Question 1: In IP header, there is a field called “protocol (type)”. What is it used for?

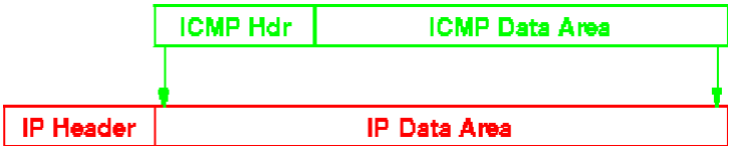
8-bit field that specifies the type of the payload

Question 2: How an ICMP message is transported (encapsulation)?

8-bits for the type, 8-bit for the Code and 16 bits for the Checksum in the header.

The type defines what error it is.

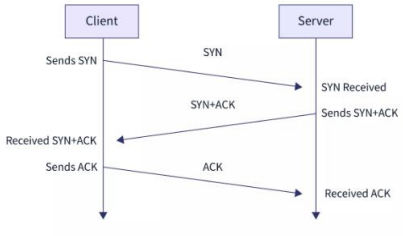
Two levels of encapsulation:



Question 3: Which ICMP messages are used to implement the Ping program?

Echo request and reply. An echo-request message can be sent by a host or router. An echo-replay message is sent by the host or router which receives an echo-request message.

Question 4: Use a figure to show the 3-way handshake to establish a connection in the TCP protocol.



```
C:\Users\jwan9>tracert  -d www.home.se

Tracing route to www.home.se [104.21.82.29]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  192.168.0.1
  2     8 ms     8 ms     8 ms  213.200.143.26
  3    29 ms    28 ms    28 ms  213.200.168.83
  4    26 ms    26 ms    26 ms  91.129.12.43
  5    26 ms    26 ms    26 ms  130.244.205.6
  6    32 ms     *       29 ms  80.81.194.180
  7    35 ms    28 ms    29 ms  172.69.148.3
  8    28 ms    28 ms    28 ms  104.21.82.29

Trace complete.
```

Tracert output

Question 5: How many routers are on the route from your computer to www.home.se? What are their IP addresses?

8 routers. Their IP addresses are shown in the image above.

Question 6: What is your computer IP address? What is the network ID for your connected network?

```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::ea49:f9f9:d9af:5abd%11
   IPv4 Address. . . . . . . . . . . : 192.168.0.163
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1
```

My IP address is: 192.168.0.163

The network ID is: 192.168.0.0

Question 7: Which domain name server(s) is responsible for the name resolution of www.home.se? How do you find this?

```
C:\Users\jwan9>nslookup -type=ns home.se
Server:  UnKnown
Address:  192.168.0.1

Non-authoritative answer:
home.se nameserver = terin.ns.cloudflare.com
home.se nameserver = sima.ns.cloudflare.com
```

Question 8: check the first packet sent by tracert

A. What is the value in the protocol (type) field of IP packet? What does it mean?

The value is 8 Echo, used by ping program

B. C. How many bytes are there in the IP header? How many bytes are there in the payload of the IP packet? Explain how you determined the number of payload bytes.

Ip header = 20 bytes, 92(Total length in ICMP) – 20 (Header of IP packet) - 8 (Header of ICMP) = 64 bytes

Question 9: Has this IP packet been fragmented? Explain how you know whether or not this packet has been fragmented. What is the Identification for this IP packet?

No, the value of more fragmentation is set to Not set. If the packet has been fragmented the value should be set to 1 and a value to the offset should not be set to 0. The identification is 0x5ebd

Question 10: What is the TTL value for this IP packet? Why this value is set so?

The value is 1. It is essentially specifying the maximum number of hops (routers or network devices) the packet can pass through before being discarded. If the TTL is set to a value of 1, it means that the packet is intended to reach its final destination with just one hop.

Question 11: What is the source IP address of this IP packet? And what is the destination IP address of this packet? What is the value in the protocol type field (in IP header) ?

The source IP address is: 192.168.0.1

The3 des IP address is: 192.168.0.163

The value is (ICMP) 1

Question 12: What is the ICMP message type carried in the packet? What is the sender of this message?

The type is 11, the sender is the gateway of my computer which is my router.

Question 13: how many ICMP echo request messages with IP TTL of 1 is sent?

3 request messages

Question 14: what is the value in the Identification field? On the line "IP Fragments (3008 bytes):", why the payload data is of 3008 bytes? Also check the response message. How many data bytes were sent in the ICMP response? Are they the same as the ICMP request?

The value in identification field is 42731, The value of “IP fragments is the size of all fragments, it’s 3008 and yes, it is the same.

