Lab Report 2

Venkatesh Kumar (M23CSE028)

Solution 1.

IP packet header of tcp segment

```
Unset
Frame 4914: 65226 bytes on wire (521808 bits), 65226 bytes captured (521808
bits) on interface eth0, id 0
Ethernet II, Src: Microsof_b4:62:69 (00:15:5d:b4:62:69), Dst:
PcsCompu_cb:7e:f5 (08:00:27:cb:7e:f5)
Internet Protocol Version 4, Src: 172.16.100.5, Dst: 172.20.230.237
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 65212
Identification: 0x2a6e (10862)
010. .... = Flags: 0x2, Don't fragment 0... .... = Reserved bit: Not set .1..
.... = Don't fragment: Set ..0. .... = More fragments: Not set
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 60
Protocol: TCP (6)
Header Checksum: 0x72b5 [validation disabled] [Header checksum status:
Unverified]
Source Address: 172.16.100.5
Destination Address: 172.20.230.237
```

- Version: 4 Usefulness: Indicates that the IP version being used is IPv4.
- Header Length: 20 bytes (5) Usefulness: Specifies the length of the IP header in 32-bit words. In this case, the header length is 20 bytes, which is the standard size for IPv4 headers without options.
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Usefulness: The DSCP (Differentiated Services Code Point) field is used for Quality of Service (QoS) markings,

but in this case, it's set to 0x00, indicating a default service. The ECN (Explicit Congestion Notification) is set to Not-ECT, meaning that congestion notification is not enabled.

- Total Length: 65212 Usefulness: Represents the total length of the IP packet (header + data) in bytes. In this example, the total length is 65212 bytes.

- Identification: 0x2a6e (10862) Usefulness: A unique identifier assigned to the packet, often used in fragmentation and reassembly. In this case, the identification is 0x2a6e (10862).

- Flags: 0x2, Don't fragment Usefulness: Flags indicate various control information for packet handling. In this case, the "Don't Fragment" (DF) flag is set (0x2), indicating that the packet should not be fragmented during transmission.

- Fragment Offset: 0 Usefulness: Specifies the position of the fragment in the original unfragmented packet. In this case, the offset is 0, indicating that this is not a fragment.

- Time to Live: 60 Usefulness: Represents the maximum time the packet is allowed to live in the network. It is decreased by routers as the packet traverses the network to prevent it from circulating indefinitely.

- Protocol: TCP (6) Usefulness: Specifies the higher-layer protocol to which the payload belongs. In this case, the value 6 indicates that the payload is a TCP packet.

- Header Checksum: 0x72b5 [validation disabled] Usefulness: Provides error-checking for the IP header to ensure data integrity during transmission. The checksum value is 0x72b5 in this example.

- Source Address: 172.16.100.5 Usefulness: Specifies the IP address of the sender (source) of the packet.

- Destination Address: 172.20.230.237 Usefulness: Specifies the IP address of the recipient (destination) of the packet.

Solution 2.

Ping request made to www.inria.fr

a. ICMP packets do not have source port and destination port. Because ICMP is not a transport or above layer protocol.

ICMP (Internet Control Message Protocol) operates at the network layer of the OSI model and

is primarily used for diagnostic and error reporting purposes in IP networks. ICMP packets are encapsulated within IP packets but do not have the concept of source and destination ports like some other transport layer protocols such as TCP or UDP.

b. Below is attached echo request packet.
Type is 8 and code is 0 which is highlighted.

```
Unset
Frame 7: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface
enp0s3, id 0 Ethernet II, Src: PcsCompu_62:db:48 (08:00:27:62:db:48), Dst:
RealtekU_12:35:02 (52:54:00:12:35:02)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 128.93.162.83
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x6ddf [correct] [Checksum Status: Good]
Identifier (BE): 10790 (0x2a26)
Identifier (LE): 9770 (0x262a)
Sequence Number (BE): 1 (0x0001)
Sequence Number (LE): 256 (0x0100) [Response frame: 8]
Timestamp from icmp data: Jan 30, 2024 04:17:00.000000000 GMT [Timestamp from
icmp data (relative): 0.608431546 seconds] Data (48 bytes)
```

c. All the fields in ICMP packets are as follows

- Type (8 bits):

  Use: Identifies the specific type of ICMP message. Different types serve different purposes, such as Echo Request, Echo Reply, Destination Unreachable, Time Exceeded, etc.

- Code (8 bits):

  Use: Further refines the message type, providing additional information about the ICMP message. For example, for an Echo Request, the code might specify variations of the request.

- Checksum (16 bits):

Use: Ensures the integrity of the ICMP packet during transmission. The checksum is computed over the ICMP header and data fields.

- Identifier (16 bits):

  Use: Typically used in Echo Request and Echo Reply messages to help match requests with their corresponding replies. It allows the sender and receiver to correlate multiple requests and responses.

- Sequence Number (16 bits):

  Use: Works in conjunction with the Identifier to identify the order of Echo Request and Echo Reply messages. Helps in distinguishing different packets within the same session.

