Southern Polytechnic State University

Electrical and Computer Engineering Technology Department

ECET 4820 Laboratory Exercise: Introduction to Network Analyzers

Objective:

Students will investigate some of the capabilities of a LAN network analyzer.

Background:

Network analyzers are useful tools for managing and troubleshooting network problems. They come in various configurations and capabilities. You are going to use Wireshark, an open-source, workstation-based analyzer. This analyzer has many capabilities to help you analyze network traffic and performance.

The workstation Ethernet card is used in "promiscuous" mode, which configures it to respond to all MAC addresses, not just its own. All incoming frames are passed up through the protocol stack regardless of MAC address. The Wireshark application analyzes the frame contents and extracts information about the higher-layer protocols. Frames can be captured and their contents analyzed on an individual basis. Also, statistics can be compiled and displayed on-screen, showing network utilization, collisions, packet distributions by protocol, the number of multicasts, etc.

Overview:

Workstations are connected to an Ethernet hub so that all traffic can be observed on the shared medium. A router is connected to the hub and serves as the default gateway for your network. Fig. 1 shows the network topology.

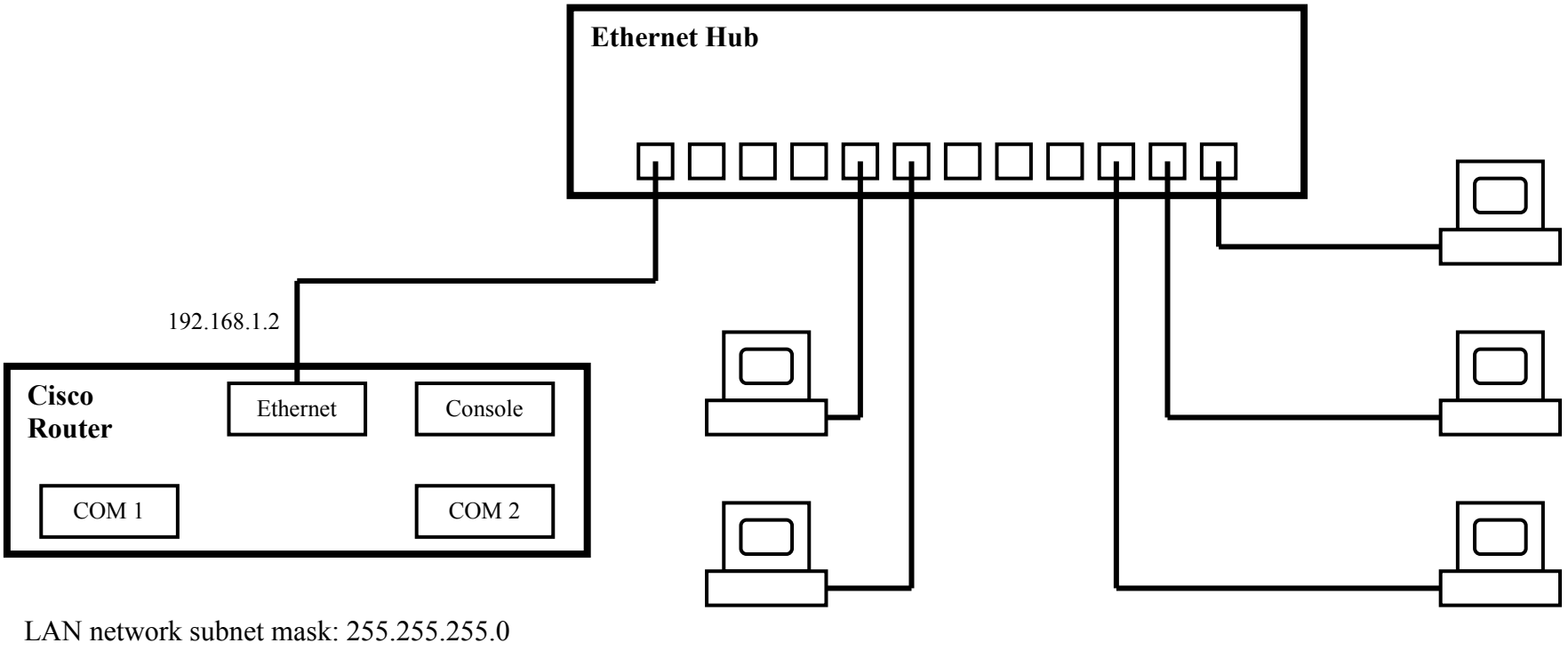
You will perform the following tasks.

1. Configure your workstation IP addresses as specified by your instructor.

2. Monitor network traffic under nominal conditions. Display protocol distributions and network utilization.

3. Capture some frames and examine the content of an ARP frame.

4. Design a filter to capture only Ethernet frames having the telnet TCP port (port 23) and see if you can read the password entered by your instructor when he/she logs on to the router.



Note: The workstations must be on the 192.168.1.0/24 network.

Fig. 1. Ethernet configuration.

