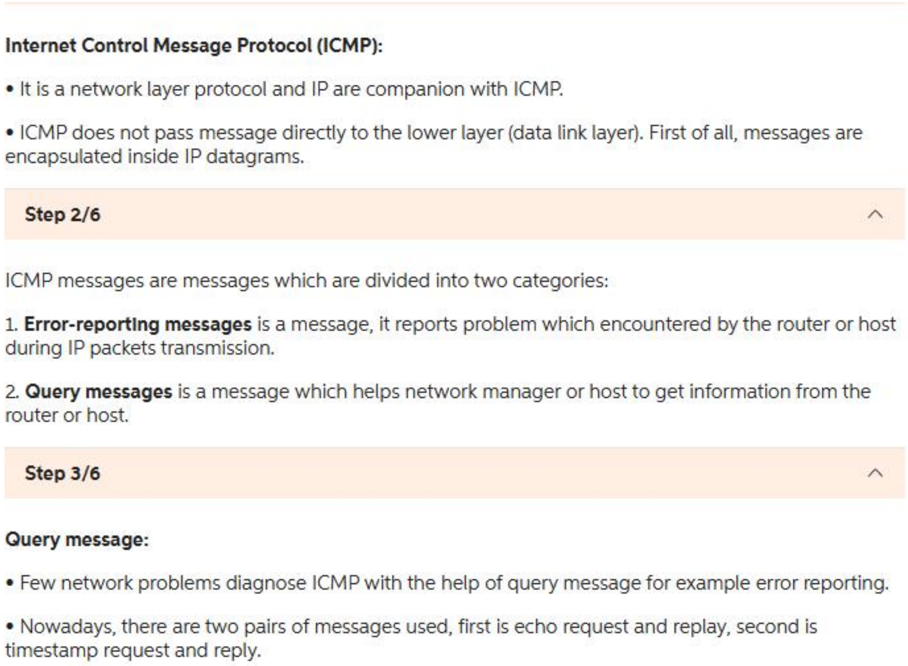
1. Host A sends a timestamp-request message to host B and never receives a reply. Discuss three possible causes and the corresponding course of action.



Internet Control Message Protocol (ICMP):

- It is a network layer protocol and IP are companion with ICMP.

- ICMP does not pass message directly to the lower layer (data link layer). First of all, messages are encapsulated inside IP datagrams.

Step 2/6

ICMP messages are messages which are divided into two categories:

1. **Error-reporting messages** is a message, it reports problem which encountered by the router or host during IP packets transmission.

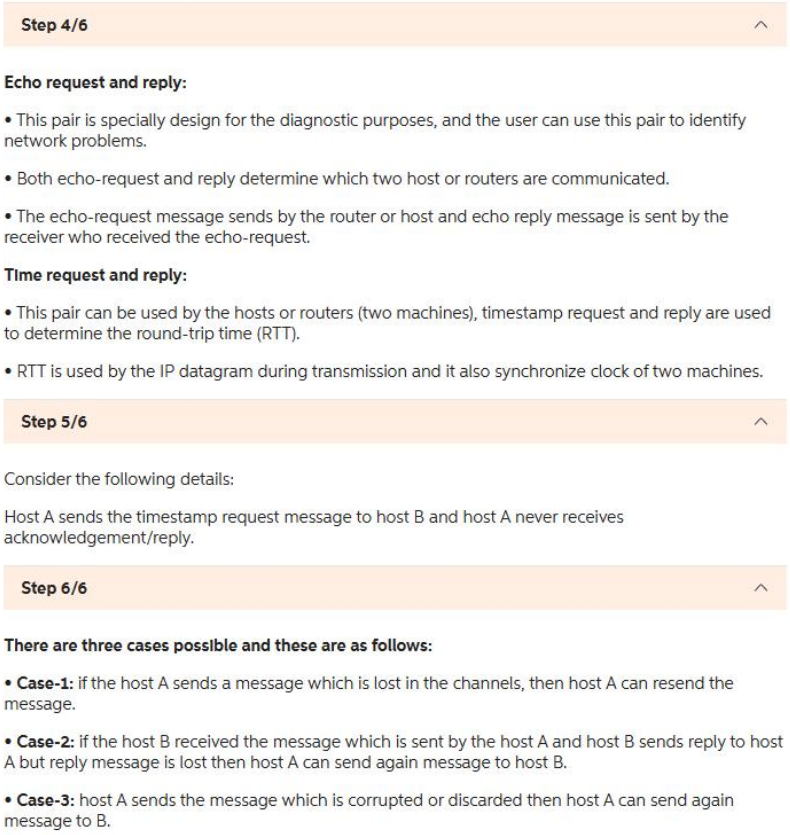
2. **Query messages** is a message which helps network manager or host to get information from the router or host.

Step 3/6

Query message:

- Few network problems diagnose ICMP with the help of query message for example error reporting.

- Nowadays, there are two pairs of messages used, first is echo request and replay, second is timestamp request and reply.



Step 4/6

Echo request and reply:

- This pair is specially design for the diagnostic purposes, and the user can use this pair to identify network problems.

- Both echo-request and reply determine which two host or routers are communicated.

- The echo-request message sends by the router or host and echo reply message is sent by the receiver who received the echo-request.

Time request and reply:

- This pair can be used by the hosts or routers (two machines), timestamp request and reply are used to determine the round-trip time (RTT).

- RTT is used by the IP datagram during transmission and it also synchronize clock of two machines.

Step 5/6

Consider the following details:

Host A sends the timestamp request message to host B and host A never receives acknowledgement/reply.

Step 6/6

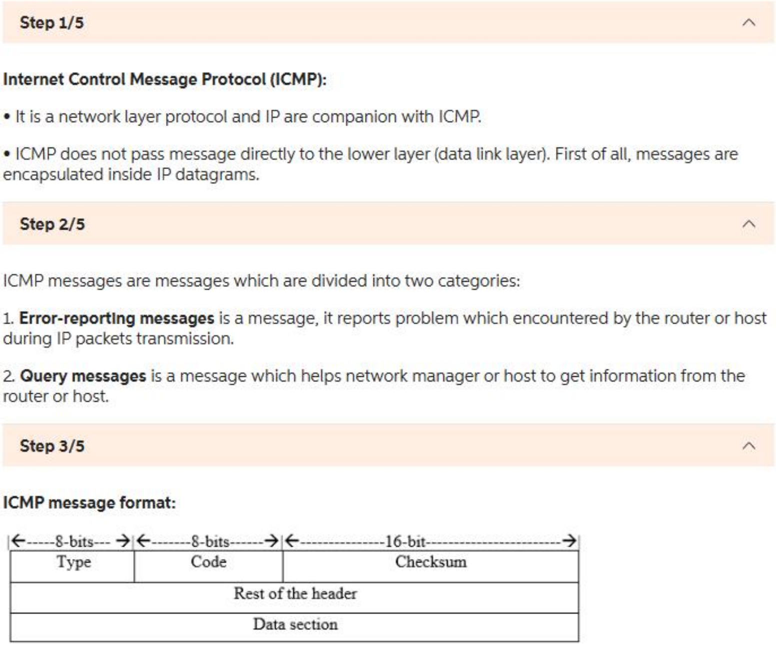
There are three cases possible and these are as follows:

- **Case-1:** if the host A sends a message which is lost in the channels, then host A can resend the message.

- **Case-2:** if the host B received the message which is sent by the host A and host B sends reply to host A but reply message is lost then host A can send again message to host B.

- **Case-3:** host A sends the message which is corrupted or discarded then host A can send again message to B.

2. Why is there a restriction on the generation of an ICMP message in response to a failed ICMP error message?



Step 1/5

Internet Control Message Protocol (ICMP):

- It is a network layer protocol and IP are companion with ICMP.

- ICMP does not pass message directly to the lower layer (data link layer). First of all, messages are encapsulated inside IP datagrams.

Step 2/5

ICMP messages are messages which are divided into two categories:

1. **Error-reporting messages** is a message, it reports problem which encountered by the router or host during IP packets transmission.

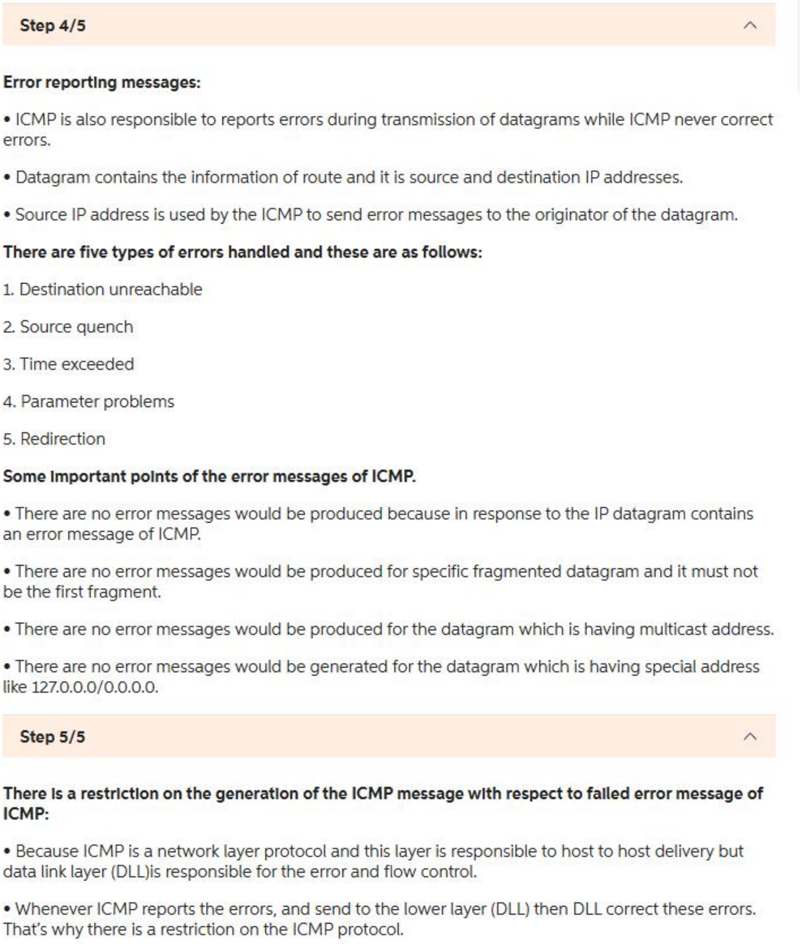
2. **Query messages** is a message which helps network manager or host to get information from the router or host.

Step 3/5

ICMP message format:

|←-----8-bits--- →|←-------8-bits------→|←---------------16-bit----------------------→|

Type	Code	Checksum
Rest of the header		
Data section		



Step 4/5

Error reporting messages:

- ICMP is also responsible to reports errors during transmission of datagrams while ICMP never correct errors.

- Datagram contains the information of route and it is source and destination IP addresses.

- Source IP address is used by the ICMP to send error messages to the originator of the datagram.

