**1/ Introduction:**

**Q1.** List the 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.

*Answer:* Some of the protocols listed in the screenshot below are UDP, TCP, ARP, ICMP, MDNS, and STUN.



**Q2.** How long did it take from when the HTTP GET message was sent until the HTT OK reply was received?

*Answer:* The GET was sent at 11.300694 and the reply was received at 11.301658. The delay was thus 0.000964 secs

**Q3.** What is the Internet address of the gaia.cs.umass.edu (also known as wwwnet.

cs.umass.edu)? What is the Internet address of your computer?

*Answer:*

* The IP address of gaia.cs.umass.edu is 128,119.245.145
* The IP address of my laptop is 128.119.66.142

**Q4.** Print the HTTP GET and REPLY messages displayed in step 9 above. To do so, select Print from the Wireshark File command menu, and select the“Selected Packet Only” and “Print as displayed” radial buttons, and then click OK.

*Answer:*

HTTP GET message:

No. Time Source Destination Protocol Length Info

74 11.300694 128.119.245.145 128.119.245.12 HTTP 489 GET /wireshark-labs/IN

Frame 74: 489 bytes on wire (3912 bits), 489 bytes captured (3912 bits)

Ethernet II, Src: HonHaiPr\_0d:ca:8f (00:22:68:0d:ca:8f), Dst: DellComp\_3b:8f:cd

(00:06:5b:3b:8f:cd)

Internet Protocol Version 4, Src: 128.119.245.145 (128.119.245.145), Dst:

128.119.245.12 (128.119.245.

Transmission Control Protocol, Src Port: 49930 (49930), Dst Port: http (80),

Seq: 1, Ack: 1, Len: 435

Hypertext Transfer Protocol

GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n

Host: gaia.cs.umass.edu\r\n

User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2.22)

Gecko/20110902 Firefox/3.

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8\r\n

Accept-Language: en-us,en;q=0.5\r\n

Accept-Encoding: gzip,deflate\r\n

Accept-Charset: ISO-8859-1,utf-8;q=0.7,\*;q=0.7\r\n

Keep-Alive: 115\r\n

©2013 Pearson Education, Inc. Upper Saddle River, NJ. All Rights Reserved.

Connection: keep-alive\r\n

\r\n

[Full request URI: <http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html>]

HTTP REPLY message:

No. Time Source Destination Protocol Length Info

76 11.301658 128.119.245.12 128.119.245.145 HTTP 434 HTTP/1.1 200 OK (text

Frame 76: 434 bytes on wire (3472 bits), 434 bytes captured (3472 bits)

Ethernet II, Src: DellComp\_3b:8f:cd (00:06:5b:3b:8f:cd), Dst: HonHaiPr\_0d:ca:8f

(00:22:68:0d:ca:8f)

Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst:

128.119.245.145 (128.119.245.1

Transmission Control Protocol, Src Port: http (80), Dst Port: 49930 (49930),

Seq: 1, Ack: 436, Len: 38

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n

Date: Mon, 26 Sep 2011 19:52:01 GMT\r\n

Server: Apache/2.2.3 (CentOS)\r\n

Last-Modified: Mon, 26 Sep 2011 19:51:01 GMT\r\n

ETag: "8734b-51-7a797340"\r\n

Accept-Ranges: bytes\r\n

Content-Length: 81\r\n

Keep-Alive: timeout=10, max=100\r\n

Connection: Keep-Alive\r\n

Content-Type: text/html; charset=UTF-8\r\n

\r\n

Line-based text data: text/html

**6/ ICMP:**

**Q1.** What is the IP address of your host? What is the IP address of the destination host?

*Answer:*

The IP address of my host is 192.168.1.101. The IP address of the destination host is 143.89.14.34.

**Q2.** Why is it that an ICMP packet does not have source and destination port numbers?

*Answer:*

The ICMP packet does not have source and destination port numbers because it was designed to communicate network-layer information between hosts and routers, not between application layer processes. Each ICMP packet has a "Type" and a "Code". The Type/Code combination identifies the specific message being received. Since the network software itself interprets all ICMP messages, no port numbers are needed to direct the ICMP message to an application layer process.

**Q3.** Examine one of the ping request packets sent by your host. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?

*Answer:*

The ICMP type is 8, and the code number is 0. The ICMP packet also has checksum, identifier, sequence number, and data fields. The checksum, sequence number and identifier fields are two bytes each.

**Q4.** Examine the corresponding ping reply packet. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?

*Answer:*

The ICMP type is 0, and the code number is 0. The ICMP packet also has checksum, identifier, sequence number, and data fields. The checksum, sequence number and identifier fields are two bytes each.

**Q5.** What is the IP address of your host? What is the IP address of the target destination host?

*Answer:*

The IP address of my host is 192.168.1.101. The IP address of the destination host is 138.96.146.2.

