ECE/CPSC 8860 - LAB 1

TRAFFIC SNIFFING

1.1. Lab Setup

The first step in this assignment is to login to the lab machines using the credentials that have been provided.

1.2. Sniffing Network

Purpose

Data collection from a network is an important step in network traffic analysis. Depending on the volume of a traffic, it might be a challenging task. One should be able to collect only desired packets and choose proper places on a network to perform an efficient data collection. In this assignment you will;

- Learn common tools used to collect network packets.
- Understand challenges in packet capturing and learn how to use capture and display filters.
- Be able to decide proper data collection points on a network.
- Have a better understanding of low level network communication and the structure of a network packet.

Necessary Equipment/Programs

- Two hub
- Three host machines
- Wireshark / Tshark

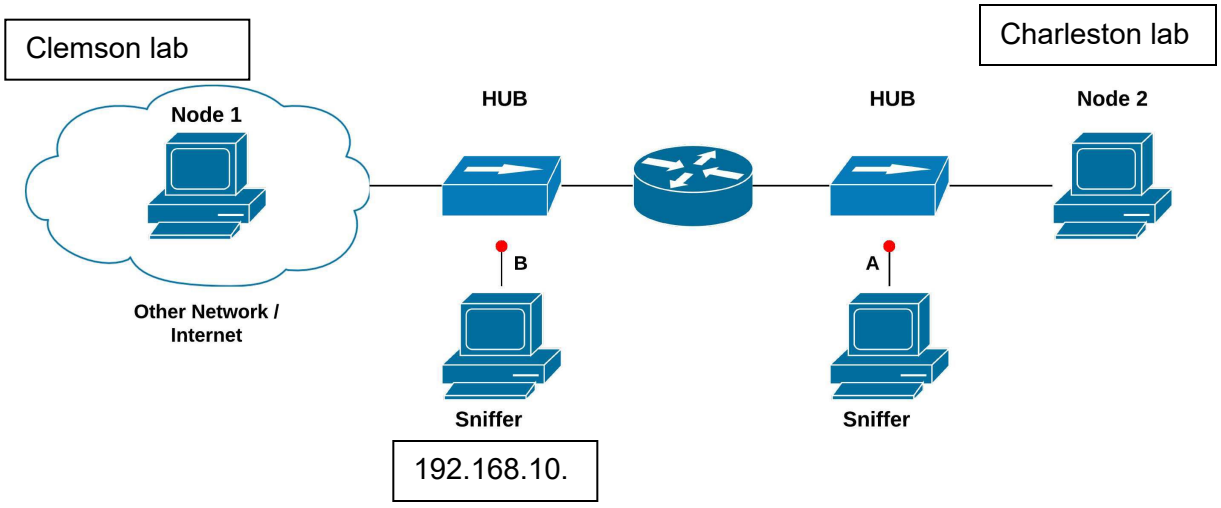

FIGURE 1.1
Sniffing experiment using a hub. Red dot is the sniffing point.

Instructions

- Setup the networks presented in Figure 1.1[1]
- Generate traffic between Node 1 and Node 2[2].

  Clemson students use “ping 192.168.20.x” x=8,9,10,11,13
  Charleston students use “ping 192.168.10.x” x=10,11,12,15,16,17,18,19,20,21,22

- Collect and save packets from the marked places using Wireshark / Tshark.

  All students use “ssh username@192.168.10.9” (this is the sniffer machine which is connected to the hub)
  Then use Wireshark / Tshark.
  If you want GUI, use “ssh -X username@192.168.10.9”

- Constrain your data collection / presentation for a specific packet type (IP address, protocol type, etc.) using proper capture / display filters.
- Students in Charleston should use capture filter in wireshark as ‘not host 192.168.20.x’ to avoid an echo, where x is the IP of local machine in Charleston lab.

2. Questions

1. Describe the layers and the fields of a packet captured from your network.
2. Explain the characteristics and functioning of a hub, switch and router in network science.

3. Explain the packet capture results obtained from the setups presented in Figure 1.1.

[1] This network has already been setup in the Clemson Network Security lab

[2] Traffic can be generated between hosts using ICMP messages. Check linux manual pages of ping and traceroute command for details.

3. DDoS Lab

1. Write capture / display filters for wireshark / tshark to collect packets coming from / going to a selected host on the network.
2. Write capture / display filters to collect packets with specific protocol type on the network. For example collect only TCP packets.
3. Generate heavy traffic on the network. [3] Try to collect all packets on the network using tcpdump. Investigate the tcpdump report after terminating the capture. Did you drop any packets? If yes explain why.
4. Plot time-series graph for captured packets which is graph of number of packets vs time to demonstrate your data.

[3] Transferring large files using scp between Node 1 and Node 2 can generate the necessary traffic.

4 Students are advised to refer https://braindump.bun.ch/Network/Visualize_pcap_file_data for help with plotting pcap data.

NOTE : Students need to write responses to questions in both sections 2 and 3 to make their lab reports.