There are five types of errors handled and these are as follows:

1. Destination unreachable

2. Source quench

3. Time exceeded

4. Parameter problems

5. Redirection

Some important points of the error messages of ICMP.

- There are no error messages would be produced because in response to the IP datagram contains an error message of ICMP.

- There are no error messages would be produced for specific fragmented datagram and it must not be the first fragment.

- There are no error messages would be produced for the datagram which is having multicast address.

- There are no error messages would be generated for the datagram which is having special address like 127.0.0.0/0.0.0.0.

Step 5/5

There is a restriction on the generation of the ICMP message with respect to failed error message of ICMP:

- Because ICMP is a network layer protocol and this layer is responsible to host to host delivery but data link layer (DLL)is responsible for the error and flow control.

- Whenever ICMP reports the errors, and send to the lower layer (DLL) then DLL correct these errors. That's why there is a restriction on the ICMP protocol.

3. Host A sends a datagram to host B. Host B never receives the datagram and host A never receives notification of failure. Give two different explanations of what might have happened.

Step 5/6

Consider the following details:

Host A sends the datagram to host B and host B never receives datagram, host A never receives the failure notification.

Step 6/6

There are two different explanation about the datagram transmission and these are as follows:

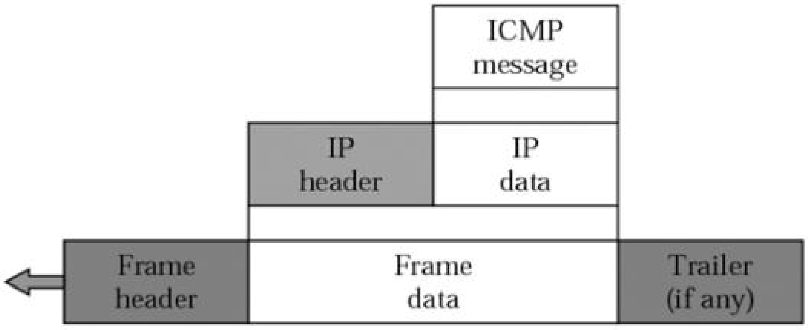
1. If the host A sends a message which is lost in the channels due to network congestion, error messages generated by the intermediate router then datagram does not receive by host B.

2. Host A sends the message to host B but host B is unreachable due to intermediate router failure.

4. What is the purpose of including the IP header and the first 8 bytes of datagram data in the error reporting ICMP messages?

Step 6/7

The diagram has the IP header and datagram which is exhibited in the diagram.



Step 7/7

The purpose of including the IP header and 8-byte datagram in error reporting message that has the description which is as follows.

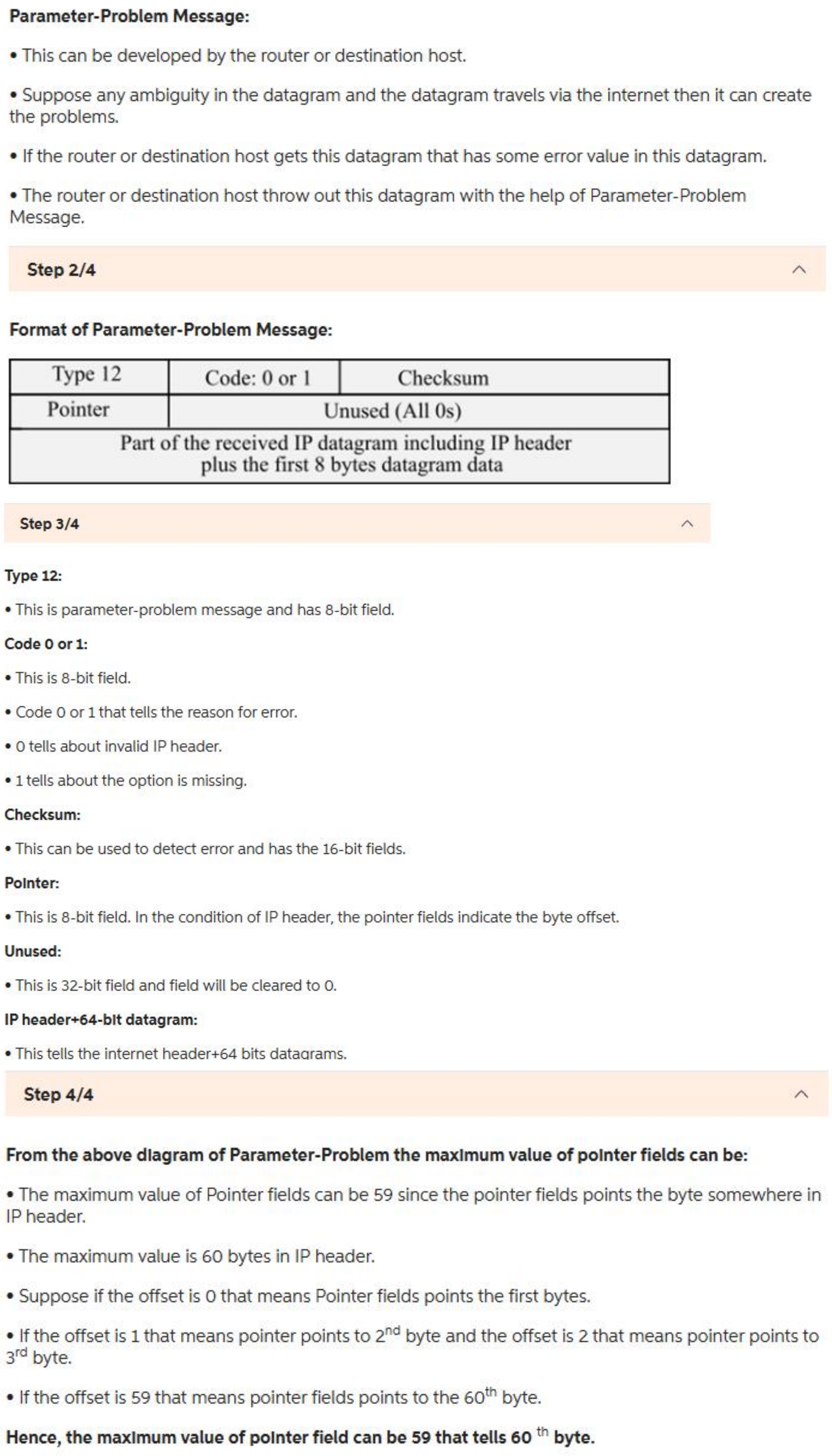
- The IP header has the source and destination address in order to tell that what is source address of the packet and what is the destination address of the packet in error reporting message.

- The IP header also has the sequence number of the packet to identify at the receiver side which packet has been arrived.

- The 8 bytes of datagram cab used to tell how much data can be transferred over the internet.

Hence, the above reasons are the purpose in order to contain the IP header and 8-byte datagram.

5. What is the maximum value of the pointer field in a parameter-problem message?



Parameter-Problem Message:

- This can be developed by the router or destination host.
- Suppose any ambiguity in the datagram and the datagram travels via the internet then it can create the problems.
- If the router or destination host gets this datagram that has some error value in this datagram.
- The router or destination host throw out this datagram with the help of Parameter-Problem Message.

Step 2/4

Format of Parameter-Problem Message:

Type 12	Code: 0 or 1	Checksum
Pointer	Unused (All 0s)	
Part of the received IP datagram including IP header plus the first 8 bytes datagram data		

Step 3/4

Type 12:

- This is parameter-problem message and has 8-bit field.

Code 0 or 1:

- This is 8-bit field.
- Code 0 or 1 that tells the reason for error.
- 0 tells about invalid IP header.
- 1 tells about the option is missing.

Checksum:

- This can be used to detect error and has the 16-bit fields.

Pointer:

- This is 8-bit field. In the condition of IP header, the pointer fields indicate the byte offset.

Unused:

- This is 32-bit field and field will be cleared to 0.

IP header+64-bit datagram:

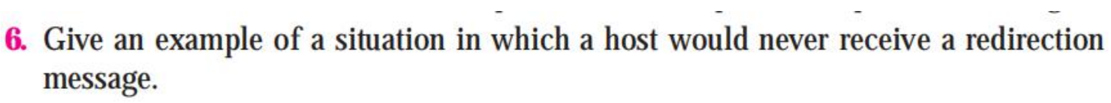
- This tells the internet header+64 bits datagrams.

Step 4/4

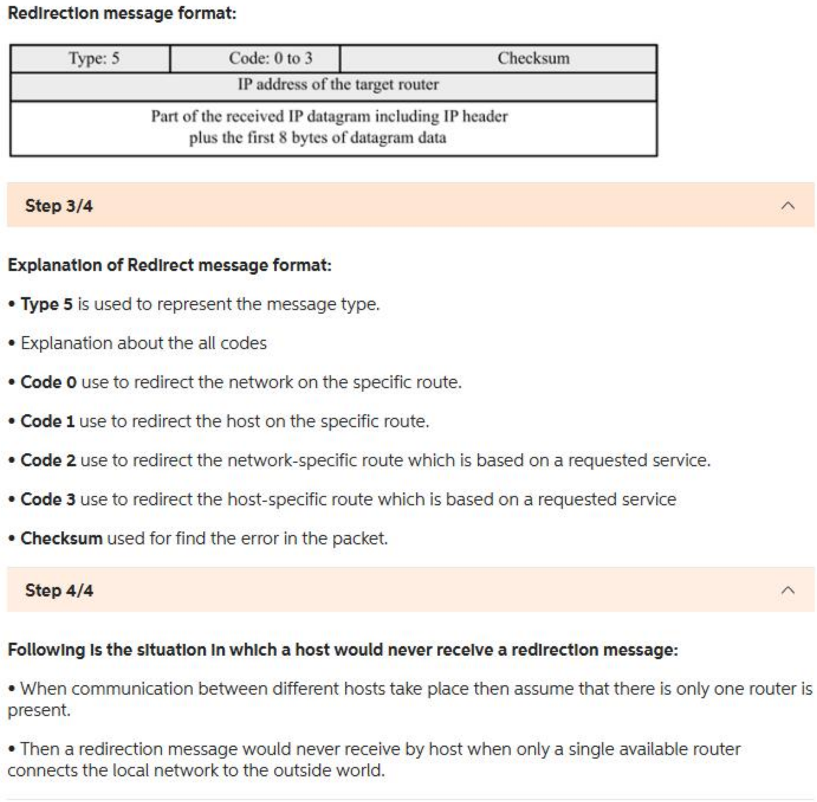
From the above diagram of Parameter-Problem the maximum value of pointer fields can be:

- The maximum value of Pointer fields can be 59 since the pointer fields points the byte somewhere in IP header.
- The maximum value is 60 bytes in IP header.
- Suppose if the offset is 0 that means Pointer fields points the first bytes.
- If the offset is 1 that means pointer points to 2nd byte and the offset is 2 that means pointer points to 3rd byte.
- If the offset is 59 that means pointer fields points to the 60th byte.

Hence, the maximum value of pointer field can be 59 that tells 60 th byte.



