**CS 6043: Computer Networking**

**SPRING 2016**

**PROJECT 3**

Sneha Jinturkar M08698220

**Given: April 10, 2016**

**Due: April 22 (Friday), 2016 (NO LATER THAN 11:59PM)**

**Submission Instructions:**

1. Submit only on-line files on Blackboard before midnight. No hard copy will be accepted.

2. For students who are working in a team, *one* submission for the team is sufficient.

3. Wireshark files for this project can be found in the zip file “Project\_3\_Wireshark\_Traces.zip”.

**Part I: IP**

Load the file ‘IP\_project\_3.pcapng’ in Wireshark and answer the following questions. The trace was generated while sending ICMP echo requests to a target host.

1. Within the IP packet header, what is the value in the upper layer protocol field?

Answer: The value of the upper layer protocol field is ICMP (0X01)

1. How many bytes are in the IP header? How many bytes are in the payload of the IP datagram? Explain how you determined the number of payload bytes.

Answer: The number of bytes in the IP header are 20. Since a packet of 56 bytes was being sent, it leaves 36 bytes for the payload.

1. Which fields in the IP datagram always change from one datagram to the next within this series of ICMP messages sent by 192.168.1.102?

Answer: The header checksum and the Identification changes from each datagram to the next.

1. What is the value in the Identification field and the TTL field of the first ICMP packet sent from 192.168.1.102?

Answer: Value of identification field = 17264 and time to live is 128

**Part II: DHCP**

Load the file ‘DHCP\_project\_3.pcapng’ in Wireshark and answer the following questions. The trace was generated while releasing the host’s current IP address and renewing it multiple times. The host is a computer in UC network.

1. What is the link-layer address and the hardware address length of the host?

Answer:

Link-layer address – 34:17:eb:bd:32:d5

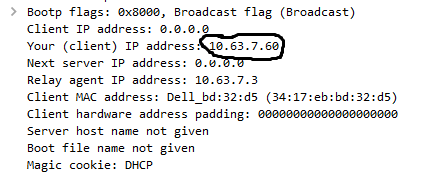
Hardware address length – 6 bytes

1. What is the value of the Transaction-ID in each of the first five (Discover/Offer/Request/ACK) DHCP messages?

Answer: The transaction ID in each of the first five (Discover/Offer/Request/ACK) DHCP messages is 0xe71fd191.

1. What IP address is the DHCP server offering to your host in the first DHCP Offer message? Include a screenshot.

Answer: IP address offered by the DHCP server to our host in the first DHCP Offer message is 10.63.7.60.



**Part III: Ethernet, ARP**

Load the file ‘Eth\_ARP\_project\_3.pcap’ in Wireshark and answer the following questions. The trace was generated while a web page was accessed (<http://gaia.cs.umass.edu/wireshark-labs/HTTP-ethereal-lab-file3.html>).

[Hint: For some of the questions, it might be helpful to disable IP or higher layer protocols. To do this, go to *Analyze->Enabled Protocols*]

1. What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of gaia.cs.umass.edu? Explain why you answered yes or no.

Answer: The 48-bit destination address in the Ethernet frame is 00:06:25:da:af:73. This is not the address of gaia.cs.umass.edu because it is the address of the router, which is the link used to get off the subnet.

1. Give the hexadecimal value for the two-byte ‘frame type’ field for frame number 15. What upper layer protocol does this correspond to?

Answer: Hexadecimal value for two-byte ‘frame type’ field for frame number 15 is 0x0800. This corresponds to the upper layer of IP.

1. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message?

Answer: Hexadecimal value for source address – 00:d0:59:a9:3d:68

Hexadecimal value for destination address – ff:ff:ff:ff:ff:ff (broadcast address)