Networking Lab 1 Physical and Datalink Layers (Hardware)

Hubs are layer 1 devices. Every signal that comes in to a hub port is replicated out all other ports as if the ports are all soldered together. In the early '90s, hubs were at the heart of most Local Area Networks (LANs). The Application Specific Integrated Circuits (ASICs) that switches need have come down in price to the point where today switches are the core of LANs and it is difficult to find hubs.

Since hubs are seldom used, part of this lab is a history lesson—texts will probably talk about hubs for years to come. This lab will give you practice in setting IP addresses, and may help you understand switches better later.

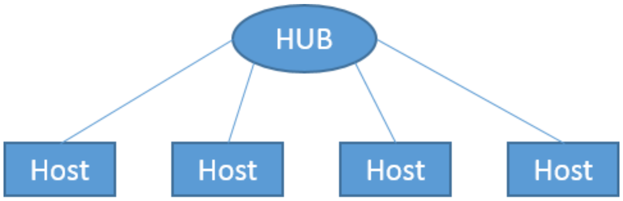
With hubs, each host must listen to make sure that no other hosts are talking before it tries to talk. Even so, there will still be times where two hosts talk at the same time and create a collision. The presence of a collision light is a way to tell a hub from a switch as only hubs have them. Collisions limit the total speed a network can reach—even though the hub and hosts are rated for 100 Mbs, collisions during heavy traffic will limit the maximum rate to 50-70 Mbps.

BEFORE you disconnect from the network

For this lab you'll use ncat to generate traffic between workstations. The ncat application is installed along with nmap. Make sure that you have nmap installed on your computer. If not, download it here--https://nmap.org/download.html, look for “Latest stable release self-installer” in the Microsoft Windows Binaries section. In addition, make sure that your computer has Wireshark installed. If it is not already installed, you can download it at https://www.wireshark.org/#download.

Initial Setup

1) Break into groups of 3-5. Each group should have a hub. Remove your computer’s network cable from the school network and connect it to the hub.



2) Since we are no longer connected to the school network and its DHCP server that assigns IP addresses, we will need to configure our IP addresses manually. We'll use one of the private IP ranges, 10.0.0.0/8. Each person in the group should select a different x for the address 10.0.0.x, and let the others know what they will use.

If you use windows, the fastest way to reach the network control panel is to type `ncpa.cpl` at an elevated command prompt. Select properties for your Ethernet connection, then properties of Internet Protocol Version 4 (TCP/IPv4). Select the radio button for "Use the following IP address" and enter the IP address you selected (10.0.0.x). The subnet mask will automatically fill in with 255.0.0.0, which is fine for our purposes. The DNS server addresses can be left blank. You can find instructions in CyberAces_Module2-Networking-Layer3-Part3-Communication.pdf on page 13.

Watching traffic with netcat or ncat

3) Make sure you can ping the other members of your group and fix the problems if you can't. You may have to turn off your firewalls to allow people to ping your hosts. You can use an elevated command prompt and `NetSh Advfirewall set allprofiles state off`. You can use the GUI if you wish—use your favorite search engine to learn how.
   Note: We will use ncat to send traffic to each other. The network mapping application, nmap, includes ncat. Download it from https://nmap.org/download.html.

Record your MAC address. In windows use `ipconfig /all` and look for the physical address. Share your IP and MAC addresses with the members of your group and put them in a table so you can use it in the next step.

Name (Joe, Jill, etc.)	IP Address	MAC address	Hub/switch port number

4) Everyone in the group should start a packet capture in Wireshark. Windows is chatty, so you will see traffic even though you are isolated from the school network and even when no one is issuing commands.
5) Two people in the group should use ncat to send messages to each other.
   a. One person needs to set their ncat to listen on a TCP port (this is what a server does; listen for connections.) For the port number, choose a number between 2000 and 65,000. If you don't choose a port, ncat defaults to 31337. If I chose port 3000, I would enter this. (The lower case "L" means listen.)
   ```
   ncat -l 3000
   ```
   b. The other person needs to use ncat to connect to the first person's listener (this is what a client does; connect to a server.) You need to know the other person's IP address and the port number they are listening on. For example, if the other person's IP is 10.0.0.4 and they are listening on port 3000, you would enter this.
   ```
   ncat 10.0.0.4 3000
   ```
   c. Now that the pair have connected with ncat, they should be able to chat back and forth.
   d. Everyone should be able to find the messages captured in Wireshark, whether they are involved in the conversation or not. Remember that a hub sends everything it hears out all ports, which means anyone can eavesdrop on the converstation. Once you find one of the packets between the two people in Wireshark, right-click one of the packets and select "follow TCP stream." This will open a second window showing the contents of that TCP conversation.
6) Take turns with different people sending messages, so that everyone gets to talk, listen, and eavesdrop.
7) Find the MAC (Ethernet) and IP source and destination addresses of the traffic in Wireshark. Check the addresses against the table you made to make sure they agree.
8) **For Hand in:**
   a. How much privacy is there for unencrypted traffic through a hub?

    b. Why?
    c. What network topology did you use for this lab?
    d. What network topology does our normal school lab use?

Introduction to Layer 2 Switches

1) Replace your hub with a switch
2) Verify that you can still ping each other
3) Repeat steps 4-8 above. This time, you should not be able to eavesdrop on the netcat connections between other users. Review page 4 of CyberAces_Module2-Networking-Layer2_20150129.pdf.
4) It would take a while to set up your VM to connect to the serial console of the switch for management, so ask the instructor to connect their laptop to the switch. The instructor will issue the command, *show mac address* (Cisco switches), to show you the MAC address table for the switch. Your computer MAC addresses should all be present, and the port numbers for the MAC addresses should match those in the table you filled in.
5) **For Hand in:**
    a. How much privacy is there for unencrypted traffic through a switch?
    b. Why?
    c. How does a switch know which port it should send traffic to?

Return the lab to its normal state.

1) Change your IP addresses back to DHCP. In Windows, select "Obtain an IP address automatically" in the TCP/IPv4 window. In Linux, change the Network GUI back to DHCP. If you used ifconfig in Linux, reboot, or restart networking by entering "sudo service network restart".
2) Turn your firewalls back on. If you turned the firewall off in a GUI you'll need to go to the GUI to turn it back on. If you used the command line you can reboot, or use
```
NetSh Advfirewall set allprofiles state on
```
3) Connect your Ethernet cables back to the school network.