6. Give an example of a situation in which a host would never receive a redirection message.



Redirection message format:

Type: 5	Code: 0 to 3	Checksum
IP address of the target router		
Part of the received IP datagram including IP header plus the first 8 bytes of datagram data		

Step 3/4

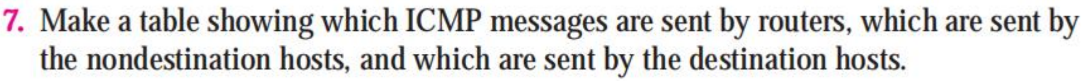
Explanation of Redirect message format:

- **Type 5** is used to represent the message type.
- Explanation about the all codes
- **Code 0** use to redirect the network on the specific route.
- **Code 1** use to redirect the host on the specific route.
- **Code 2** use to redirect the network-specific route which is based on a requested service.
- **Code 3** use to redirect the host-specific route which is based on a requested service
- **Checksum** used for find the error in the packet.

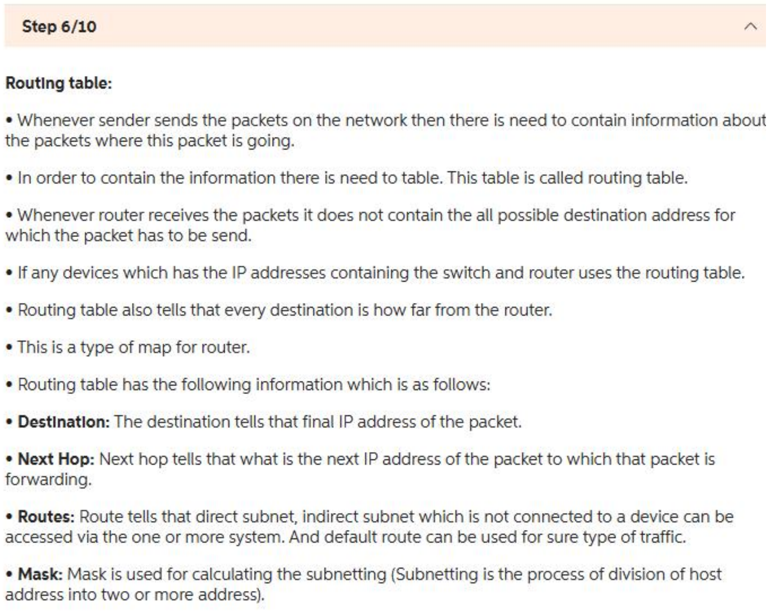
Step 4/4

Following is the situation in which a host would never receive a redirection message:

- When communication between different hosts take place then assume that there is only one router is present.
- Then a redirection message would never receive by host when only a single available router connects the local network to the outside world.



7. Make a table showing which ICMP messages are sent by routers, which are sent by the nondestination hosts, and which are sent by the destination hosts.



Step 6/10

Routing table:

- Whenever sender sends the packets on the network then there is need to contain information about the packets where this packet is going.
- In order to contain the information there is need to table. This table is called routing table.
- Whenever router receives the packets it does not contain the all possible destination address for which the packet has to be send.
- If any devices which has the IP addresses containing the switch and router uses the routing table.
- Routing table also tells that every destination is how far from the router.
- This is a type of map for router.
- Routing table has the following information which is as follows:
- **Destination:** The destination tells that final IP address of the packet.
- **Next Hop:** Next hop tells that what is the next IP address of the packet to which that packet is forwarding.
- **Routes:** Route tells that direct subnet, indirect subnet which is not connected to a device can be accessed via the one or more system. And default route can be used for sure type of traffic.
- **Mask:** Mask is used for calculating the subnetting (Subnetting is the process of division of host address into two or more address).

Step 7/10

Destination host:

- This is a type of computer that has the destination address of the packets.

Step 8/10

Nondestination host:

- This is a type of computer that has not the destination address of the packets.

Step 9/10

Below is the table that is displaying the ICMP messages and also shows that which messages is sent by the routers, which is sent by the nondestination host and which is sent by the destination host.

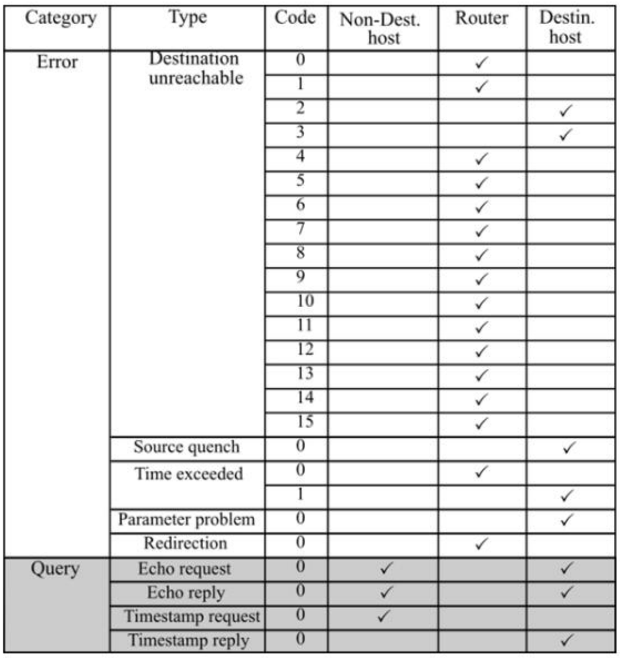
- In the diagram, there is the corresponding code different type of messages which is exhibited.

•

Step 10/10

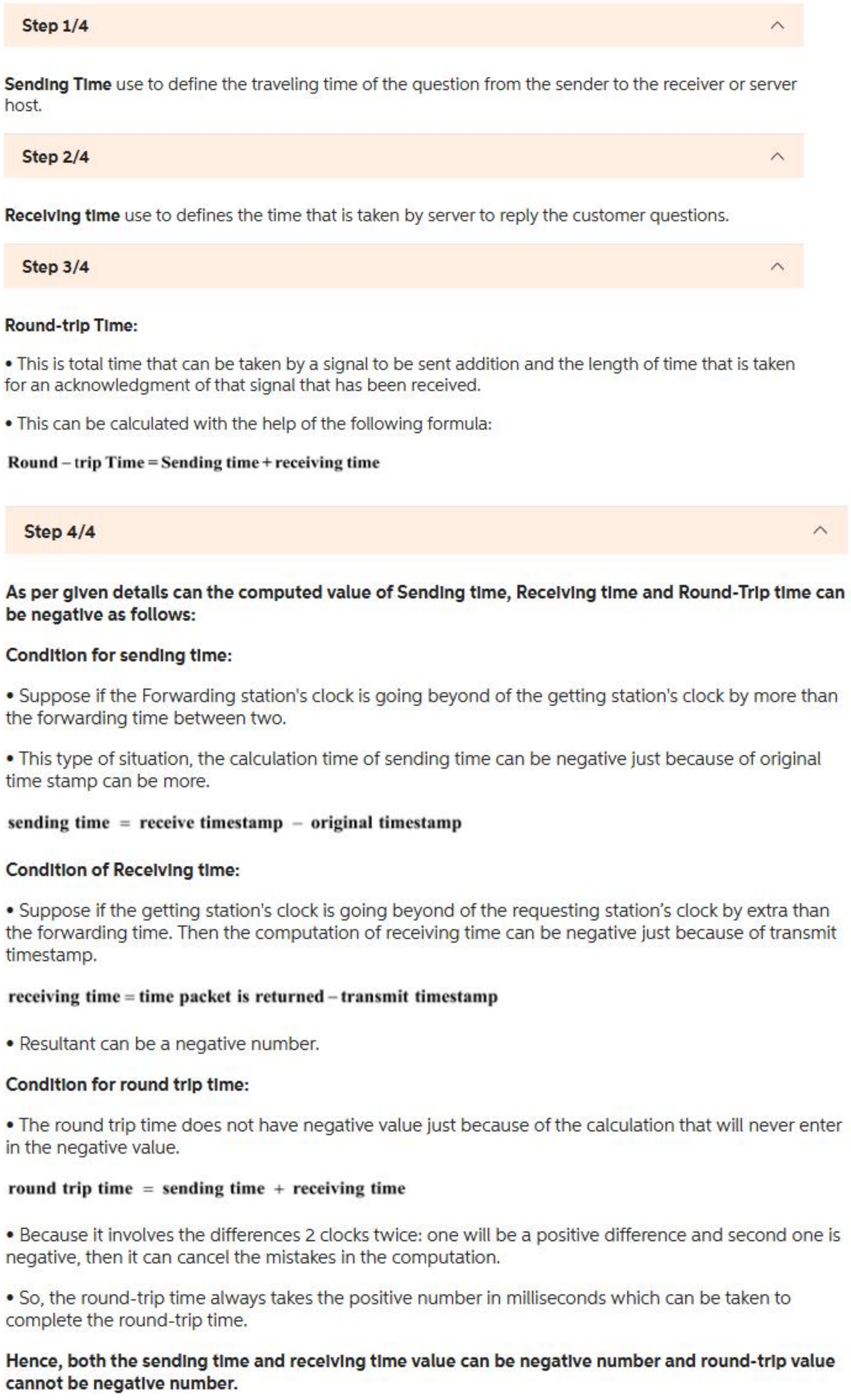
The diagram has two messages which is as follows:

- Error
- Query



Category	Type	Code	Non-Dest. host	Router	Destin. host
Error	Destination unreachable	0		✓	
		1		✓	
		2			✓
		3			✓
		4		✓	
		5		✓	
		6		✓	
		7		✓	
		8		✓	
		9		✓	
		10		✓	
		11		✓	
		12		✓	
		13		✓	
		14		✓	
		15		✓	
	Source quench	0			✓
	Time exceeded	0		✓	
		1			✓
	Parameter problem	0			✓
	Redirection	0		✓	
Query	Echo request	0	✓		✓
	Echo reply	0	✓		✓
	Timestamp request	0	✓		
	Timestamp reply	0			✓

8. Can the calculated sending time, receiving time, or round-trip time have a negative value? Why or why not? Give examples.



Step 1/4

Sending Time use to define the traveling time of the question from the sender to the receiver or server host.

Step 2/4

Receiving time use to defines the time that is taken by server to reply the customer questions.

Step 3/4

Round-trip Time:

- This is total time that can be taken by a signal to be sent addition and the length of time that is taken for an acknowledgment of that signal that has been received.

- This can be calculated with the help of the following formula:

Round – trip Time = Sending time + receiving time

Step 4/4

As per given details can the computed value of Sending time, Receiving time and Round-Trip time can be negative as follows:

Condition for sending time:

- Suppose if the Forwarding station's clock is going beyond of the getting station's clock by more than the forwarding time between two.

- This type of situation, the calculation time of sending time can be negative just because of original time stamp can be more.

sending time = receive timestamp − original timestamp

Condition of Receiving time:

- Suppose if the getting station's clock is going beyond of the requesting station’s clock by extra than the forwarding time. Then the computation of receiving time can be negative just because of transmit timestamp.

receiving time = time packet is returned − transmit timestamp

- Resultant can be a negative number.

