Assignment 3: Network Data Capture and Analysis

Assignment goals ：

1. Practice using tools such as tcpdump to capture data transmitted on the actual network;
2. Practice using matlab, python and other tools to process network data;
3. Develop a deeper understanding of network transport, IP and other concepts;

Background ：

The content of this experiment is to use tcpdump to capture the traffic on a physical network connected by a host or router, and use the data analysis function of data processing software such as python and matlab to process and analyze the collected data;

Tcpdump is a command line utility that allows you to capture and analyze network traffic going through your system. It is often used to help troubleshoot network issues, as well as a security tool. You can learn how to install and use this tool at reference's Reference website.

Once you have collected the data file, you need to use python or matlab to analyze and process it (extract valid information and make statistics). Both of them have plenty of libraries and functions to help you accomplish this task. This process will also help you gain a deeper understanding of the data flow composition on the network.

Procedures :

1. Use tcpdump to capture the traffic on a physical network connected to your computer, and save it to a file. (You can set the traffic collection period to 5 minutes)

2. Process the data you've collected and try to answer the following questions.

1) Give the load proportion of different transport layer protocols carried by IP packets, you can use a pie chart to show.

2) How to identify fragmented IP packets? How many IP packets are fragmented?

3) Give the cumulative distribution curve of IP packet length, and compare the difference under different loads. (TCP or UDP)

4) Process data from the data link layer, try to find the broadcast packets.

5) Try using tcpdump filters to capture ipv6 traffic and see if that works.

Platform & language & submission requirements :

※ The required system : Ubuntu/Linux/MacOs/Windows.

※ The required language : C/C++/python3/Matlab.

※ You need to submit an Experimental report, which should include: 1.One screenshot which shows the web data you've captured; 2. Description of your data processing methods and data processing program; 3. Analysis and answers to the questions mentioned in the previous section;

Reference :

[1] https://opensource.com/article/18/10/introduction-tcpdump