StudentID:z5195715
Name: Junyu Ren

Lab 7

Exercise 1: Understanding NAT using Wireshark

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

Client ip address is 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 Source port:4335
destination IP:64.233.169.104 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?

At 7.158797s.
Source IP:64.233.169.104 Source port:80
destination ip:192.168.1.100 destination port:4335

Question 4: Recall that before a GET command can be sent to an HTTP server, TCP must first set up a connection using the three-way SYN/ACK handshake. At what time is the client-to-server TCP SYN segment sent that sets up the connection used by the GET sent at time 7.109267? What are the source and destination IP addresses and source and destination ports for the TCP SYN segment?

At 7.075657s
Source ip:192.168.1.100 Source port:4335
Destination ip : 64.233.169.104 destination port:80

Question 5: What are the source and destination IP addresses and source and destination ports of the ACK sent in response to the SYN. At what time is this SYN/ACK received at the client?

Source ip:64.233.169.104 Source port:80
Destination ip:192.168.1.100 destination port:4335
At 7.108986s

Question 6: At what time does this message appear in the NAT_ISP_side trace file?

At 6.069168s in NAT_ISP_side trace file.

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 Source port:4335
Destination:64.233.169.104 destination port:80
Compared with Q2, source ip is different, remains are same.

Question 8: Are any fields in the HTTP GET message changed?

No,there aren't.

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 changed and others don't.Because checksum contains source ip address and now source ip address changed.So, checksum need to update to new source ip address.

Question 10: In the NAT_ISP_side trace file, at what time is the first 200 OK HTTP message received from the Google server?

At time 6.117570s

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 Source port:80
Destination ip:71.192.34.104 destination ip:4335
Compared with Q3, destination ip is different and remains are same

Question 12: In the NAT_ISP_side trace file, at what time were the client-to-server TCP SYN segment and the server-to-client TCP SYN/ACK segment corresponding to the segments in Question 4 and 5 above captured?

At time 6.035475s,client-to-server syn send.At time 6.067775s,server-to-client syn/ack send.

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 ip 71.192.34.104   Source port 4335
    Destination ip 64.233.169.104   destination port 80
SYN/ACK: Source ip 64.233.169.104   Source port 80
    Destination ip 71.192.34.104 destination port 4335
Compared with Q4 & Q5, SYN's source ip and SYN/ACK's destination ip are different.Both SYN or SYN/ACK 's port number remain the same.

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.

WAN	LAN
71.192.34.104,4335	192.168.1.100,4335

Question 15: The trace files investigated above have additional connections to Google servers above and beyond the HTTP GET, 200 OK request/response studied above. For example, in the NAT_home_side trace file, consider the client-to-server GET at time 1.572315, and the GET at time 7.573305. Research the use of these two HTTP messages and safe browsing in general. Explain your findings in a concise manner.

Google Safe Browsing is a blacklist service provided by Google that provides lists of URLs for web resources that contain malware or phishing content.The Google Chrome, Safari, Firefox,etc Web browsers use the lists from the Google Safe Browsing service for checking pages against potential threats.Google also provides a public API for the service.

Google also provides information to Internet service providers, by sending e-mail alerts to autonomous system operators regarding threats hosted on their networks.(adapted from Wikipedia)

Exercise 2: Using Wireshark to understand Ethernet

Question 1. What is the 48-bit Ethernet address of the source host of this packet?

The address is 00:d0:59:a9:3d:68

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?

The destination address is 00:06:25:da:af:73.The source host and destination are not belongs to the same subnet.So the Ethernet address is not Ethernet address of gaia.cs.unmass.edu. It should be the MAC address of the first hop router on the source to destination path.

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

It is 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?

G appear after 54 bytes.Because First 14 bytes are Ethernet frame header.And then,20 bytes for IP header and 20 bytes for tcp header.And the 'G' starts from right here.Wireshark don't capture preamble bytes.

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 is 00:06:25:da:af:73.It is not the address of GET HTTP or gaia.cs.umass.edu.It refers to the MAC address of the nearest hop router on the path from source router to gaia.cs.umass.edu.

Question 6. What is the destination address in the Ethernet frame? Is this the Ethernet address of the source host that sent the earlier GET HTTP request?

Destination address is 00:d0:59:a9:3d:68.
Yes,it is.

Question 7. How many bytes from the very start of the Ethernet frame does the ASCII "O" in "OK" (i.e., the HTTP response code) appear in the Ethernet frame?

67 bytes.Because 14 bytes for Ethernet frame header,20 bytes for ip header,20 bytes for tcp header and also 13 bytes for “HTTP/1.1 200”.And then,”O” starts right here.

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 is 00:d0:59:a9:3d:68, destination address is ff:ff:ff:ff:ff:ff.Destination address is the broadcast address,every host in this subnet will process this message.

Question 2. Give the hexadecimal value for the two-byte Ethernet Frame type field.

It is 0x0806

Question 3: How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?

It begins from 20 bytes.

Question 4. What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP request is made?

The value is 0x0001

Question 5. Does the ARP request message contain the IP address of the sender?

Yes,it is.IP address of sender is 192.168.1.105.

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

IP address which want to request is filled in target IP address, the MAC address is left blank(00:00:00:00:00:00).

Question 7. How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?

It begins from 20 bytes.

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 value is 0x0002.

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 sender’s MAC address field.

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

Source address is 00:06:25:da:af:73
Destination address is 00:d0:59:a9:3d:68.