Condition for round trip time:

- The round trip time does not have negative value just because of the calculation that will never enter in the negative value.

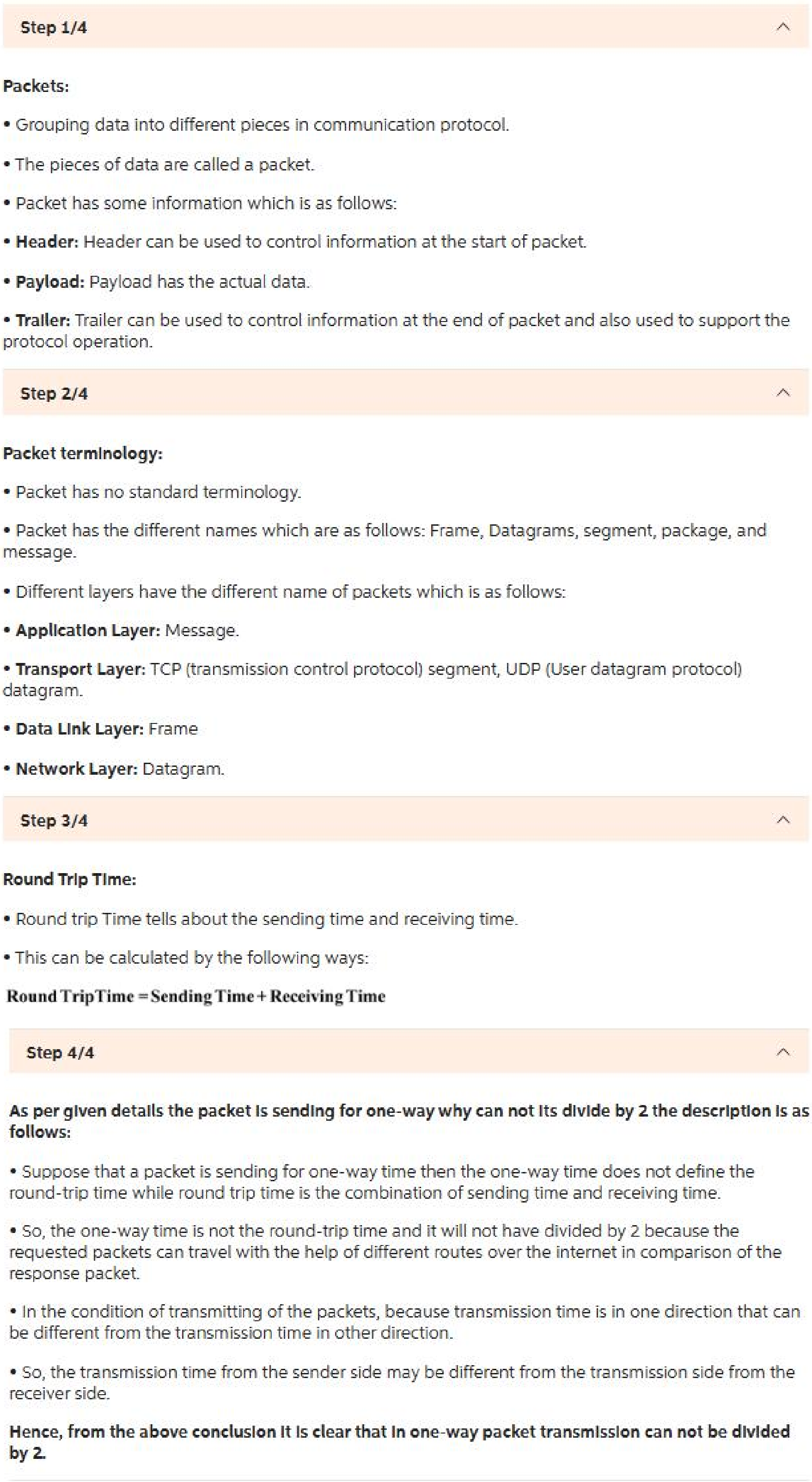
round trip time = sending time + receiving time

- Because it involves the differences 2 clocks twice: one will be a positive difference and second one is negative, then it can cancel the mistakes in the computation.

- So, the round-trip time always takes the positive number in milliseconds which can be taken to complete the round-trip time.

Hence, both the sending time and receiving time value can be negative number and round-trip value cannot be negative number.

9. Why isn’t the one-way time for a packet simply the round-trip time divided by two?



Step 1/4

Packets:

- Grouping data into different pieces in communication protocol.
- The pieces of data are called a packet.
- Packet has some information which is as follows:
- **Header:** Header can be used to control information at the start of packet.
- **Payload:** Payload has the actual data.
- **Trailer:** Trailer can be used to control information at the end of packet and also used to support the protocol operation.

Step 2/4

Packet terminology:

- Packet has no standard terminology.
- Packet has the different names which are as follows: Frame, Datagrams, segment, package, and message.
- Different layers have the different name of packets which is as follows:
- **Application Layer:** Message.
- **Transport Layer:** TCP (transmission control protocol) segment, UDP (User datagram protocol) datagram.
- **Data Link Layer:** Frame
- **Network Layer:** Datagram.

Step 3/4

Round Trip Time:

- Round trip Time tells about the sending time and receiving time.
- This can be calculated by the following ways:

$$\textbf{Round TripTime} = \textbf{Sending Time} + \textbf{Receiving Time}$$

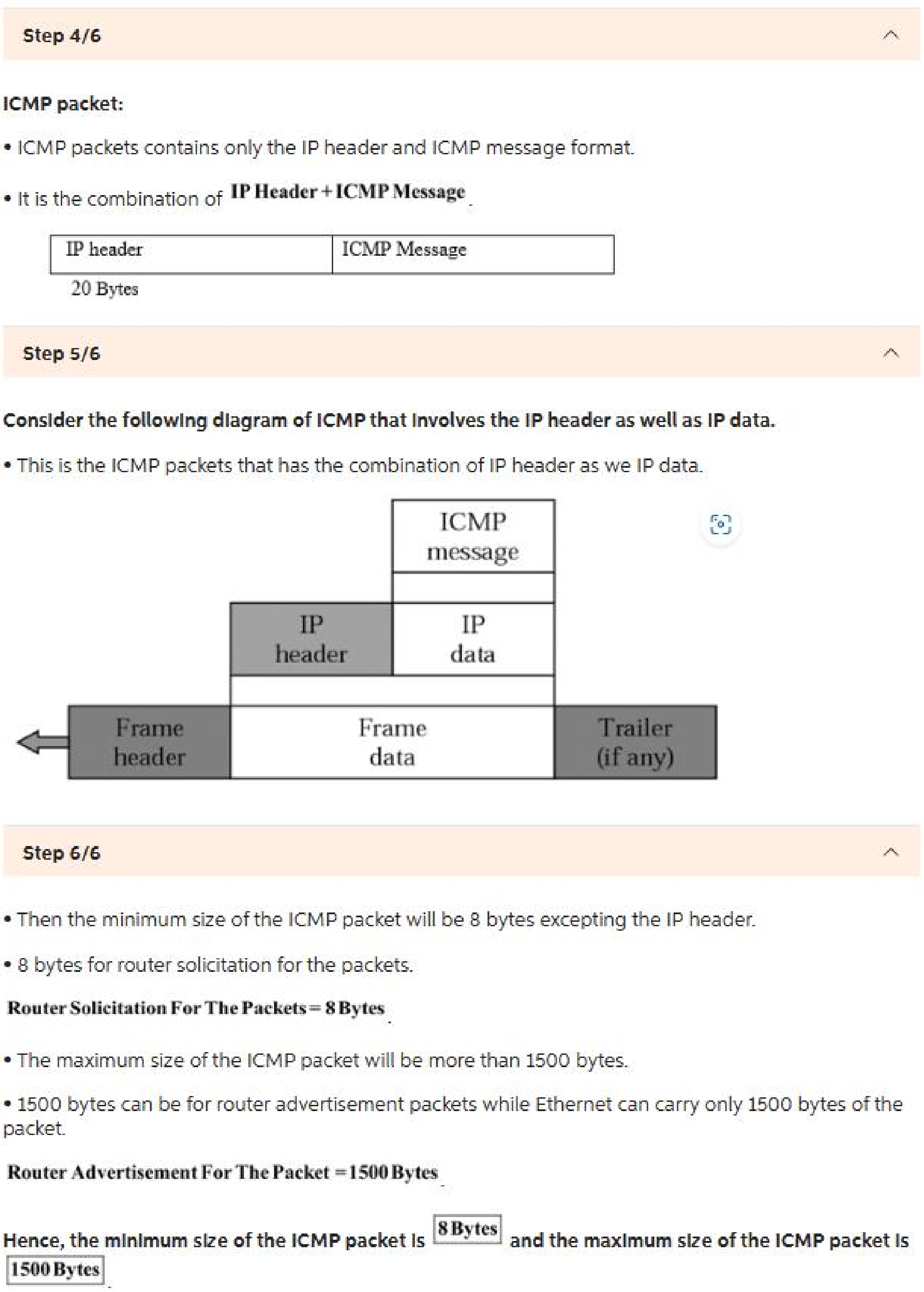
Step 4/4

As per given details the packet is sending for one-way why can not its divide by 2 the description is as follows:

- Suppose that a packet is sending for one-way time then the one-way time does not define the round-trip time while round trip time is the combination of sending time and receiving time.
- So, the one-way time is not the round-trip time and it will not have divided by 2 because the requested packets can travel with the help of different routes over the internet in comparison of the response packet.
- In the condition of transmitting of the packets, because transmission time is in one direction that can be different from the transmission time in other direction.
- So, the transmission time from the sender side may be different from the transmission side from the receiver side.

Hence, from the above conclusion it is clear that in one-way packet transmission can not be divided by 2.

10. What is the minimum size of an ICMP packet? What is the maximum size of an ICMP packet?



Step 4/6

ICMP packet:

- ICMP packets contains only the IP header and ICMP message format.

- It is the combination of **IP Header + ICMP Message** .

IP header	ICMP Message
20 Bytes	

Step 5/6

Consider the following diagram of ICMP that involves the IP header as well as IP data.

- This is the ICMP packets that has the combination of IP header as we IP data.

Step 6/6

- Then the minimum size of the ICMP packet will be 8 bytes excepting the IP header.

- 8 bytes for router solicitation for the packets.

Router Solicitation For The Packets = 8 Bytes .