Question 15: Fill in the following table based on IP headers in these fragments:

Commented [JM1]: Ask

Frame Number	IP Identification	Fragment offset, In bytes, in 8-bytes	Header length	Total length
1603	0xa6eb	0	20 bytes	1500
1604	0xa6eb	1480 in bytes, 185 in 8-bytes	20 bytes	1500
1605	0xa6eb	2960 in bytes, 370 in 8-bytes	20 bytes	68

Question 16: How do you know if an IP fragment is the first fragment, and an IP fragment is the last fragment?

When the 'More fragments' bit in the Flags field is set to 1, it indicates that it is the first fragment. Conversely, when the value is set to 0 again, it signifies that it is the last fragment.

Question 17: What is the IP address for your computer, and what is the IP address for databases.cs.hkr.se?

My IP address: 192.168.0.163

Databases.cs.hkr.se IP address: 194.47.29.127

Question 18: What are port numbers for the databases.cs.hkr.se web server and your web browser applications?

databases.cs.hkr.se web server port number is: 80

My web browser application port number is: 58041

Question 19: what are the 3 packet numbers for the connection setup? Do they have any pay-load data in the TCP segments? Is there any options exchanged in the connection setup? What are the main purpose of the 3-way handshake connection setup?

Packets numbered 22, 24, and 25, do not contain any payload data in the TCP segments. The reason for this is that the main purpose of the 3-way handshake connection is to establish a connection before sending any data.

Question 20: What is the sequence number of the TCP SYN segment that is sent from the client computer by checking it in raw data? What are the sequence number and acknowledgment number of the TCP SYN segment that is sent from the server by checking them in raw data? What are the window sizes on both sides? What purpose is the window size used for?

Seq = 0 from client to server, Seq = 1 from server to client. Win = 64240 from client to server, Win = 262144. The window size tells the sender how much data the receiver can accept without congesting the network or overwhelming the receiver's buffer.

Question 21: what is the sequence number of the TCP segment that contains the first HTTP GET command to download the small home page alice.htm? And what are the sequence number and the acknowledgment number of the TCP segment that positively acknowledges the segment? How to interpret the acknowledgment number?

Seq = 0, Seq = 1 Ack = 1

Question 22: How many TCP segment is used for the client to send the “get” command to the database server (for downloading alice.htm)? How many TCP segments are used for the database server to send the home page alice.htm?

1 TCP segments to send the request, 1 TCP segments to send the home page back

Question 23: How many TCP segments are used for the database server to send the home page alice-ch1.txt?

4 TCP segments

Question 24: How long in bytes is the HTTP response message containing the file alice.htm? How do you find it out?

172 bytes long, we can find it by looking at the content length in the http message.

Question 25: A TCP connection is identified by a pair of (ip, port) numbers. How many TCP connections were created between your web browser and the web server?

There were two concatenations with different port number

Question 26: select one connection to answer this question. What information has been exchanged during this connection setup? Give their values.

•Source Port: 49906

•Destination Port: 80

•Header Length: 44 bytes

•Flags: SYN (Synchronize)

•Window Size: 65535

•Checksum: 0x92cd

•Urgent Pointer: 0

•Options: Maximum segment size, No-Operation (NOP), Window scale, Timestamps, SACK permitted, End of Option List (EOL)

Question 27: how many GET commands were sent to download this home page (and embedded objects)?

There were 4 get requests

Question 28: how many TCP connections were used to download this home page and embedded objects? Which of them were downloaded in serial and which of them were downloaded in parallel (need to provide the fact)?

There were two connections established during the download process:

Connection 1, which utilized port number 49906, and Connection 2, operating on port number 49907, were employed to retrieve the home page, and they seemed to operate concurrently. Within Connection 1, the HTML, GIF, and icon components were sequentially downloaded. Concurrently, within Connection 2, the email GIF was fetched.

Question 29: how many TCP segments were used to transport the image sunrise.gif? how is it possible to assemble these data in right order to form file sunrise.gif?

There were 231 TCP segments used to transport the image "sunrise.gif." These segments are numbered and reassembled to form the complete image.

Question 30: If one of these segments (of sending sunrise.gif) were lost during the transportation, what would happen? Will all the segments be discarded? Why or why not

TCP uses a mechanism called Automatic Repeat reQuest (ARQ) to recover lost or corrupted segments. When a segment is lost, the receiver can detect the loss because the missing segment's sequence number is not acknowledged. The sender will then retransmit the lost segment. Only the lost segment will be retransmitted, not all of them.

Question 31. How many TCP segments were used to transport the file eric-email.gif? How many bytes are there in the HTTP message containing this file?

1.There were two TCP segments used to transport the file "eric-email.gif."

2.The HTTP message containing this file had a total of 1492 bytes.

Problem encountered:

I misunderstood the seq and ack values in Wireshark. Solved by asking the teacher.

Learnings:

In this Lab I learned a lot about analyzing the second and third layers in Wireshark. I learned how a fragmented packet is sent; how different port numbers lead to new connection with the server.