Lab 4: Introduction to Wireshark

Objective

The objective of this lab exercise will be for the student to gain experience observing and analyzing network traffic using a packet sniffer and network analyzer.

Required Tasks

The basic tool for observing the messages exchanged between executing protocol entities is called a packet sniffer. As the name suggests, a packet sniffer captures ("sniffs") messages being sent/received from/by your computer; it will also typically store and/or display the contents of the various protocol fields in these captured messages. A packet sniffer itself is passive. It observes messages being sent and received by applications and protocols running on your computer, but never sends packets itself. Similarly, received packets are never explicitly addressed to the packet sniffer. Instead, a packet sniffer receives a copy of packets that are sent/received from/by application and protocols executing on your machine.

We will be using the Wireshark packet sniffer for these labs, allowing us to display the contents of messages being sent/received from/by protocols at different levels of the protocol stack.

[Wireshark textbook paragraph]

Procedure

1. Download and install Wireshark.
2. Enable packet capturing through the Ethernet interface.
3. Open a web browser and browse to http://www.cmcc.edu
4. Collect a screen Shot of the Wireshark capture.

What is the Internet Protocol Version 4 Source Address?

What is the Internet Protocol Version 4 Source Port?

What is the Internet Protocol Version 4 Destination Address?

What is the Internet Protocol Version 4 Destination Port?

What is the transmission protocol being used for this request?