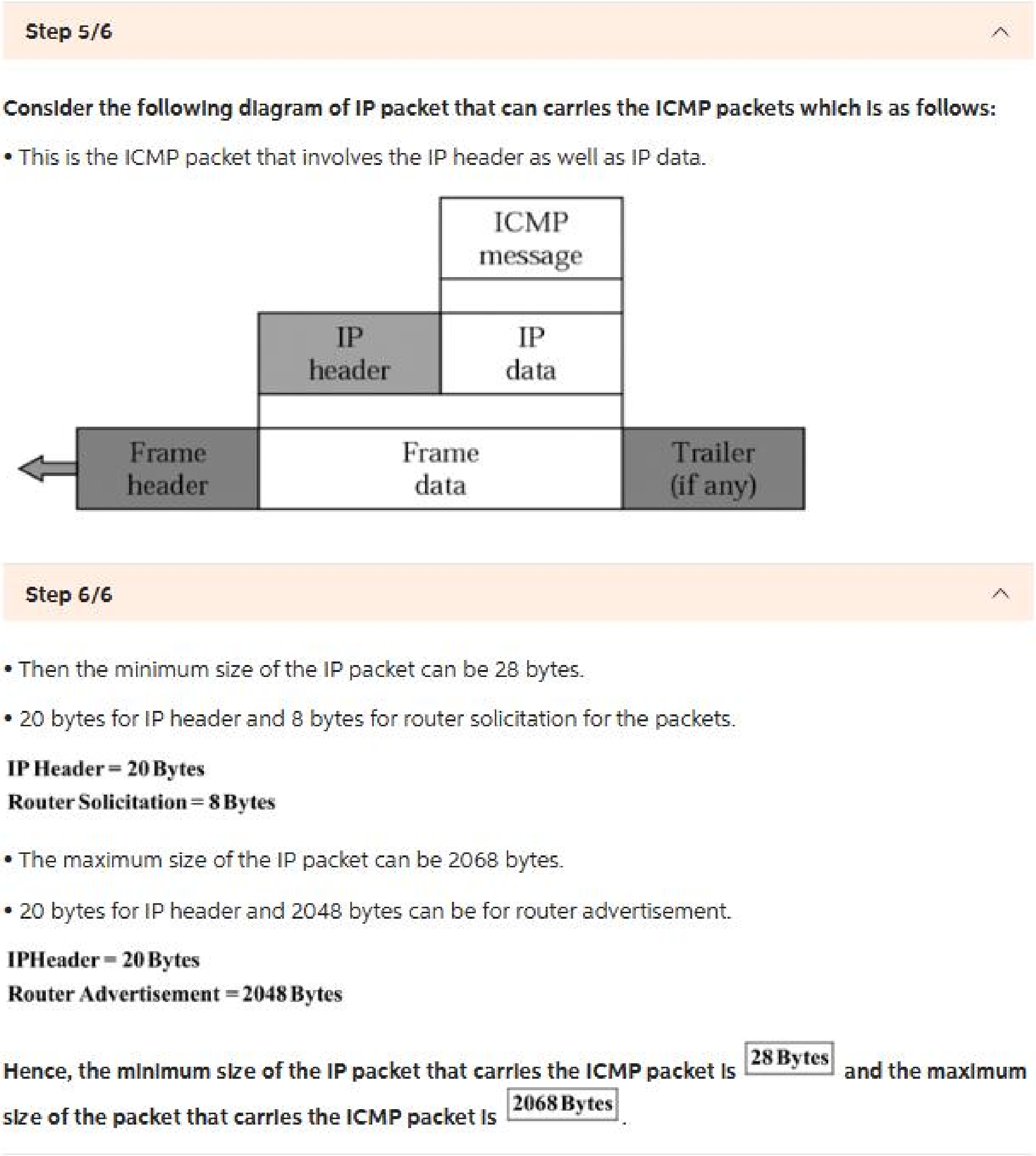
- The maximum size of the ICMP packet will be more than 1500 bytes.

- 1500 bytes can be for router advertisement packets while Ethernet can carry only 1500 bytes of the packet.

Router Advertisement For The Packet = 1500 Bytes .

Hence, the minimum size of the ICMP packet is $\boxed{\textbf{8 Bytes}}$ **and the maximum size of the ICMP packet is** $\boxed{\textbf{1500 Bytes}}$.

11. What is the minimum size of an IP packet that carries an ICMP packet? What is the maximum size?



Step 5/6

Consider the following diagram of IP packet that can carries the ICMP packets which is as follows:

- This is the ICMP packet that involves the IP header as well as IP data.

Step 6/6

- Then the minimum size of the IP packet can be 28 bytes.
- 20 bytes for IP header and 8 bytes for router solicitation for the packets.

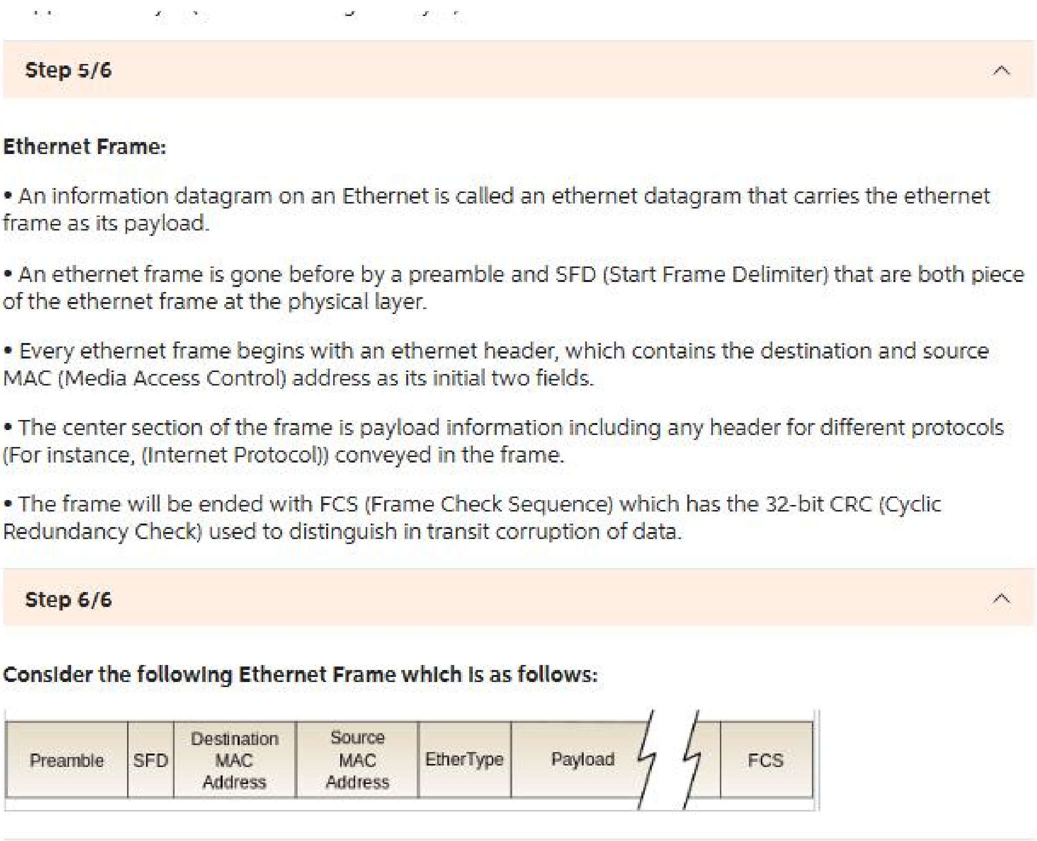
$\textbf{IP Header} = \textbf{20 Bytes}$
$\textbf{Router Solicitation} = \textbf{8 Bytes}$

- The maximum size of the IP packet can be 2068 bytes.
- 20 bytes for IP header and 2048 bytes can be for router advertisement.

$\textbf{IPHeader} = \textbf{20 Bytes}$
$\textbf{Router Advertisement} = \textbf{2048 Bytes}$

Hence, the minimum size of the IP packet that carries the ICMP packet is $\boxed{\textbf{28 Bytes}}$ **and the maximum size of the packet that carries the ICMP packet is** $\boxed{\textbf{2068 Bytes}}$.

12. What is the minimum size of an Ethernet frame that carries an IP packet which in turn carries an ICMP packet? What is the maximum size?



Step 5/6

Ethernet Frame:

• An information datagram on an Ethernet is called an ethernet datagram that carries the ethernet frame as its payload.

• An ethernet frame is gone before by a preamble and SFD (Start Frame Delimiter) that are both piece of the ethernet frame at the physical layer.

• Every ethernet frame begins with an ethernet header, which contains the destination and source MAC (Media Access Control) address as its initial two fields.

• The center section of the frame is payload information including any header for different protocols (For instance, (Internet Protocol)) conveyed in the frame.

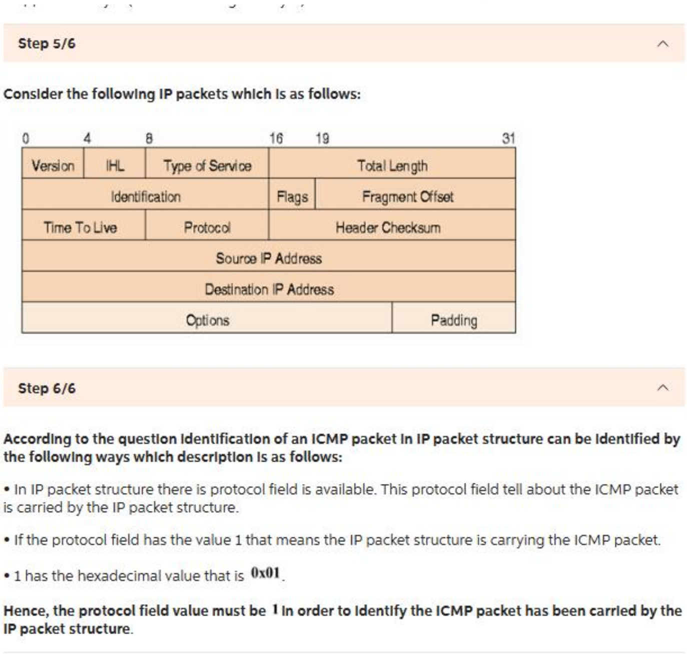
• The frame will be ended with FCS (Frame Check Sequence) which has the 32-bit CRC (Cyclic Redundancy Check) used to distinguish in transit corruption of data.

Step 6/6

Consider the following Ethernet Frame which is as follows:

Preamble	SFD	Destination MAC Address	Source MAC Address	EtherType	Payload	FCS

13. How can we determine if an IP packet is carrying an ICMP packet?



Step 5/6

Consider the following IP packets which is as follows:

0	4	8	16	19 31
Version	IHL	Type of Service	Total Length	
Identification			Flags	Fragment Offset
Time To Live		Protocol	Header Checksum	
Source IP Address				
Destination IP Address				
Options				Padding

Step 6/6

According to the question identification of an ICMP packet in IP packet structure can be identified by the following ways which description is as follows:

• In IP packet structure there is protocol field is available. This protocol field tell about the ICMP packet is carried by the IP packet structure.