Procedure:

Disconnect the Lab from the Campus Network

1. Ask your instructor to disconnect the lab from the campus network.

Boot Your Workstations and Configure IP address

2. a) Boot your workstations to Windows.

   b) Configure the workstation IP address, subnet mask, and default gateway as specified by your instructor.

Start Wireshark

3. Click **Start→Programs→Wireshark→Wireshark**. The program will start and some windows may be displayed. Maximize theWireshark window.

Setting Up and Starting a Capture

4. a) At the top of the Wireshark window, click **Capture→Interfaces.**

   b) Locate the Ethernet interface connected to the hub in the list of interfaces and click on its **Options** button.

   c) Look over the options available and make the following changes if they are not already selected.

   - Select 10 Mbytes for the **Buffer Size**
   - Under **Display Options**, make sure all options are checked.

   d) Click the **Start** button to begin capture. The display window will begin to list the captured packets.

Erase the ARP Cache and Generate ARP Traffic

5. We wish to generate some Address Resolution Protocol (ARP) traffic in order to capture it. To do so, it is a good idea to erase the ARP cache.

   a) To erase the cache, open a command prompt window and type **arp –d** .

   b) Now ping the default gateway or your neighbor's computer to generate an ARP broadcast and reply.

Examining Captured Frames

6. Let the capture session run for a while until you have at least 50 frames.

   a) At the top of the Wireshark window, click **Capture→Stop.**

   b) The Wireshark buffer window has three sections. The top section is the **Packet List Pane**. It lists the frames in the order they were captured. You will see the following columns.

Order number

Time

Ethernet MAC Source Address

Ethernet MAC Destination Address

Protocol (the type of protocol in the payload)

Info

Note that the **Time** format can be changed in the **View** menu.

The second section of the buffer window is the **Packet Details Pane**. It displays the detailed breakdown of the Ethernet frame selected in the **Packet List Pane**. It interprets the Ethernet frame parameters and the payload protocol parameters in an easy-to-read hierarchical format. The third section of the buffer window is the **Packet Bytes Pane**. It displays the frame contents in hexadecimal and ASCII format.

c) Click on an ARP frame in the **Packet List Pane**. ARP allows a source entity (computer or router) to find the hardware (MAC) address of its destination entity. The source is attempting to match its destination IP address that it does know to a destination MAC address that it does not know. The source broadcasts the request to all stations on the network (in our case it is an Ethernet broadcast). If the destination answers and gives its MAC address to the source, the source will use it from then on as its destination MAC address. Fig. 1 shows a Wireshark window where an ARP frame has been selected (frame number 423).

i) In the **Details Pane** for your ARP frame, find the source (sender) MAC address, source IP address, destination (target) MAC address, and destination IP address.

Source hardware address: _____

Source IP address: _____

Destination hardware address: _____

Destination IP address: _____

ii) Is your ARP frame a request or a reply?

ARP type: _____

Capturing Frames Using a Filter

7. You will set up Wireshark to capture only telnet traffic. To do this, you will need to design a filter that passes only telnet packets to the capture buffer and rejects all others. Your instructor will telnet from a workstation to your router and log in with a user name and password. Your task is to determine the password.

