Basics Experiment

A. Objective
  1. Understand the wiring infrastructure of the Internet Teaching Lab (ITL)
  2. Find out the Ethernet and IP addresses of your host station
  3. Test connectivity between your computers
  4. Monitor traffic at specific ports

B. Configuration and Network Setup
  1. Use the existing setup at the ITL lab. Refer to the ITL Lab Manual at
     http://linux.cs.sonoma.edu/itl/manual/contents.html

C. Procedure
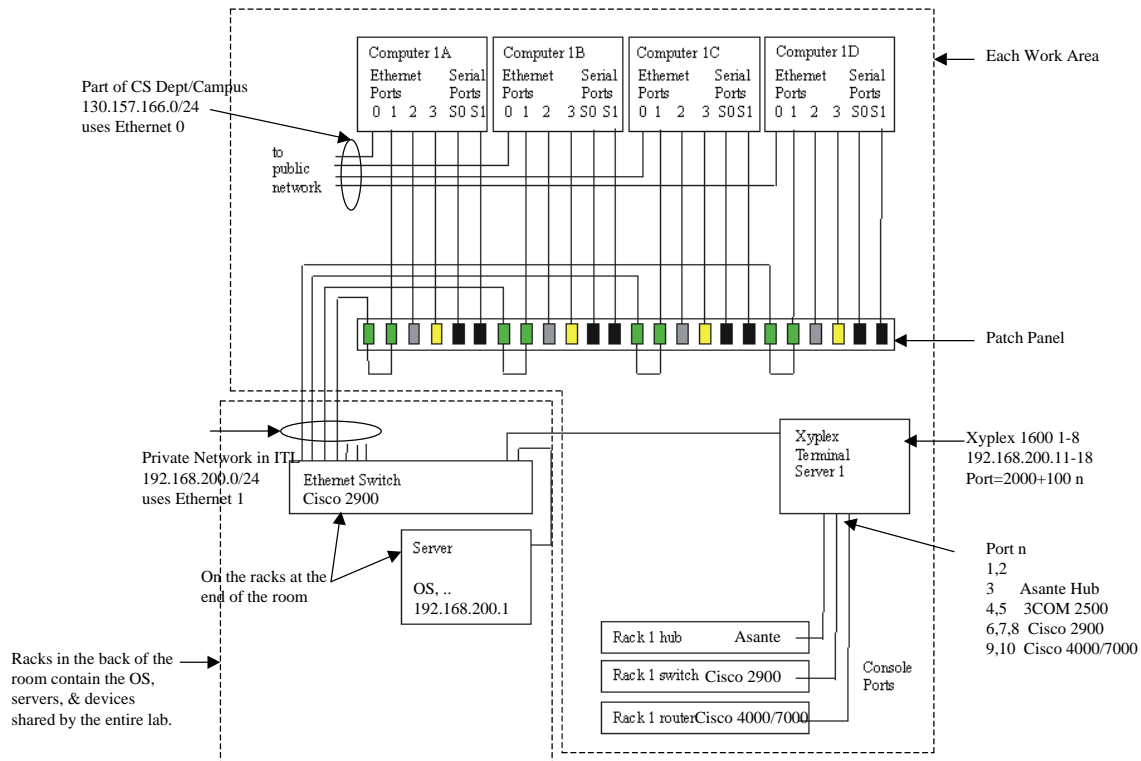1. Study the wiring diagram of your Work Area as shown in Figure1.

Figure 1.   Wiring diagram of Work Area 1.

2. Boot the computer in the **itl-linux** mode. Using the **ifconfig** command, determine
   - The active interfaces of the computer at your station. Note that there are several interfaces.
   - Ethernet and IP addresses of the active interfaces.

- The corresponding Subnet Masks[1].

3. Use exactly 5 **ping**s to eth1 of your computer and check the connectivity. Refer to "**man ping**" for the command format. How long does it take to receive the response? Record min/average/max/mdev of your result.

4. Use the "**ifconfig**" command to attach to eth2 of your computer the IP address 192.168.0.x. You need to go to the root level for the configuration using the "**sudo command**" or the "**su root**" command (see the ITL manual). The instructor can provide you with the password for this. For the eth2 *ipaddress*, use 192.168.0.x, where "x" is the computer number ya, yb, yc, and yd in the decimal for the Work Area y.

     E.g. for Work Area 1, use
        1a=1*16 + 10 = 26
        1b=1*16 + 11 = 27
        1c=1*16 + 12 = 28
        1d=1*16 + 13 = 29

5. Use the "**ifup eth2**" command to make sure that eth2 is up. "**ifdown eth2**" can bring it down.

6. Display the configuration of all the interfaces using the "**ifconfig**" command to make sure that interfaces eth1 and eth2 are both up.

7. Record the Ethernet and IP addresses of the eht2 interface.

8. **Ping** (5 pings) between your computer and the eth1 of another computer in your Work Area. What do you observe? What is the response to the **Ping** command? Record the data.

9. **Ping** (5 pings) between your computer and the eth2 of another computer in your Work Area. What do you observe? What is the response to the **Ping** command? Record the data.

10. In the following sections use the "**ethereal**" as a protocol analyzer to monitor the traffic. Refer to the ITL Lab Manual (i.e., Useful Computer Applications) and "**man ethereal**" for the command format and the filter. Note the data displayed in the three ethereal panels for your interpretation.
    - List of the packets in the top panel.
    - Logical structure of the packets in the middle panel.
    - Content of the packets in the bottom panel.

11. For this part you can work in a group of two in your work area. In order to generate some traffic at eth1 port, you can ask your partner to continuously **ping** the eth1 interface of your computer with a packet size of <u>100 bytes</u> and packet content of all **ff**. Capture the ping traffic at the eth1 interface. The filter in this case would be "**icmp**" since **ping** is an **icmp** packet. For each ping packet there is a pair of **request** and **response** packets. Select one of the request packets and identify its individual

---

[1] The bits in the subnet mask and the Internet address have a one to one correspondence. The bits of the subnet mask are set to 1 (one) if the system examining the address should treat the corresponding bit in the IP address as part of the extended network prefix. The bits in the mask are set to 0 (zero) if the system should treat the bit as part of the host number. We will discuss the subnet mask later in the IP-Lab session.

components using the ethereal panels. Record your results for the details of the packet. Can you locate the packet content of all **ff**?

12. For this part we would like to access a website, e.g., cisco.com, via the eth0 interface of your computer. Prepare your computer to capture ping packets at the eth0 interface and **ping** the website with a few packets and capture the packets.   Identify a packet with the content of "web site. What is the ip address of the server of the web site? Record your results.

D. Report
   1. Answer all the questions in the procedure section above.
   2. Interpret the data you captured in the ethereal panels. Did you expect such a result?
   3. From the subnet mask in section C2, determine the number of hosts the subnet (that the host is connected to) can accommodate.