**Q6.** If ICMP sent UDP packets instead (as in Unix/Linux), would the IP protocol number still be 01 for the probe packets? If not, what would it be?

*Answer:*

No. If ICMP sent UDP packets instead, the IP protocol number should be 0x11

**Q7.** Examine the ICMP echo packet in your screenshot. Is this different from the ICMP ping query packets in the first half of this lab? If yes, how so?

*Answer:*

The ICMP echo packet has the same fields as the ping query packets.

**Q8.** Examine the ICMP error packet in your screenshot. It has more fields than the ICMP echo packet. What is included in those fields?

*Answer:*

The ICMP error packet is not the same as the ping query packets. It contains both the IP header and the first 8 bytes of the original ICMP packet that the error is for.

**Q9.** Examine the last three ICMP packets received by the source host. How are these packets different from the ICMP error packets? Why are they different?

*Answer:*

The last three ICMP packets are message type 0 (echo reply) rather than 11 (TTL expired). They are different because the datagrams have made it all the way to the destination host before the TTL expired.

**Q10.** Within the tracert measurements, is there a link whose delay is significantly longer than others? Refer to the screenshot in Figure 4, is there a link whose delay is significantly longer than others? On the basis of the router names, can you guess the location of the two routers on the end of this link?

*Answer:*

There is a link between steps 11 and 12 that has a significantly longer delay. This is a transatlantic link from New York to Aubervilliers, France. In figure 4 from the lab, the link is from New York to Pastourelle, France.

**8/ NAT:**

**Q1.** What is the IP address of the client?

*Answer:*

The address of the client is: 192.168.1.100

**Q3.** 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 7.102967. What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP GET?

*Answer:*

* Source: 192.168.1.100, 4335
* Destination: 64.233.169.104, 80)

**Q4.** 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?

*Answer:*

* The time at which the corresponding 200 OK HTTP message received from the Google server is: 7.158798
* Source: 64.233.169.104, 80 || Destination: 192.168.1.100, 4335

**Q5.**

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 7.102967?

*Answer:*

The time is: 7.075657

What are the source and destination IP addresses and source and destination ports for the TCP SYN segment?

*Answer:*

* Source: 192.168.1.100, 4335
* Destination: 64.233.169.104, 80

What are the sources and destination IP addresses and source and destination ports of the ACK sent in response to the SYN?

*Answer:*

* Source: 64.233.169.104, 80
* Destination: 192.168.1.100, 4335

At what time is this ACK received at the client?

*Answer:*

7.108986

**Q6.**

In the NAT\_ISP\_side trace file, find the HTTP GET message was sent from the client to the Google server at time 7.102967 (where t=7.102967 is time at which this was sent as recorded in the NAT\_home\_side trace file). At what time does this message appear in the NAT\_ISP\_side trace file?

*Answer:*

6.069168

What are the sources and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP GET (as recording in the NAT\_ISP\_side trace file)?

*Answer:*

* Source: 71.192.34.104, 4335
* Destination: 64.233.169.104, 80

Which of these fields are the same, and which are different, than in your answer to question 3 above?

*Answer:*

Only the source IP address has changed.

**Q7.**

Are any fields in the HTTP GET message changed?

*Answer:*

No

Which of the following fields in the IP datagram carrying the HTTP GET are changed: Version, Header Length, Flags or Checksum?

*Answer:*

Version is not changed. Neither are header length or flags. Checksum is changed.

If any of these fields have changed, give a reason (in one sentence) stating why this field needed to change.

*Answer:*

Since the IP source address has changed, and the checksum includes the value of the source IP address, the checksum has changed.

**Q8.**

In the NAT\_ISP\_side trace file, at what time is the first 200 OK HTTP message received from the Google server?

*Answer:*

6.308118

What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP 200 OK message?

*Answer:*

* Source: : 64.233.169.104, 80
* Destination: 71.192.34.104, 4335

Which of these fields are the same, and which are different than your answer to question 4 above?

*Answer:*

Only the destination IP address has changed.

**Q9.**

In the NAT\_ISP\_side trace file, at what time were the client-to-server TCP SYN segment and the server-to-client TCP ACK segment corresponding to the segments in question 5 above captured?

*Answer:*

6.035475, and 6.067775, respectively.

What are the source and destination IP addresses and source and destination ports for these two segments?

*Answer:*

For the SYN:

* Source: 71.192.34.104, 4335
* Destination: 64.233.169.104, 80

For the ACK:

* Source: : 64.233.169.104, 80
* Destination: 71.192.34.104, 4335

Which of these fields are the same, and which are different than your answer to question 5 above?

*Answer:*

For the SYN, the source IP address has changed, For the ACK, the destination IP address has changed. The port numbers are unchanged.

**Q10.** Using your answers to 1-8 above, fill in the NAT translation table entries for HTTP connection considered in questions 1-8 above.

*Answer:*

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