EECS 563
Project 3
Network Protocol Analysis

Provide your results in the form of a technical report using the provided format.
See: **Technical Report Format**

Also see this paper for advice on writing technical reports.
See: **Paper on writing technical reports**
Do not pad your reports, all figures and tables must be discussed in the text.

The purpose of this project is to use a network protocol analyzer, Wireshark, to examine packet sequences and contents for IP protocols, specifically, ICMP and ARP. While Wireshark is available on the EECS computers I recommend you install on your own computer so you can run Wireshark as administrator. You can also download and run Wireshark on your own machine. Wireshark can be downloaded from wireshark.org. If you install on your own machine; you need to install and run Wireshark as administrator.

ICMP
Use Wireshark and Ping to examine transmit and received ICMP packets. In this class you **must** run Wireshark with the promiscuous mode turned **off**.

Approximate Process:

a) Start Wireshark
b) Confirm that the capture of packets is NOT in promiscuous mode. Under the Capture tab the Enable promiscuous mode on all interfaces is NOT checked.
c) Under capture → options select the interface your computer uses to send and receive packets.
d) Type icmp into the capture filter field. Press enter
e) Click start
f) Get one round trip time to www.google.com using ping,
    ping –n 1 www.google.com
    To force ping to use IPv4 use ping –n 1 www.google.com -4
g) Under Capture → stop Wireshark
h) Save results
i) Repeat for ping –n 1 –l 256 www.google.com (it is –l 16, -l is length option, not -1 [one])
j) The files from parts h) and i) are used to report the results.

Address the issues below in your report.

1) Report the contents of the Frame, Ethertnet, IP, and ICMP packets for the default and 256 byte ICMP packets
2) Report the length of the default ICMP packet, what is the length of the corresponding IP and frame on the wire. Report lengths in bytes.
3) Repeat 1) for the -l 256 case.

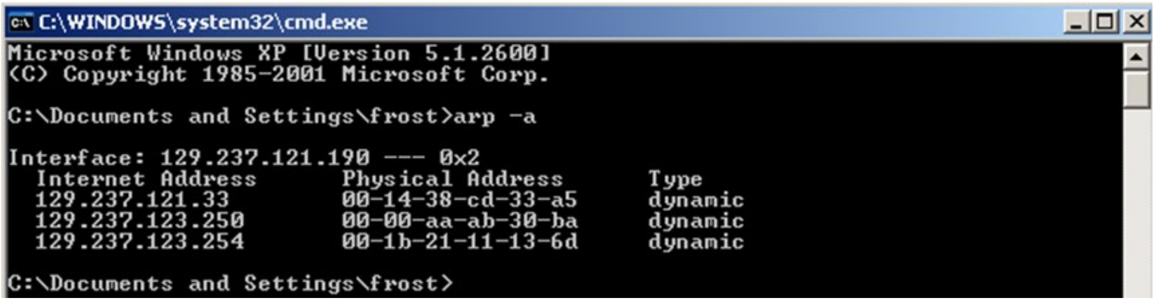
4) What is the IP address of destination www.google.com, report in dotted decimal and in Hex?
5) What is the source IP address (in Hex).
6) What is the “Time to live” set on each Echo (ping) requests? Why do these packets have these “Time to live” values? What are the units of the TTL.
7) What are the sent data bytes (in Hex) when using the default ping packet length.
8) What are the sent data bytes (in Hex) when using the default ping packet with the -l 256 option.
9) Why is the length of IP packet not the same as the length of the ICMP packet.
10) What is the MAC address (physical address) of your NIC? Find the MAC address by examining the Echo (ping) request in the Packet Bytes Plane (the bottom window). You will need your MAC address for ARP section of this project.
11) In Wireshark, generate a flow graph under Statistics→Flow graph. Discuss the resulting flow graph. Check box “Limit to display filter”

<u>ARP</u>

Use Wireshark and the arp command to examine transmit and received arp packets. NOTE: This assignment requires Wireshark and permissions to execute the arp –d * command. You must execute Wireshark and the arp –d * on your own computer as administrator.

Approximate Process:

a) In Windows bring up a "command" window by Start → Run→cmd
b) In the command window run arp –a, this command displays the local ARP table.
c) Record the results, it should look something like that shown in Figure 1:



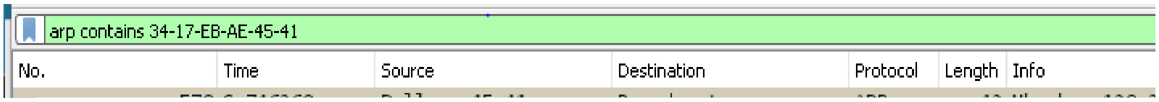
```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\frost>arp -a

Interface: 129.237.121.190 --- 0x2
  Internet Address      Physical Address      Type
  129.237.121.33        00-14-38-cd-33-a5     dynamic
  129.237.123.250       00-00-aa-ab-30-ba     dynamic
  129.237.123.254       00-1b-21-11-13-6d     dynamic

C:\Documents and Settings\frost>
```

d) Figure 1 Result of arp –a command

e) Start Wireshark
f) Confirm that the capture of packets is NOT in promiscuous mode. Under the Capture tab the Enable promiscuous mode on all interfaces is NOT checked.
g) Under capture → options select the interface your computer uses to send and receive packets.
h) Click start.
i) In the computer's command window run arp –d *, this command clears the local ARP table. In the computer's command window run arp –a and record the results again. You must be administrator to run the arp –d * command.
j) Check your ARP table, stop Wireshark when you see a new address in the arp table.
k) In Windows bring up a "command" window by Start → Run→cmd
l) In the command window run ipconfig /all. Note the physical address (MAC) of your machine.
m) In display filter input "arp contains physical address (MAC)",
   e.g. arp contains 34-17-EB-AE-45-40

Address the issues below in your report.

1) Examine the arp request packet
   a. Explain the Info field, see Figure 2



arp contains 34-17-EB-AE-45-41

No.	Time	Source	Destination	Protocol	Length	Info

Figure 2

   b. What is the destination MAC address? Why is this address used?
2) In the arp reply packet
   a. Explain the Info field
   b. What is the information contained in the arp reply packet.
3) Compare the arp tables before and after executing the arp –d * command and discuss any resulting changes.
4) Examine an ARP Request packet, in your report discuss why is the target MAC address all 0's?
5) Under Statistics→Flow Graph. Discuss the resulting flow graph.

How does the Wireshark output demonstrate protocol layering and encapsulation. How are network protocol analyzers, e.g., Wireshark, used to examine the operation of network protocols?