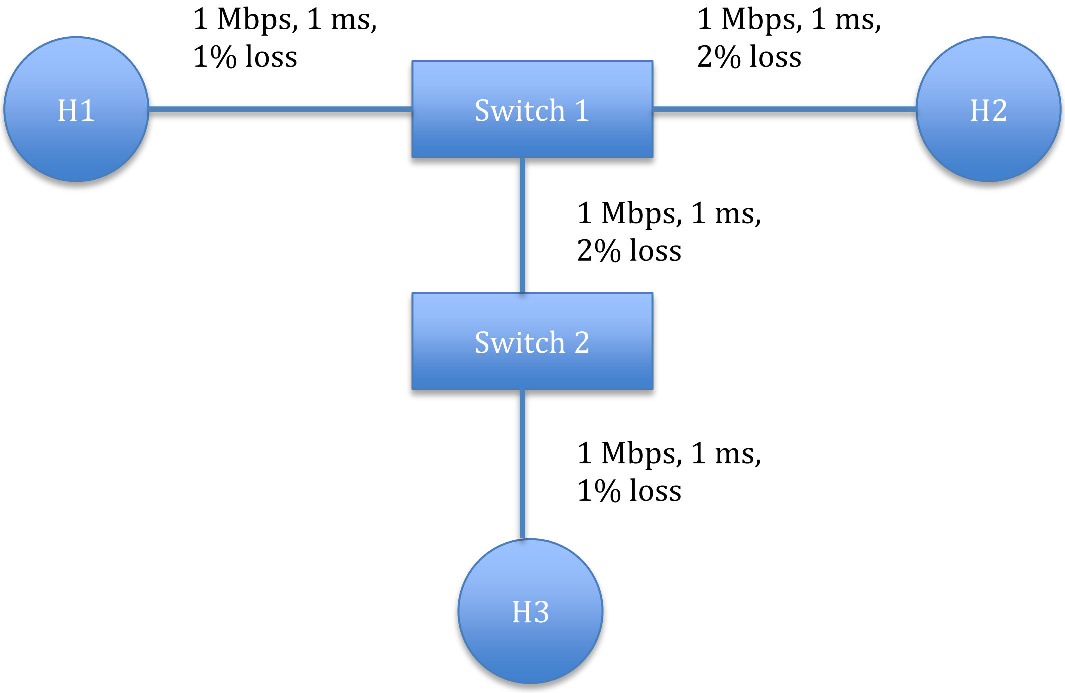
1. Steps followed in executing the experiments.
2. Observations from the experiments.
3. Intuitive justification behind the observations.

You need to submit the report and relevant scripts (source files) in a single compressed (tar.gz) file. Rename the compressed file as Assignment_3_Roll1_Roll2.tar.gz, where Roll1 and Roll2 are the roll numbers of the two members in the group. Submit the compressed file through Moodle by the submission deadline. The submission deadline is: **February 07, 2017 02:00 PM.** Please note that this is a strict deadline and no extension will be granted.

Please note that your submission will be awarded zero marks without further consideration, if it is find to be copied. In such cases, all the submissions will be treated equally, without any discremination to figure out who has copied from whom.

Assignment Statement:

Construct the following topology using Mininet.



Install an FTP server at Mininet VM. Start the FTP server at H1 and keep a large file (http://scholar.princeton.edu/sites/default/files/oversize_pdf_test_0.pdf) at the host H1. Host H2 and H3 works as FTP clients. Now from the hosts H2 and H3, download the file through FTP. You need to start both the FTP sessions (H3->H1 and H2->H1 almost simultaneously).
While the FTP sessions for file transfer is going on, collect all the data packets through Wireshark (or tcpdump) at H1, H2 and H3.

1. From the packet traces, identify different protocols used in the following layers of the protocol stack:
(a) Application layer
(b) Transport layer
(c) Network layer
(d) Data link layer

2. For each of the protocols you observe at different layers of the protocol stack, note down the followings,
(a) The header size at different layers
(b) Different fields inside the headers
(c) Source IP, Destination IP, Source port and Destination port for different end-to-end flows at the transport layer. How many different such flows can you observe in the given experiment? (A flow is identified by the 4-tuple <source IP, destination IP, source port, destination port> at the transport layer)

3. Find out whether the transport layer flows are uni-directional or bi-directional (a bi-directional flow means that you can observe packets from both H1 to H3 as well as from H3 to H1 for the same flow identified by the 4-tuple <source IP, destination IP, source port, destination port>).

4. What are the source and destination MAC addresses for the packets generated at H3? Check whether the destination MAC address is the MAC address of H1?

5. What are the source and destination IP addresses for the packets generated at H3? Check whether the destination IP address is the IP address of H1?

6. From (4) and (5), find out the utility of having two addresses (IP address and MAC address) associated with each device.