Lab07: NAT, Ethernet, and ARP

EXERCISE 1

Question 1: What is the IP address of the client?

- 192.168.1.100

Question 2: Consider now the HTTP GET sent from the client to the Google server (whose IP address is IP address 64.233.169.104) at time 7.109267. What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP GET?

- Source IP: 192.168.1.100
- Destination IP: 64.233.169.104
- Source Port: 4335
- Destination Port: 80

Question 3: At what time is the corresponding 200 OK HTTP message received from the Google server? What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP 200 OK message?

- OK received at 7.158797
- Source IP: 64.233.169.104
- Destination IP: 192.168.1.100
- Source Port: 80
- Destination Port: 4335

Question 7: What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP GET message (as recorded in the NAT_ISP_side trace file)? Which of these fields are the same, and which are different, than in your answer to Question 2 above?

- Source IP: 71.192.34.104
- Destination IP: 64.233.169.104
- Source Port: 4335
- Destination Port: 80
- Everything is the same except for the Source IP

Question 9: Which of the following fields in the IP datagram carrying the HTTP GET are changed: Version, Header Length, Flags, Checksum. If any of these fields have changed, give a reason (in one sentence) stating why this field needed to change.

- Checksum has changed because the TCP checksum includes source and destination IPs. Since source IP changed, it changes the checksum

Question 11: What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP 200 OK message? Which of these fields are the same, and which are different than your answer to Question 3 above?

- Source IP: 64.233.169.104
- Destination IP: 71.192.34.104
- Source Port: 80
- Destination Port: 4335
- Destination IP has changed. Everything else is different

Question 13: What are the source and destination IP addresses and source and destination ports for these two segments (TCP SYN and TCP SYN/ACK)? Which of these fields are the same, and which are different than your answer to Question 4 and 5 above?

- Source Port: 80
- Destination: 4335

Question 14: The discussion on NAT in the Week 7 lecture slide No 71 shows the NAT translation table used by a NAT router. Using your answers to the questions above, fill in the NAT translation table entries for the HTTP connection considered in the questions above.

ISP Side	Home Side
• 71.192.34.104, 80	• 192.168.1.100, 4335

EXERCISE 2

Question 2. What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of gaia.cs.umass.edu? If not, then which device has this address? (Note: this is an important question, and one that students sometimes get wrong. You may want to refer back to relevant parts of the text and lecture notes and make sure you understand the answer here.)

- 48-bit address: 00:06:25:da:af:73
- No, the address is most likely that of a link called LinksysG, a router

Question 4. How many bytes from the very start of the Ethernet frame does the ASCII "G" in "GET" appear in the Ethernet frame? Note that when you examine the Data portion of this frame, it actually consists of both the Ethernet frame headers as well as the payload (i.e. bottom window in Wireshark shows the entire 686 byte frame that is captured). Of the bytes preceding the G, the first few bytes are the Ethernet frame header. Does this include the preamble bytes, or are those bytes omitted from the capture? Given this, how many bytes of frame header are present? What are the remainder of the bytes before the G?

- It follows position 0x36 = 54 bytes from the very start until the ASCII "G" appears
- The ethernet frame header omits preamble bytes from capture
- 14 bytes are present in the Ethernet frame header
- The remaining bytes are IP and TCP headers which are 20+20 = 40bytes

Question 5. What is the value of the Ethernet source address? Is this the address of the host that sent the GET HTTP request, or of gaia.cs.umass.edu? If not then which device has this address?

- Ethernet source address = 00:06:25:da:af:73
- No it is not the same address as the host that sent the GET HTTP request of gaia.cs.umass.edu
- The device that has the address is LinksysG

Exercise 3

Question 1. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message? Is there something special about the destination address?

- Source value: 00:d0:59:a9:3d:68
- Destination Value: ff:ff:ff:ff
- The destination address is broadcast to all hosts on the network

Question 6. Where in the ARP request does the "question" (IP address for which the mapping is being requested) appear?

- It appears in the 'target' field. The address is 192.168.1.1

Question 8. What is the value of the *opcode* field within the ARP-payload part of the Ethernet frame in which an ARP response is made?

- The opcode value is 0x0002 = 2

Question 9. Where in the ARP message does the "answer" to the earlier ARP request appear – the Ethernet address of the machine whose corresponding IP address is being queried?

- The answer appears in the Sender MAC address

Question 10. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP reply message?

- Source Value: 00:06:25:da:af:73
- Destination Value: 00:d0:59:a9:3d:68