COMP3331 Computer Networks and Applications
Lab Exercise 07: NAT, Ethernet and ARP

HyoJoo Kwon
z5222646
W12A

Exercise 1: Understanding NAT using Wireshark

(*) 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: 192.168.1.100, 4335
- Destination: 64.233.169.104, 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?

-200 OK HTTP received at 7.158798
-Source: 64.233.169.104, 80
-Destination: 192.168.1.100, 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: 71.192.34.104, 4335
- Destination: 64.233.169.14, 80
- Only the source IP address changed

(*) 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. The value has changed because checksum includes the source IP address, which has changed.

(*) 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: 64.233.169.104, 80
- Destination: 71.192.34.104, 4335
- The destination IP address 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?

- SYN: source: 71.192.34.104, 4335 / destination: 64.233.169.104, 80
- ACK: source: 64.233.169.104, 80 / destination: 71.192.34.104, 4335

- For SYN, the source IP is different and for ACK, the destination IP is different.

(*) Question 14: The discussion on NAT in the Week 7 lecture slide No 80 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.

- NAT translate table
- WAN side: 71.192.34.104, 4335
- LAN side: 192.168.1.100, 4335

Exercise 2: Using Wireshark to understand Ethernet

(*) 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.)

- 00:0c:41:45:90:a8
- No. It is the address of my router.

Question 3. Give the hexadecimal value for the two-byte Frame type field.

- 0x0800

(*) 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?

- The ASCII G appears 52 bytes from the start of the ethernet frame. There are 14B ethernet frame, and then 30 bytes of ip header followed by 20 bytes of tcp header before the http data is encountered.

(*) 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?

- source address: 00:0c:41:45:90:a8
- It is the address of my router, which is the link used to get into my subnet.

Exercise 3: Using Wireshark to understand ARP

(*) 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 address: 00:d0:59:a9:3d:68.
- destination address: ff:ff:ff:ff:ff:ff.

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

- The field "Target MAC address" is set to 00:00:00:00:00:00 to question the machine, corresponding IP address (192.168.1.1) is being queried.

(*) 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?

- 0x0002 for reply

(*) 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 to the earlier ARP request appears in the “Sender MAC address” field, which contains the Ethernet address 00:06:25:da:af:73 for the sender with IP address 192.168.1.1

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

- source: 00:06:25:da:af:73
- destination: 00:d0:59:a9:3d:68