CS 326e F2002
Lab 1. Basic Network Setup & Ethereal
Time: 2 hrs

Tasks:

1 – (10 min) Verify that TCP/IP is installed on each of the computers

2 – (10 min) Connect the computers together via a switch

3 – (10 min) Observe the configuration of each of the NICs for each computer

4 – (10 min) Statically configure an IP address and subnet mask for each computer

5 – (15 min) Verify connections in your network with ping

6 – (15 min) Examine non-existent IP address and subnet conflicts

7 – (15 min) Introducing Ethereal, a packet capture tool
    7B – Examine packet capture on a Hub

8 – Sniffing the network for passwords with Ethereal

Each team of two students will use the following components for this experiment:

<table>
<thead>
<tr>
<th>2 computers with Microsoft Windows 2000 Professional</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Cisco Systems Catalyst 2900 Series Switch</td>
</tr>
<tr>
<td>and 1 Cisco Systems Fast Hub 400</td>
</tr>
<tr>
<td>2 Ethernet Cables</td>
</tr>
<tr>
<td>Ethereal Network Analyzer Software</td>
</tr>
</tbody>
</table>

Each student will be in command of one computer.

Task 1 - Verify that TCP/IP is installed on each of the computers

1. Looking at the desktop window, find the icon labeled My Network Places. Right click on this icon and select "Properties."

2. A window named “Network and Dial-up Connections” will appear with an icon named Local Area Connection. Right click on this icon and again select "Properties."

3. Another window called "Local Area Connection Properties" will appear that has a white area with three items listed. One of these should be Internet Protocol (TCP/IP). Verify that this item is checked. If it is not, please do so.
4. Select OK to exit

**Task 2 - Connect the computers together via a switch**

1. Observe the icon Local Area Connection in "Network and Dial-up Connections". We will compare this icon to that in step 7.

2. In the back of the computer there will be a slot that looks much like a phone cord slot. This is actually an RJ-45 connection that is meant for Ethernet cables. This port is part of a card that is plugged into the motherboard of the system. It is commonly referred to as a NIC, or Network Interface Controller. The card that you will be using is capable of transfers up to 100 Megabits per second, also referred to as the transfer rate.

3. Each computer has been supplied with one Ethernet cable. Plug one end of this cable into the RJ-45 port. Listen for a click from the end of the cable to tell you that it is plugged in all the way.

4. Locate the switch that has also been supplied. There is one switch for each group of two computers. Plug the other end of the Ethernet cable into one of the ports on the switch. The ordering of ports does not matter.

5. Turn on the switch when all computers have been plugged in.

6. The switch will go through a boot up process, so there will be a sequence of lights switching on and off. These lights will begin as orange, and for the ports that are connected correctly, they will turn green after the boot up sequence is completed. Verify that the ports that are connected do indeed turn green.

7. Observe the difference in the Local Area Connection icon.

**Task 3 - Observe the configuration of the NIC(s) for each computer**

1. Click on the Start button at the lower left of the computer screen and select "Run..."

2. In the field, type cmd This will allow for a command prompt window to appear.

3. Type in ipconfig /all and press enter.

4. There is a lot of information that is returned, but we are interested in only a few items at this time. In particular, we would like to know whether DHCP is enabled, the IP address of the interface, and the Subnet Mask. Fill in the following table with values from the information that is returned.

<table>
<thead>
<tr>
<th>DHCP enabled?</th>
<th>IP address of interface</th>
<th>Subnet Mask</th>
</tr>
</thead>
</table>

Dynamic Host Configuration Protocol (DHCP) is a protocol that is used to allocate an IP address to each interface that requests one. In particular, a DHCP server sends this information to the DHCP client. In our current setup, there is no such server. Configuring IP addresses will, thus, need to be done manually.
Task 4 - Statically configure an IP address and subnet mask for each computer

1. Again navigate to "Local Area Connection Properties" as in Task 1.
2. Double click "Internet Protocol (TCP/IP)". Select *Use the following IP address.*
3. Input to the fields the IP address shown on the top of the monitor. Clear the Default Gateway and DNS Server fields and click on OK for both windows.
4. Verify that the IP Address for the computer has indeed changed. To do this, execute the "ipconfig /all" command again.

Task 5 - Verify connections in your network with ping

Once each of you have set up the configuration correctly, it is time to verify that all computers are on the same network, and can indeed communicate with each other. There is one commonly used command that can verify communication between hosts. This command is called ping.

1. Connect your team's switch with another team's via a crossover cable provided by the lab proctor (in order to ping all 4 hosts).
2. Type `ping X` in the command prompt where `X` is one of the IP addresses of the four computers in your network.
3. Repeat for each of the four IP addresses.
4. Fill in the following table with values returned after each execution.