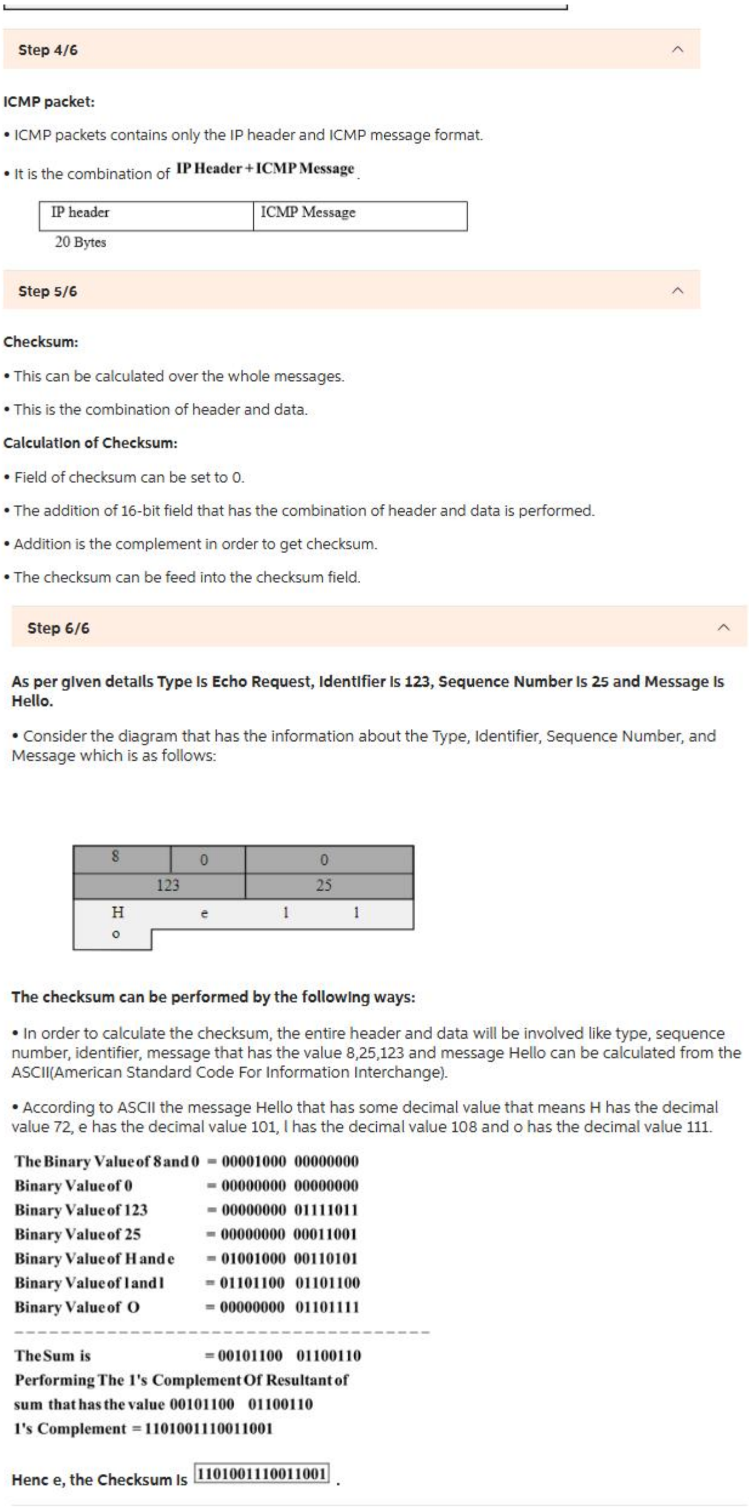
• If the protocol field has the value 1 that means the IP packet structure is carrying the ICMP packet.

• 1 has the hexadecimal value that is **0x01**.

Hence, the protocol field value must be 1 in order to identify the ICMP packet has been carried by the IP packet structure.

14. Calculate the checksum for the following ICMP packet:

Type: Echo Request Identifier: 123 Sequence Number: 25 Message: Hello



Step 4/6

ICMP packet:

- ICMP packets contains only the IP header and ICMP message format.
- It is the combination of **IP Header + ICMP Message**.

IP header	ICMP Message
20 Bytes	

Step 5/6

Checksum:

- This can be calculated over the whole messages.
- This is the combination of header and data.

Calculation of Checksum:

- Field of checksum can be set to 0.
- The addition of 16-bit field that has the combination of header and data is performed.
- Addition is the complement in order to get checksum.
- The checksum can be feed into the checksum field.

Step 6/6

As per given details Type is Echo Request, Identifier is 123, Sequence Number is 25 and Message is Hello.

- Consider the diagram that has the information about the Type, Identifier, Sequence Number, and Message which is as follows:

8	0	0	
123		25	
H	e	1	1
o			

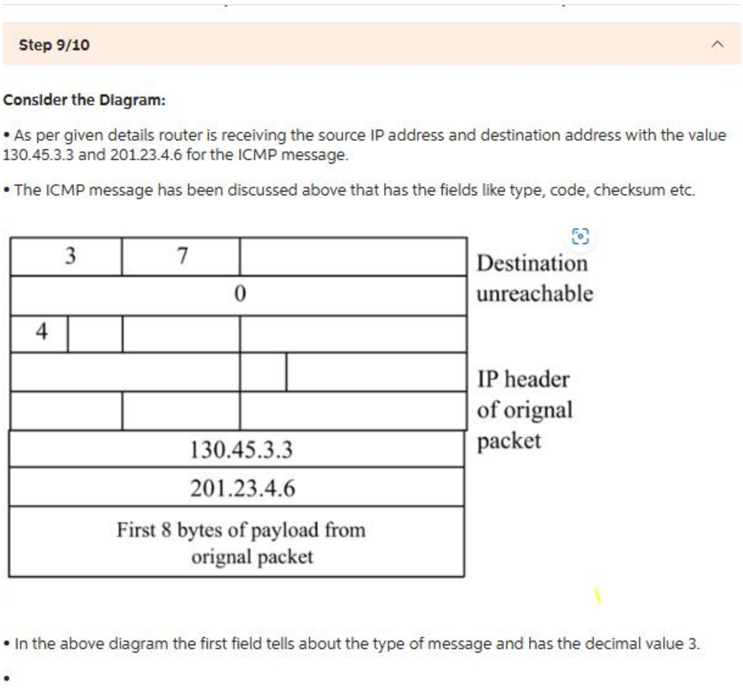
The checksum can be performed by the following ways:

- In order to calculate the checksum, the entire header and data will be involved like type, sequence number, identifier, message that has the value 8,25,123 and message Hello can be calculated from the ASCII(American Standard Code For Information Interchange).
- According to ASCII the message Hello that has some decimal value that means H has the decimal value 72, e has the decimal value 101, l has the decimal value 108 and o has the decimal value 111.

The Binary Value of 8 and 0 = 00001000 00000000
Binary Value of 0 = 00000000 00000000
Binary Value of 123 = 00000000 01111011
Binary Value of 25 = 00000000 00011001
Binary Value of H and e = 01001000 00110101
Binary Value of l and l = 01101100 01101100
Binary Value of O = 00000000 01101111
------------------------------------
The Sum is = 00101100 01100110
Performing The 1's Complement Of Resultant of sum that has the value 00101100 01100110
1's Complement = 1101001110011001

Henc e, the Checksum is $\boxed{1101001110011001}$.

15. A router receives an IP packet with source IP address 130.45.3.3 and destination IP address 201.23.4.6. The router cannot find the destination IP address in its routing table. Fill in the fields (as much as you can) for the ICMP message sent.



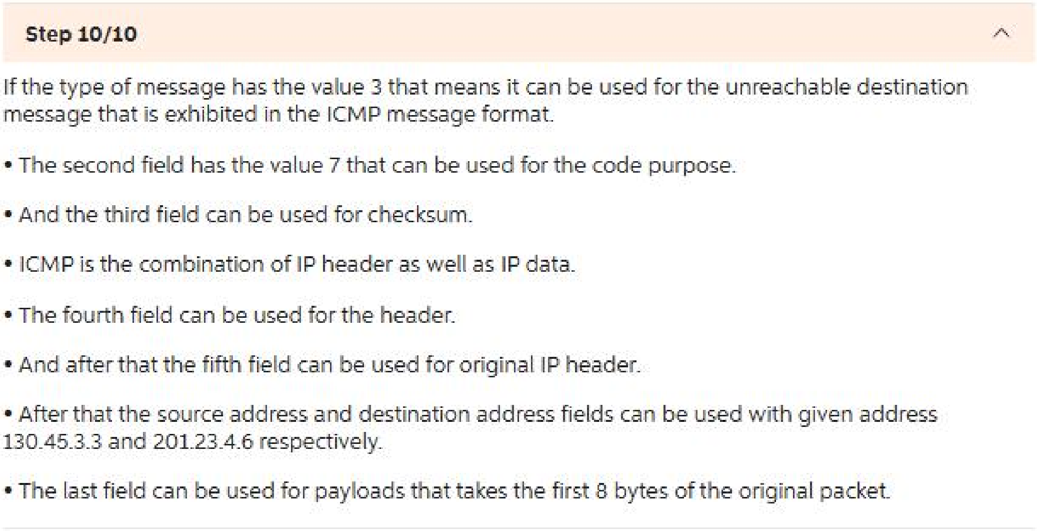
Step 9/10

Consider the Diagram:

- As per given details router is receiving the source IP address and destination address with the value 130.45.3.3 and 201.23.4.6 for the ICMP message.
- The ICMP message has been discussed above that has the fields like type, code, checksum etc.

3
7
0
4
130.45.3.3
201.23.4.6
First 8 bytes of payload from orignal packet
Destination unreachable
IP header of orignal packet

- In the above diagram the first field tells about the type of message and has the decimal value 3.
-

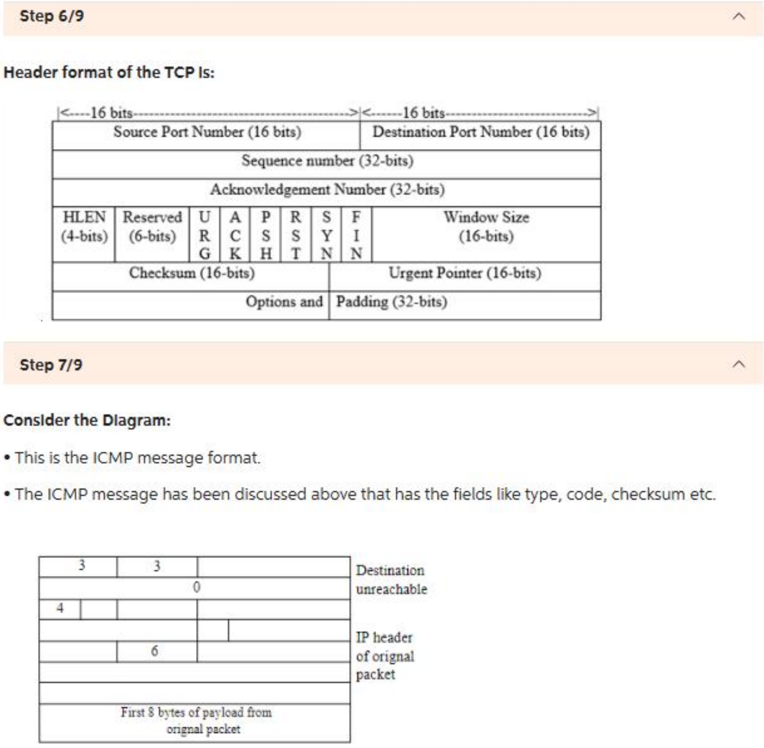


Step 10/10

If the type of message has the value 3 that means it can be used for the unreachable destination message that is exhibited in the ICMP message format.

