CS 356 Lab #1: Basic LAN Setup & Trace analysis using Ethereal

Tasks: Time: 2:00 hrs
(Task 1-6 should take 45 min; the rest of the time is for Ethereal)

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

2 - Connect the computers together via an Ethernet switch

3 - Observe the configuration of each of the Network Interfaces for each computer

4 - Statically configure an IP address and subnet mask for each computer

5 - Verify connectivity in your network with ping

6 - Examine non-existent IP address and subnet conflicts

7 - Capturing and Analyzing Application layer packets using Ethereal

The components that will be used for this experiment are as follows:

| 2 computers (each w/ Microsoft Windows 2000 Professional and w/ 2 Ethernet cards but you will use only one Ethernet) |
| 1 Cisco Systems Catalyst 2900 Series Ethernet Switch |
| 2 Ethernet Cables, 1 crossover cable per 2 teams |
| Ethereal Network Analyzer Software |
| Web Server, FTP server, Web Browser |

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. (First disable the NIL 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 an Ethernet switch**

1. Observe the icon **Local Area Connection** in “Network and Dial-up Connections”. We will compare this with what happens after the computers are connected (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 **transmission 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 Ethernet 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 Ethernet switch when all computers have been plugged in.

6. The Ethernet 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. What’s different about the Local Area Connection icon?

**Task 3 - Observe the configuration of the Network Interface Cards (NICs) 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**, which 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, and the IP address of the interface, and the Subnet Mask. (The text uses the term **Network Mask** instead of 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>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Task 4 - Statically configure an IP address and subnet mask for each computer (Configuring IP addresses will, thus, need to be done manually.)

1. Again navigate to "Local Area Connection Properties" as in the 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 “wallpaper” of the monitor. Set the Subnet mask to be 255.255.255.0. 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 connectivity in a larger network (2 teams) with ping
Once each of you has 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 Ethernet 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 (2 in your team’s and 2 in the other team’s network).

Task 6 - Examine non-existent IP address and subnet conflicts

1. Wait for everyone to reach this step, then, 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. Why were you not able to reach some of the computers? Explain.

4. Ping an address that is in your subnet but is not connected (i.e an address that matches your current subnet but with an address that we know does not exist). What is the result and how is it different from the result of the above step?

**Task 7 – Capturing and Analyzing Application layer messages and TCP segments using Ethereal**

We will be using Ethereal to capture and analyze the packets that are generated when we run a network application on the networked machines. The applications we will be running are a Web Server and a Web Browser. These applications make use of the HTTP protocol. The second application we will be running is an FTP server and a FTP client. We shall see the difference in these protocols by analyzing the packets that we capture.

**HTTP protocol:**

1. Each group must designate one machine as the Web Server machine. (Say Machine 1 and 3, machines 2 and 4 will then be the client machines).

2. Confirm that the Web Server is running on the server machine by going to Control Panel | Services, and check for Web service as being ‘started’.

3. Start a browser on the client machine.


5. Start capturing packets by clicking on the menu Capture → Start.

6. Verify that the first, fourth, fifth, and sixth options after the Capture Length are selected. Switch the Interface to the second choice, which represents the 2nd Ethernet card.

7. Click on Ok to start capturing packets.

8. Type in the following URL into the address bar of the browser

9. Once the browser displays the entire page on the browser, stop capturing packets in Ethereal by clicking on the Stop button in the Ethereal window. How many images does the web page have???

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

11. View the packets that have been captured by Ethereal. There may be some other protocol packets that were also captured. You can sort the packets by clicking on the protocol heading in the list-view of the Ethereal window.

12. The Ethereal window is divided into 3 parts. The top displays the captured packets. The middle displays the encapsulated headers (for each layer) and their values for the selected packet. The bottom part displays the actual raw bytes from the packet (in hex).
13. Did the client's TCP piggyback the ack found in the 3\textsuperscript{rd} segment of the 3 way handshake onto the data message, i.e. the HTTP GET request message?

14. What is the client TCP's sender window size once the connection is established?

15. How many TCP connections were opened to fetch the page (and images)? How were the images fetched, were any optimizations performed in fetching the images? (If the connection is persistent, then is pipelining used?) Cite the data you found to support your observations:

16. **Comparing the difference between a persistent connection and non-persistent connection:** Turn off HTTP 1.1 in the browser. In IE this is done by going to Tools | Internet Options | Advanced Tab, scroll down to the HTTP 1.1 settings, uncheck Use HTTP 1.1.

17. On the server turn off HTTP keep-alive. This is done by going to Control Panel | Administrative Tools | Internet Services Manager. Expand the tree on the left of the window that comes up. Right click on Default Web Site and go to the properties. Select the Web Site tab and uncheck the HTTP Keep-Alives enabled check box. Click **OK**.

18. Clear the browser cache. On IE this is done by going to Tools | Internet Options…| General Tab, click on Delete Files in the Temporary internet files section. In the window that pops up check Delete all offline content and press OK. Press OK on the General Tab.


20. How many connections were opened to fetch the page (and images)? How does this example compare to the time-space diagrams we drew in class and in Exam 1. Does the browser open multiple concurrent connections?
FTP protocol (if time):
1. Choose one of the machines as the FTP server (switch machines from the previous task, i.e. use the server machine as the client now and vice versa). Confirm that the FTP server is running on the machine by going to Control Panel | Services, and check for FTP Publishing service as being 'started'.
2. Run Ethereal and start capturing packets.
3. Bring up the command prompt on the client machine, by choosing the windows Start | Run. Type in cmd <Enter>.
4. Type cd c:\temp <Enter> at the command prompt.
5. Type ftp ip_address_of_server_machine <enter>
6. When prompted for user name type anonymous
7. When prompted for password type any valid email id.
8. Once at the ftp> prompt, type get index.html <enter>
9. The index.html file will be fetched and stored in the c:\temp directory on the client machine.
10. Type bin to change over to binary mode.
11. Type get oe_a01.gif <enter>.
12. Exit the ftp client by typing quit at the ftp> prompt.
13. Stop capturing packets in Ethereal on both machines by clicking on the Stop button in the Ethereal window.
14. Wait until Ethereal loads all the captured packets onto the screen.
15. View the packets captured in the Ethereal window.
16. Which side initiated creating the TCP data connections? What FTP command was used to initiate the TCP 3way handshake?
17. What port numbers were used for the client and the server for:
   a. Control :
   b. Data connection 1:
   c. Data Connection 2:

If time, explore what you wish.... Here are some ideas.
1. What other protocols did Ethereal capture as you were running Ethereal in Task 7? Can you guess what these protocols do?
2. Looking back to Task 2, step 6, repeat this task using Ethereal to capture any packets related to the switch’s “boot up sequence”.