Southern Polytechnic State University

Electrical and Computer Engineering Technology Program

ECET 4820 Laboratory Exercise: Ethernet Basics

Objective:

The student will observe characteristics of Ethernet LAN operation.

Introduction:

You will work with an Ethernet LAN that has several active workstations on it. The LAN will be isolated from the outside world by disconnecting the interface cable to the campus network. By examining network traffic with a LAN protocol analyzer, you will identify the MAC (hardware) addresses of the workstation Ethernet NICs. In the first part of the lab exercise, the workstations are connected to a 10 Mbps shared hub. In the second part, they are to a 100 Mbps switch. You will be asked to observe and comment on performance differences.

Procedure:

Set Up Workstation TCP/IP Communication Protocol

1. Configure your IP protocol stack.
   a) Boot to Windows using the user name and password supplied by your instructor. Make sure you are logging in *locally* to your computer and *are not* logging into a domain.
   b) Bring up the network properties dialog box and configure your workstation IP address manually or choose DHCP. Verify connectivity to the lab LAN.
   c) Double-click on the **My Network Places** icon. You should see icons for each of the active workstations.

Identify Workstation MAC Addresses

2. The first part of this lab exercise will be performed with all workstations connected to an Ethernet hub, which acts like a repeater. The pairs of workstations will work together to generate network traffic. By observing the traffic using Wireshark, a table of the lab workstation MAC addresses will be created. Workstations 1 and 2 of each pair should perform the steps below at the same time.
   a. Set up an appropriate capture filter for Wireshark if desired and use the Ping utility to send Ethernet frames to four of the other active workstations in the lab. Ping operates at the IP layer, but an Ethernet frame is created with the Ping packet as the payload. The Ethernet frame will have its own source and destination addresses.
   b. By capturing the Pings, you can determine the Ethernet addresses of the other workstations as well as your own. Fig. 1 shows the fields in a standard Ethernet frame. Fill in Table 1 with the workstation addresses. Use one of the captured pings to verify the fields in the Ethernet frame.

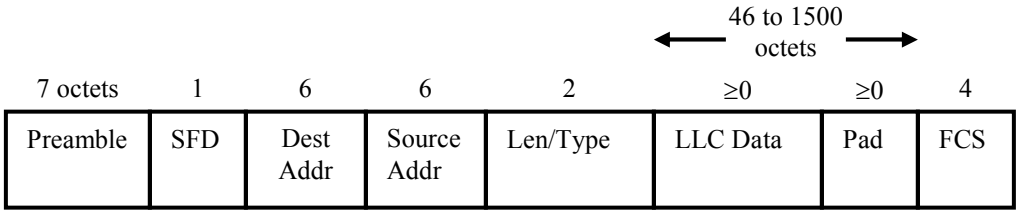

Fig. 1 Ethernet frame format.

Table 1. Workstation Ethernet addresses

Workstation Name	IP Address	Ethernet Address

c. Verify your table data by displaying the arp cache using the arp –a command from the command prompt. You may have to run the command prompt as administrator. To do this, right click on the command prompt icon and select **run as administrator**.

Analyzing Files on the Network

3. Collaborate with another student or group at another workstation and identify one workstation as Workstation 1 and another as Workstation 2. Workstation 1 of each pair will send its text file to Workstation 2 and students at both Workstations will determine the content of the file.

Workstation 1:

a) You will create a small text file (.txt) using the Notepad application to be sent across the network for traffic monitoring purposes.

i) Set up a shared folder on your Windows partition called "**Shares**." Put it on the c:\ directory. Right click on the folder and choose **Share with→Specific people**. Then in the **File Sharing** box, choose the down arrow next to the **Add** button and pick **Everyone**. This will share your folder with all other users on the workgroup or domain.

ii) Create your text file and save it in the c:\shares folder.

Workstation 2:

b) Set up a shared folder called "**Shares**" on your Windows. **Do not put the folder in any other partition.**

c) Use Wireshark to monitor the network. If you want, you can set up a capture filter to minimize the extra frames captured.

   i) Start a Wireshark capture on both workstations.

   ii) Ask Workstation 1 in your pair to transfer their text file to your shared folder.