- The second field has the value 7 that can be used for the code purpose.
- And the third field can be used for checksum.
- ICMP is the combination of IP header as well as IP data.
- The fourth field can be used for the header.
- And after that the fifth field can be used for original IP header.
- After that the source address and destination address fields can be used with given address 130.45.3.3 and 201.23.4.6 respectively.
- The last field can be used for payloads that takes the first 8 bytes of the original packet.

16. TCP receives a segment with destination port address 234. TCP checks and cannot find an open port for this destination. Fill in the fields for the ICMP message sent.



Step 6/9

Header format of the TCP is:

|<----16 bits--------------------------------------->|<------16 bits----------------------------->|

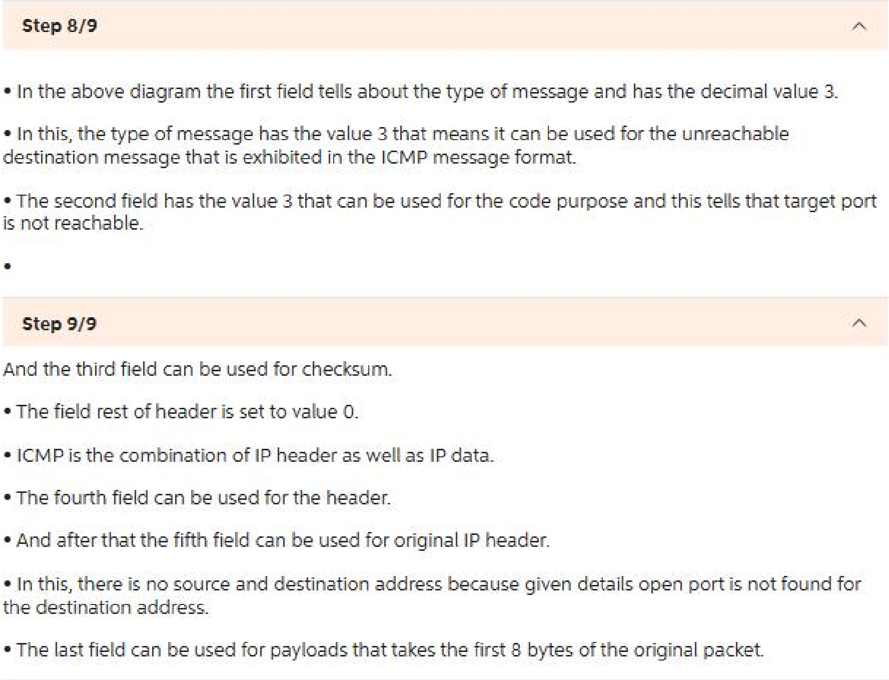
Source Port Number (16 bits)								Destination Port Number (16 bits)
Sequence number (32-bits)								
Acknowledgement Number (32-bits)								
HLEN (4-bits)	Reserved (6-bits)	U R G	A C K	P S H	R S T	S Y N	F I N	Window Size (16-bits)
Checksum (16-bits)						Urgent Pointer (16-bits)		
Options and						Padding (32-bits)		

Step 7/9

Consider the Diagram:

- This is the ICMP message format.
- The ICMP message has been discussed above that has the fields like type, code, checksum etc.

3
3
0
4
6
First 8 bytes of payload from orignal packet
Destination unreachable
IP header of orignal packet



Step 8/9

- In the above diagram the first field tells about the type of message and has the decimal value 3.
- In this, the type of message has the value 3 that means it can be used for the unreachable destination message that is exhibited in the ICMP message format.
- The second field has the value 3 that can be used for the code purpose and this tells that target port is not reachable.
-

Step 9/9

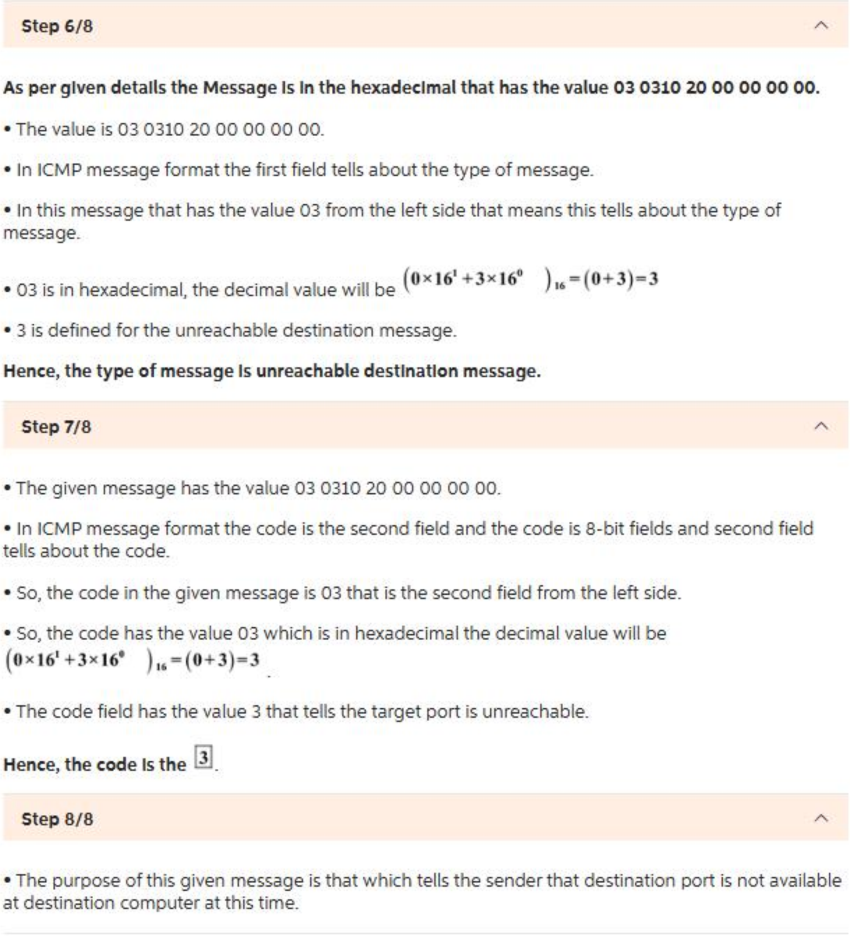
And the third field can be used for checksum.

- The field rest of header is set to value 0.
- ICMP is the combination of IP header as well as IP data.
- The fourth field can be used for the header.
- And after that the fifth field can be used for original IP header.
- In this, there is no source and destination address because given details open port is not found for the destination address.
- The last field can be used for payloads that takes the first 8 bytes of the original packet.

17. An ICMP message has arrived with the header (in hexadecimal):

03 0310 20 00 00 00 00

What is the type of the message? What is the code? What is the purpose of the message?



Step 6/8

As per given details the Message is in the hexadecimal that has the value 03 0310 20 00 00 00 00.

- The value is 03 0310 20 00 00 00 00.
- In ICMP message format the first field tells about the type of message.
- In this message that has the value 03 from the left side that means this tells about the type of message.
- 03 is in hexadecimal, the decimal value will be $(0\times16^1+3\times16^0\quad)_{16}=(0+3)=3$
- 3 is defined for the unreachable destination message.

Hence, the type of message is unreachable destination message.

Step 7/8

- The given message has the value 03 0310 20 00 00 00 00.
- In ICMP message format the code is the second field and the code is 8-bit fields and second field tells about the code.
- So, the code in the given message is 03 that is the second field from the left side.
- So, the code has the value 03 which is in hexadecimal the decimal value will be $(0\times16^1+3\times16^0\quad)_{16}=(0+3)=3$.
- The code field has the value 3 that tells the target port is unreachable.

Hence, the code is the $\boxed{3}$.

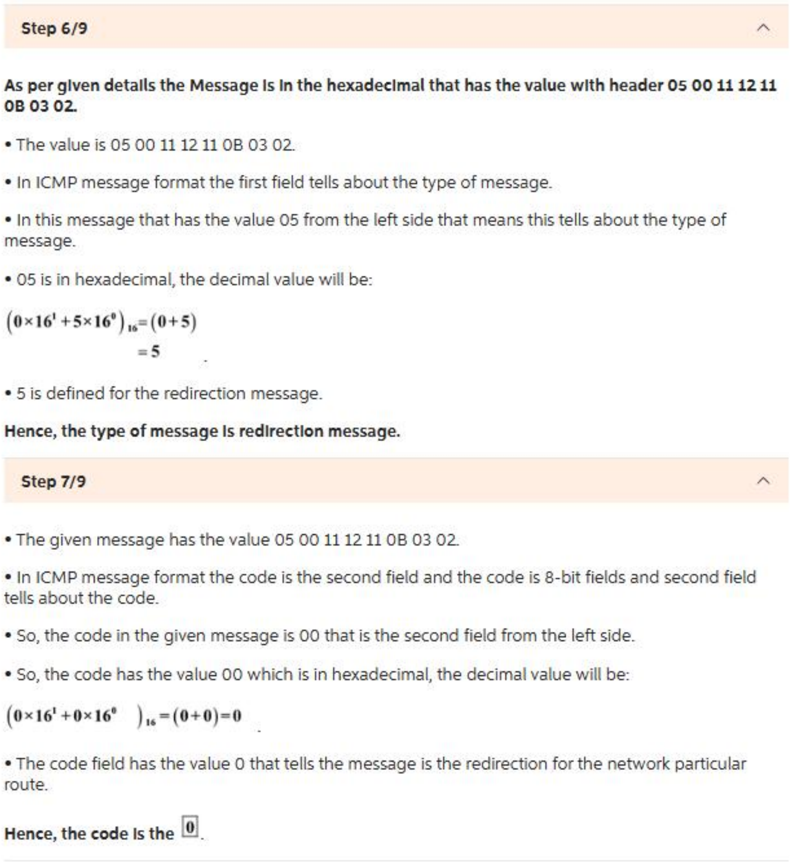
Step 8/8

- The purpose of this given message is that which tells the sender that destination port is not available at destination computer at this time.

18. An ICMP message has arrived with the header (in hexadecimal):

05 00 11 12 11 0B 03 02

What is the type of the message? What is the code? What is the purpose of the message? What is the value of the last 4 bytes? What do the last bytes signify?



Step 6/9

As per given details the Message is in the hexadecimal that has the value with header 05 00 11 12 11 0B 03 02.