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Success</th>
<th>Time Out</th>
<th>Unreachable</th>
<th>Packet Sent</th>
<th>Packets Received</th>
<th>Packets Lost</th>
<th>Minimum RTT</th>
<th>Maximum RTT</th>
<th>Average RTT</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.0.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.0.6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.0.7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.0.8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Task 6 - Examine non-existent IP address and subnet conflicts

1. Change the IP addresses according to the following table. Note that the Subnet Mask remains the same as before.

<table>
<thead>
<tr>
<th>Computer 1</th>
<th>Computer 2</th>
<th>Computer 3</th>
<th>Computer 4</th>
<th>Subnet Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.10</td>
<td>192.168.0.11</td>
<td>192.168.1.12</td>
<td>192.168.2.13</td>
<td>255.255.255.0</td>
</tr>
</tbody>
</table>

2. Ping all 4 computers. Fill in the following table with values returned after each execution.

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Success</th>
<th>Time Out</th>
<th>Unreachable</th>
<th>Packet Sent</th>
<th>Packets Received</th>
<th>Packets Lost</th>
<th>Minimum RTT</th>
<th>Maximum RTT</th>
<th>Average RTT</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.0.11</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.1.12</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.2.13</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

3. Explain the results. Are they what you expected?

4. Ping an address that is in your subnet but is not connected, for example 192.168.0.253. Is the result different from the Step 2? Explain.

Task 7 - Introducing Ethereal

We will be running one particular application, Ethereal. It can capture all the packets that are transmitted to and from your Ethernet interface. Once it has finished capturing, it will display the packets in a list ordered by a value that can be changed like time, protocol, or source.

We will first capture network traffic generated by ping which uses ICMP (Internet Control Messaging Protocol).

1. Set the computers' IP addresses as follows.

<table>
<thead>
<tr>
<th>Computer 1</th>
<th>Computer 2</th>
<th>Computer 3</th>
<th>Computer 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>192.168.0.5</td>
<td>192.168.0.6</td>
<td>192.168.0.7</td>
</tr>
<tr>
<td>192.168.0.8</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Launch Ethereal. The icon is on the desktop.

2. To begin capturing packets, under the Capture menu choose Start.

3. Verify that the first, fourth, fifth, and sixth options after the Capture Length are selected.

4. Note that many packets can be collected within a short time after Capture is started. It is best to start capturing only right before you do a transfer of packets that you want to
analyze. In this case, you need to be ready to ping before start capturing. When you are ready, click OK to start collecting packets.

5. Ping all 4 hosts on the network.

6. Stop capturing by the click Stop button in Ethereal when you have completed pinging all the hosts click.

7. Wait until Ethereal loads all the captured packets onto the screen.

8. Order the packets according to Protocol by clicking on Protocol column heading.

9. Scroll down in the upper window to packets that are ICMP. Note that in the Info column, there are basically two types of ICMP packets that were transferred. What were these two types of ICMP packets?

10. Click on the first row of the ICMP packets. This should be a request packet and should have the source listed as the IP address/name of your computer, and the destination listed as the address/name you first pinged. The middle and bottom screens should have changed to represent the content of that particular packet. Note that the bottom screen is primarily listed as a hexadecimal representation of the binary bits of the packet, though the rightmost column also lists the contents in an ASCII format.

11. In the middle window, expand the content by clicking on the + within the boxes. Note that you can contract the content again by clicking on the - within the boxes.

12. Fill in the table below. All information can be found within the middle screen for this packet.
13. Now click on the second row of the ICMP packet. This should be the **reply** packet from the host that you pinged in the previous packet. Fill in the table below with the information for this reply packet.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source IPv4</td>
<td></td>
</tr>
<tr>
<td>Source MAC</td>
<td></td>
</tr>
<tr>
<td>Dest IPv4</td>
<td></td>
</tr>
<tr>
<td>Dest MAC</td>
<td></td>
</tr>
</tbody>
</table>

14. Note that when clicking on something in the middle of the screen the actual bits of the packet are highlighted in the bottom screen. This is both done in hexadecimal and in ASCII.

15. In ASCII, what are the 32 bytes of data that fill the end of either of these packets?

16. What packets besides those generated by ping do you see? What generated these packets?
**EXTRA CREDIT #1: Task 7B – Examine packet capture on a Hub**

In this experiment we will capture packets while connected to a hub instead of a switch and examine the differences between the results.

1. Remove each Ethernet plug from the switch and plug it into the Fast Hub 400. Push until you hear a click.
2. Ping your neighbor to verify that you can see them.
3. There will a long cord connecting the switches used in the last exercise. Remove this plug and place it in the Hub just as with the other cords. The Hub should already be on. Wait for each port to turn Green.
4. Prepare to ping the other computers before starting to capture packets.
5. Capture packets just like in Task 7 steps 2-7
6. Order the packets according to Protocol by clicking on Protocol column heading.
7. What packets besides those generated by ping do you see? How does this differ from the switches and why?

**EXTRA CREDIT #2: Task 8 – Sniffing application layer protocols using Ethereal**

This experiment requires the Windows 2000 PCs have Internet Information Services installed (specifically the FTP service). This has already been done for you on all the machines.

**Password sniffing**

1. Open a command prompt.
2. Start Ethereal to capture network traffic.
3. FTP to your partner’s PC.
4. Use user name = anonymous, password = your email id.
5. Stop network traffic capturing in Ethereal.
6. Search for the packets where the password is found in plain text.