Both Workstations:

d) Once the transfer is complete, both workstations should stop their captures and examine the captured frames.

e) Use the **Packet Details Pane** and the **Packet Bytes Pane** to read the text file contents.

f) **Have your instructor verify your results.**

4. Repeat this file transfer using tftp. One workstation will run the tftp server and the other will run the tftp client and download the file from the server. Note that Windows may not automatically install the tftp client utility. You can find out by opening a command prompt and typing **tftp <Enter>**. If the error message says the command is not recognized, then tftp is not installed. To install it, go to the **Control Panel→Programs and Features→Turn** Windows features on and off and check the TFTP Client box when the list is populated. Note that you may have to disable firewalls or create exceptions for the tftp file transfer to work.

   a) Start the tftp server on the server workstation. Your instructor will tell you which server program to use

   b) In the server program, change the server's source directory to the one with the text file you created earlier.

   c) Prepare to restart a Wireshark capture on each computer but wait to start it just before entering the tftp get command on the client as described below.

   d) Open a command prompt window on the client computer and change directory to your desktop folder. The prompt will look something like this:

      c:\users\username\Desktop>

      where *username* is the username you logged on with.

   e) Enter the following command but start the Wireshark capture before pressing **Enter**.

      tftp *hostaddress* get *filename*

      where hostaddress is the ip address of the server computer and filename is the name of the file you are transferring

   f) Observe your capture buffer and see if you can find the file contents.

   e) Delete the file on the client's desktop and close the tftp server application when you are done.

Determining File Transfer Time on 10Mbps Hub

4. To avoid the effect of collisions on file transfers, your instructor will transfer a large file to another workstation. You will observe the approximate transfer time using the capture time tags Wireshark logs for each frame it captures. Alternatively, your instructor may use the iperf utility to send generic TCP traffic across the LAN.

a) Set up a Wireshark capture with a buffer size of 20 Mbytes (the default is 1 Mbyte). Set up a capture filter to capture traffic *from* (download direction only) the instructor's workstation.

b) Your instructor will inform you to start capturing just before the file transfer takes place.

c) At the end of the transfer, stop capturing and display the buffer.

d) Display statistics that inform you many packets were captured.

Number of packets captured: _____

e) Using the time tags and the known file size, determine the effective network capacity in bits per second.

Start time: _____

End time: _____

File transfer time: _____

Computed network capacity: _____

f) Use the Wireshark **IO Graph** in the **Statistics** menu to see if the bit rate you calculated matches the rate obtained from the graph. The **Statistics→Endpoints or Statistics→Conversations** also provides information that can be used to calculate the bit rate.

g) If you missed the file transfer, your instructor will repeat it.

Determining File Transfer Time on 100Mbps Switch

5. Move your workstation's Ethernet connection to the 100 Mbps switch. Your instructor will transfer the same file to each shared folder so you can capture it. Alternatively, your instructor may use iperf to send traffic on a TCP connection across the switch. In this case each student will run iperf as the client and the instructor will have the server workstation. Each student will take turns with the file transfer or iperf connection.

   The iperf command for client operation is: iperf –c *ipaddress* –i 1and must be entered from the command prompt window. Where *ipaddress* is the address of the server workstation. The –i 1 option tells iperf to print out updates every 1 second on your screen. You may have to navigate to the folder where iperf is located.

   Start time: _____

   End time: _____

   File transfer time: _____

   Computed network capacity: _____

   a) Did each group see the file transfer?

b) If not, your instructor will repeat the transfer by sending the file directly to your workstation.

Questions

1. What were the approximate transfer rates in bps for the file transfers across the hub and the switch? Compare your calculations with the IO Graph or other Wireshark statistics results.
2. Could all workstations see the file transfer on the switch? Why or why not?
3. Which of the two devices, the switch or hub, has the better security? Why?
4. What is the difference between how the switch and the hub operate?
5. If Wireshark missed some frames in the middle of the file transfer, is your capacity calculation valid? Why or why not?

Report

Each pair of students should analyze their data and prepare one brief, concise report. Answer the questions in the procedure and make meaningful conclusions about what you learned.

.