- Timestamp (32 bits) and Timestamp Reply (32 bits):

  Use: Present in Timestamp and Timestamp Reply messages, used for measuring the round-trip time between the source and destination. The Timestamp field contains the time the Echo Request was sent, and the Timestamp Reply field contains the time the reply was sent.

d. Below is attached echo reply packet. Type is 0 and code is 0 which is highlighted.

```
Unset
Frame 8: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface
enp0s3, id 0
Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst:
PcsCompu_62:db:48 (08:00:27:62:db:48)
Internet Protocol Version 4, Src: 128.93.162.83, Dst: 10.0.2.15
Internet Control Message Protocol
Type: 0 (Echo (ping) reply)
Code: 0
Checksum: 0x75df [correct] [Checksum Status: Good]
Identifier (BE): 10790 (0x2a26)
Identifier (LE): 9770 (0x262a)
Sequence Number (BE): 1 (0x0001) Sequence Number (LE): 256 (0x0100) [Request
frame: 7] [Response time: 186.840 ms]
Timestamp from icmp data: Jan 30, 2024 04:17:00.000000000 GMT [Timestamp from
icmp data (relative): 0.795271068 seconds] Data (48 bytes)
```

e. Yes ICMP echo request and reply packets have the same fields.As it is visible in the above echo request and echo reply packet, they have the same fields. In general, ICMP Echo Request and Echo Reply packets have similar fields, but there are some differences related to the specific nature of the request and response.

Solution 3.

Traceroute request to website www.inria.fr

a. First ICMP response packet are as follows

```
Unset
Frame 10: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on
interface eth0, id 0
Ethernet II, Src: Microsof_b4:62:69 (00:15:5d:b4:62:69), Dst:
PcsCompu_cb:7e:f5 (08:00:27:cb:7e:f5)
Internet Protocol Version 4, Src: 172.20.224.1, Dst: 172.20.230.237 Internet
Control Message Protocol
Type: 11 (Time-to-live exceeded)
Code: 0 (Time to live exceeded in transit)
Checksum: 0xaaec [correct] [Checksum Status: Good] Unused: 00000000 Internet
Protocol Version 4, Src: 172.20.230.237, Dst: 128.93.162.83
 User Datagram Protocol, Src Port: 40528, Dst Port: 33434 Data (32 bytes)
Data: 404142434445464748494a4b4c4d4e4f505152535455565758595a5b5c5d5e5f
[Length: 32]
```

Type: 11 (Time-to-live exceeded) and Code: 0 (Time to live exceeded in transit)

Reason: This message is generated by a router along the path when the Time to Live (TTL) value of a packet reaches zero, indicating that the packet has traversed a certain number of hops.This is used to check that at which router response is coming from by setting TTL.

b. Last Icmp response are as follows

```
Unset
Frame 437: 163 bytes on wire (1304 bits), 163 bytes captured (1304 bits) on interface eth0, id 0
Ethernet II, Src: PcsCompu_cb:7e:f5 (08:00:27:cb:7e:f5), Dst: Microsof_b4:62:69 (00:15:5d:b4:62:69)
Internet Protocol Version 4, Src: 172.20.230.237, Dst: 172.20.224.1 Internet Control Message Protocol
Type: 3 (Destination unreachable)
Code: 3 (Port unreachable)
Checksum: 0x1c8c [correct] [Checksum Status: Good] Unused: 00000000 Internet Protocol Version 4, Src: 172.20.224.1, Dst: 172.20.230.237
User Datagram Protocol, Src Port: 53, Dst Port: 46097 Domain Name System (response)
```

Type: 3 (Destination unreachable) and Code: 3 (Port unreachable)

The Type field in the ICMP header indicates the type of ICMP message. Type 3 corresponds to a "Destination unreachable" message, suggesting that the destination (or a part of the path) is unreachable.Code 3 specifically indicates that the destination is unreachable because the destination port is unreachable. This is often encountered when trying to establish a connection to a specific port on a host, and that port is not open or not responding.

Now, let's compare it with the ICMP response in Question 2(a):

- **Question 2(a) ICMP Response:**
  - Type: 11 (Time-to-live exceeded)
  - Code: 0 (Time to live exceeded in transit)
- **Current ICMP Response:**
  - Type: 3 (Destination unreachable)
  - Code: 3 (Port unreachable)

Comparison:

- The ICMP response in Question 2(a) indicates a "Time-to-live exceeded" condition, often encountered during the traceroute process when the TTL value reaches zero in transit through a router.
- The current ICMP response indicates a "Destination unreachable" condition with a specific reason: "Port unreachable." This is often encountered when a host receives a packet directed to a specific port that is not open or not responsive.

c. These are the following ***traceroute*** output whose latencies are longer than others

```
Unset
nkn.mx1.gen.ch.geant.net (62.40.125.214) 198.757
ms ae7.mx1.par.fr.geant.net (62.40.98.239) 195.742
ms nkn.mx1.gen.ch.geant.net (62.40.125.214) 185.718
ms ae7.mx1.par.fr.geant.net (62.40.98.239) 195.707
ms ae7.mx1.par.fr.geant.net (62.40.98.239) 195.691 ms 195.673 ms
renater-lb1-gw.mx1.par.fr.geant.net (62.40.124.70) 195.030 ms
renater-lb1-gw.mx1.par.fr.geant.net (62.40.124.70) 195.411 ms * 196.699 ms
inria-rocquencourt-vl1631-te1-4-inria-rtr-021.noc.renater.fr
(193.51.184.177) 196.667 ms *
inria-rocquencourt-vl1631-te1-4-inria-rtr-021.noc.renater.fr
(193.51.184.177) 198.568 ms 198.553 ms
```

so corresponding ip address and their location and link is as follows

ip Address	Location	Possible type of link
62.40.125.214	Geneva,Switzerland	optical Fiber sea link
62.40.98.239	Paris,France	Inter country
62.40.124.70	Paris,France	Physical Link
193.51.184.177	Rennes,France	Physical link