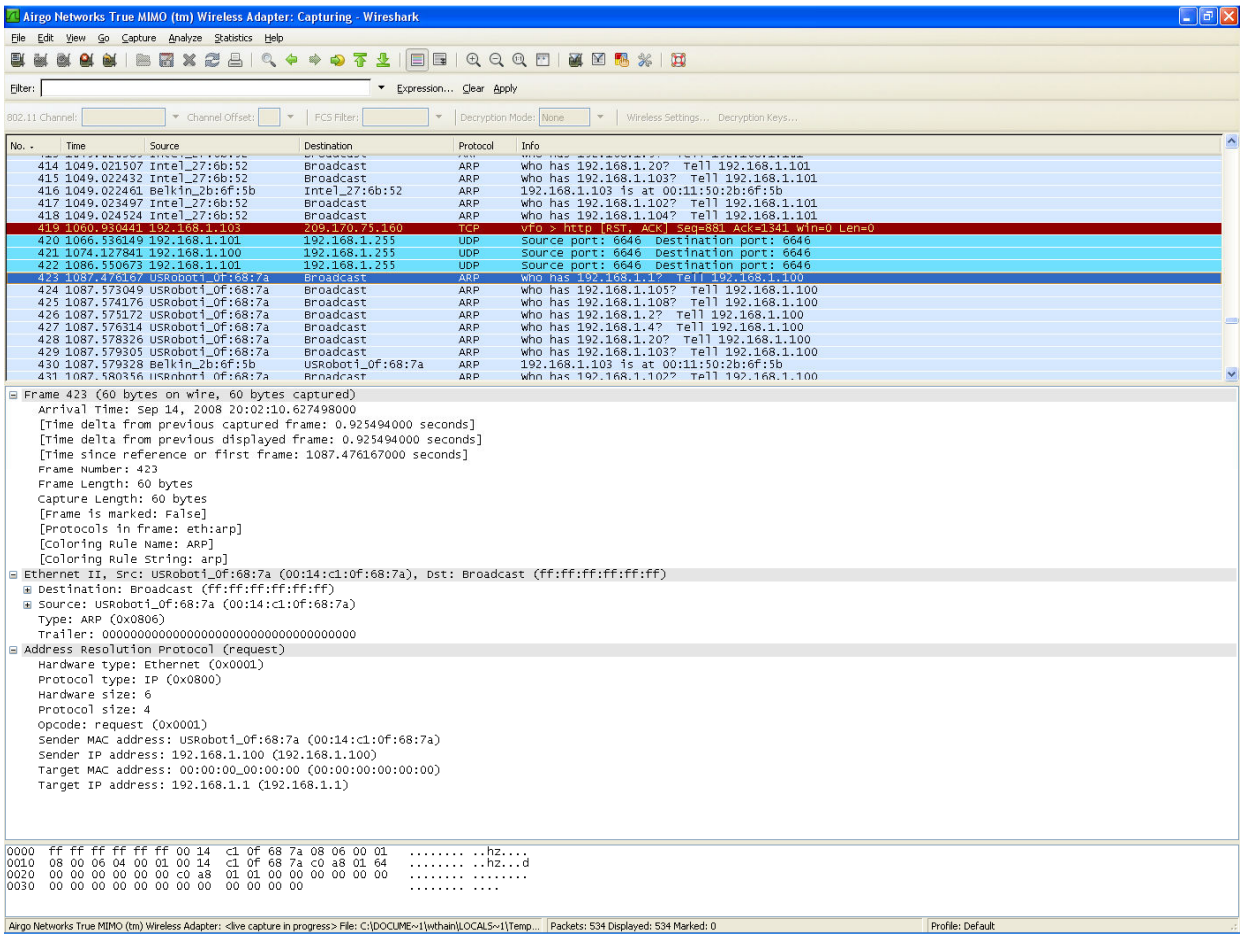


Fig. 1. Wireshark window with ARP frame selected.

a) At the top of the Wireshark window, click **Capture→Interfaces.**

b) In the **Capture Options** window, click the **Capture Filter** button. The **Capture Filter** window will open allowing you to either select or create and select a capture filter. You can select pre-designed filters from the **Filters** box, but you will create a new one. Your filter will capture only packets going to and from the router interface with IP address 192.168.1.2 and having TCP port number 23. This port number is associated with the Telnet protocol.

c) In the **Filter String** box type **host 192.168.1.2 and tcp port 23** .

d) In the **Filter Name** box type **Telnet Filter 1**.

- **Have your instructor verify your filter settings *before* you click OK to exit the Capture Filter box.**

e) Once you click OK and exit the **Capture Filter** box, you will return to the **Capture Options** box. Click **Start** to start capture.

f) At the top of the Wireshark window, click **Capture→Start.**

g) Your instructor will log on to the router using Telnet. When he/she is done, stop your capture.

h) Examine the **Details Pane** in the capture buffer display. Starting at the beginning of the buffer, scan down the buffer contents and look at the **Info** column. You will see the interpretation of the Telnet portion of the TCP segment. Determine the router user name and password and fill them in below. If the

Router user name: _____

Router password: _____

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

j) Delete your **Telnet Filter 1** filter as follows.

i) Click **Capture→Interfaces.**

ii) Click **Options** next to your Ethernet interface.

iii) Click Capture Filter

iv) Select **Telnet Filter 1** in the **Filters** box and click **Delete**.

v) **Have your instructor verify that you deleted the filter**.

vi) Then click OK to return to the Capture Options box. Stay here. You will start capturing again later.

Examine Capture Statistics

You will start another capture and this time you will examine some typical statistics.

8. a) Start a new capture without using a filter. Stop after you have captured at least 100 frames.

b) Click **Statistics→Protocol Hierarchy**. What are the percentages of IP and UDP frames?

IP percentage: _____

UDP percentage: _____

c) Click **Statistics→IO Graphs**. Your instructor will send a file across the network for you to capture. Determine the highest number of bytes captured in a 1 second interval.

Maximum Bits/second: _____

d) Click **Statistics→Endpoints**. Determine the IP address receiving the most packets and the one sending the most packets and the number of packets in each case.

Most packets received address and number of packets: _____

Most packets sent address and number of packets:: _____

Restore Your TCP/IP Settings

9. Restore the original TCP/IP settings you had on your computer when you started the lab exercise. **Have your instructor verify this.**

Questions:

1. You are a network administrator. What is the importance of monitoring network utilization statistics?
2. You are a network administrator in a small company. One of the engineers outside your network support group wants to install Wireshark on their computer. Should you let them? Why or why not?
3. Comment on the security issues concerning using Telnet to access remote computers.
4. What is the advantage of using capture filters?

Conclusions:

Bring together the concepts illustrated in the lab and make conclusions as to what they mean, and what you learned.