# Networking Lab 1 Physical and Datalink Layers

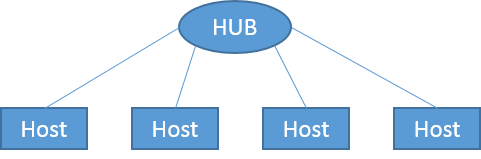
Hubs are layer 1 devices. Every signal that comes in to a hub port is replicated out all other ports as if the ports are all soldered together. In the early '90s, hubs were at the heart of most Local Area Networks (LANs). Application Specific Integrated Circuits (ASICs) have come down in price to the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

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. 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.

For this lab you'll use either ncat (Windows and Linux, installed along with nmap) or netcat (nc in Linux.) If you want to use your Windows computer, make sure that you have installed nmap so that you'll be able to use ncat—do this BEFORE you disconnect from the network. If you use Linux, both ncat (installed in a previous lab using sudo apt-get nmap) and netcat (nc) should be there. In either case, make sure that your computer has Wireshark installed.

## 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'll 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*" (without the quotes) 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. 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\_20150129.pdf on page 13.

Instructions for setting the IP address in CentOS using the GUI are in the same module, page 14. You may be able to temporarily set the address using the command, “*sudo ifconfig eth0 10.0.0.x netmask 255.0.0.0”* (substitute the number you selected for x.) Note: Linux servers normally do not have the GUI installed. Permanent address changes are made by editing /etc/sysconfig/network-scripts/ifcfg-eth0 (in CentOS—Debian/Ubuntu is different.) If you want to practice that, you’ll need to disable the GUI, Network Manager, or else it will fight you. The command is “*sudo service NetworkManager stop*.”

# Watching traffic with netcat or ncat

1. If you are using a virtual machine for this exercise, set its network adapter to “Bridged.” 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. Linux users can turn off their firewalls with, “*sudo service iptables stop*.” Windows users can use an elevated command prompt and “*NetSh Advfirewall set allprofiles state off*.” Both CentOS and Windows users can use the GUI if they wish—use your favorite search engine to learn how.
2. Record your MAC address. In windows use "ipconfig /all" and look for the physical address. In Linux, use "ifconfig" and look for the HWaddr. 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.
3. Everyone in the group should start a packet capture in Wireshark. Windows is fairly chatty, so you will see traffic even though you are isolated from the school network and even when no one is issuing commands.
4. Two people in the group should use nc (CentOS or Kali) or ncat (Windows with nmap installed) to send messages to each other. Everyone should be able to find the messages captured in Wireshark. 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.
5. Take turns with different people sending messages, so that everyone gets to talk and listen for traffic.
6. 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.
7. **For Hand in:**
   1. How much privacy is there for unencrypted traffic through a hub?
   2. Why?
   3. What network topology did you use for this lab?
   4. 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 6-8 above. This time, you should not be able to spy 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.

# Return the lab to its normal state.

1. If you used a VM and set its network adapter to “Bridged”, set it back to “NAT.”
2. 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".
3. 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 (Windows) “*NetSh Advfirewall set allprofiles state on*” or (Linux) “*sudo service iptables start.”*