- The value is 05 00 11 12 11 0B 03 02.
- In ICMP message format the first field tells about the type of message.
- In this message that has the value 05 from the left side that means this tells about the type of message.
- 05 is in hexadecimal, the decimal value will be:

$$\begin{aligned}\left(0\times16^{1}+5\times16^{0}\right)_{16} &= (0+5)\\ &= 5\end{aligned}$$

- 5 is defined for the redirection message.

Hence, the type of message is redirection message.

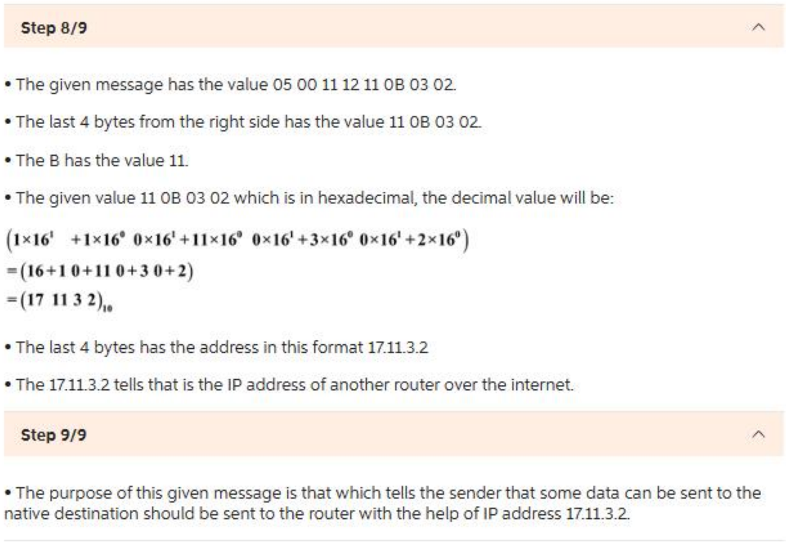
Step 7/9

- The given message has the value 05 00 11 12 11 0B 03 02.
- In ICMP message format the code is the second field and the code is 8-bit fields and second field tells about the code.
- So, the code in the given message is 00 that is the second field from the left side.
- So, the code has the value 00 which is in hexadecimal, the decimal value will be:

$$\left(0\times16^{1}+0\times16^{0}\quad\right)_{16}=(0+0)=0$$

- The code field has the value 0 that tells the message is the redirection for the network particular route.

Hence, the code is the $\boxed{0}$.



Step 8/9

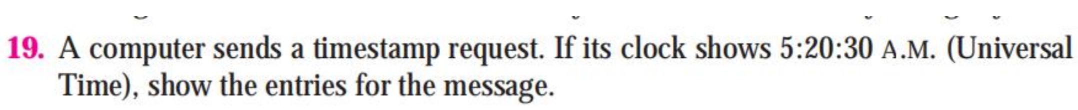
- The given message has the value 05 00 11 12 11 0B 03 02.
- The last 4 bytes from the right side has the value 11 0B 03 02.
- The B has the value 11.
- The given value 11 0B 03 02 which is in hexadecimal, the decimal value will be:

$$\begin{aligned}&\left(1\times16^{1}\quad+1\times16^{0}\ \ 0\times16^{1}+11\times16^{0}\ \ 0\times16^{1}+3\times16^{0}\ \ 0\times16^{1}+2\times16^{0}\right)\\ &=(16+1\ 0+11\ 0+3\ 0+2)\\ &=(17\ \ 11\ 3\ 2)_{10}\end{aligned}$$

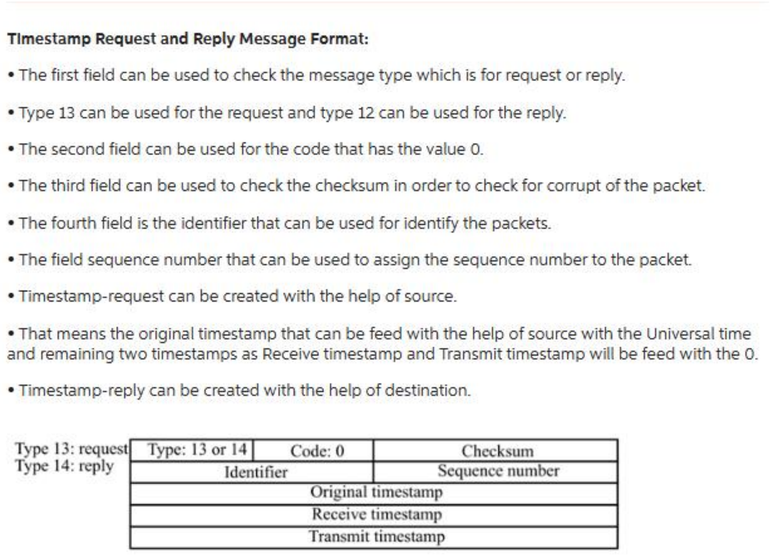
- The last 4 bytes has the address in this format 17.11.3.2
- The 17.11.3.2 tells that is the IP address of another router over the internet.

Step 9/9

- The purpose of this given message is that which tells the sender that some data can be sent to the native destination should be sent to the router with the help of IP address 17.11.3.2.



19. A computer sends a timestamp request. If its clock shows 5:20:30 A.M. (Universal Time), show the entries for the message.

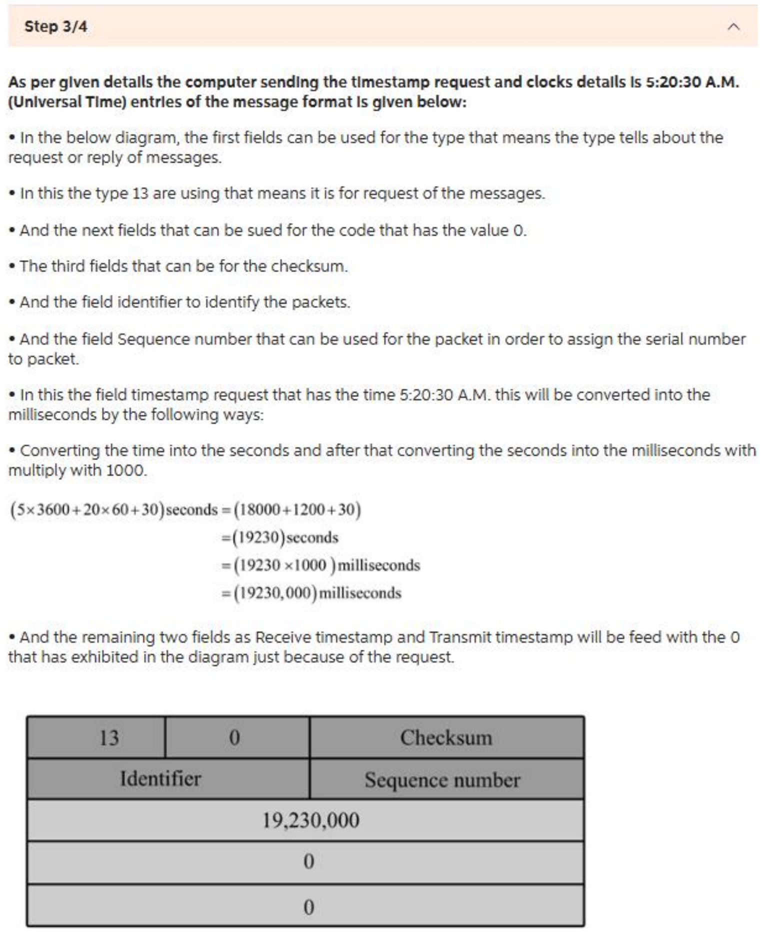


Timestamp Request and Reply Message Format:

- The first field can be used to check the message type which is for request or reply.
- Type 13 can be used for the request and type 12 can be used for the reply.
- The second field can be used for the code that has the value 0.
- The third field can be used to check the checksum in order to check for corrupt of the packet.
- The fourth field is the identifier that can be used for identify the packets.
- The field sequence number that can be used to assign the sequence number to the packet.
- Timestamp-request can be created with the help of source.
- That means the original timestamp that can be feed with the help of source with the Universal time and remaining two timestamps as Receive timestamp and Transmit timestamp will be feed with the 0.
- Timestamp-reply can be created with the help of destination.

Type 13: request
Type 14: reply

Type: 13 or 14	Code: 0	Checksum
Identifier		Sequence number
Original timestamp		
Receive timestamp		
Transmit timestamp		



Step 3/4

As per given details the computer sending the timestamp request and clocks details is 5:20:30 A.M. (Universal Time) entries of the message format is given below:

- In the below diagram, the first fields can be used for the type that means the type tells about the request or reply of messages.
- In this the type 13 are using that means it is for request of the messages.
- And the next fields that can be sued for the code that has the value 0.
- The third fields that can be for the checksum.
- And the field identifier to identify the packets.
- And the field Sequence number that can be used for the packet in order to assign the serial number to packet.
- In this the field timestamp request that has the time 5:20:30 A.M. this will be converted into the milliseconds by the following ways:
- Converting the time into the seconds and after that converting the seconds into the milliseconds with multiply with 1000.

$$\begin{aligned}(5\times3600+20\times60+30)\text{seconds} &= (18000+1200+30)\\ &=(19230)\text{seconds}\\ &=(19230\times1000)\text{milliseconds}\\ &=(19230,000)\text{milliseconds}\end{aligned}$$

- And the remaining two fields as Receive timestamp and Transmit timestamp will be feed with the 0 that has exhibited in the diagram just because of the request.

13	0	Checksum
Identifier		Sequence number
19,230,000		
0		
0		

20. Repeat Exercise 19 for the time of 3:40:30 P.M. (Universal Time).

As per given details referring exercise 19 the computer sending the timestamp request and clocks details is 3:40:30 P.M. (Universal Time) entries of the message format is given below:

• In the below diagram, the first fields can be used for the type that means the type tells about the request or reply of messages.

• In this, the type 13 are using that means it is for request of the messages.

• And the next fields that can be sued for the code that has the value 0.

• The third fields that can be for the checksum.

• And the field identifier to identify the packets.

• And the field Sequence number that can be used for the packet in order to assign the serial number to packet.

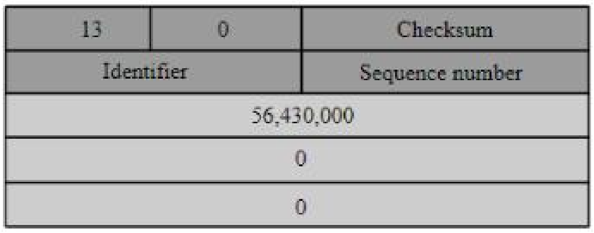
• In this the field timestamp request that has the time 3:40:30 P.M. this will be converted into the milliseconds by the following ways:

• And 3 will converted to the 15 and minute and seconds will be same.

• Converting the time into the seconds and after that converting the seconds into the milliseconds with multiply with 1000.

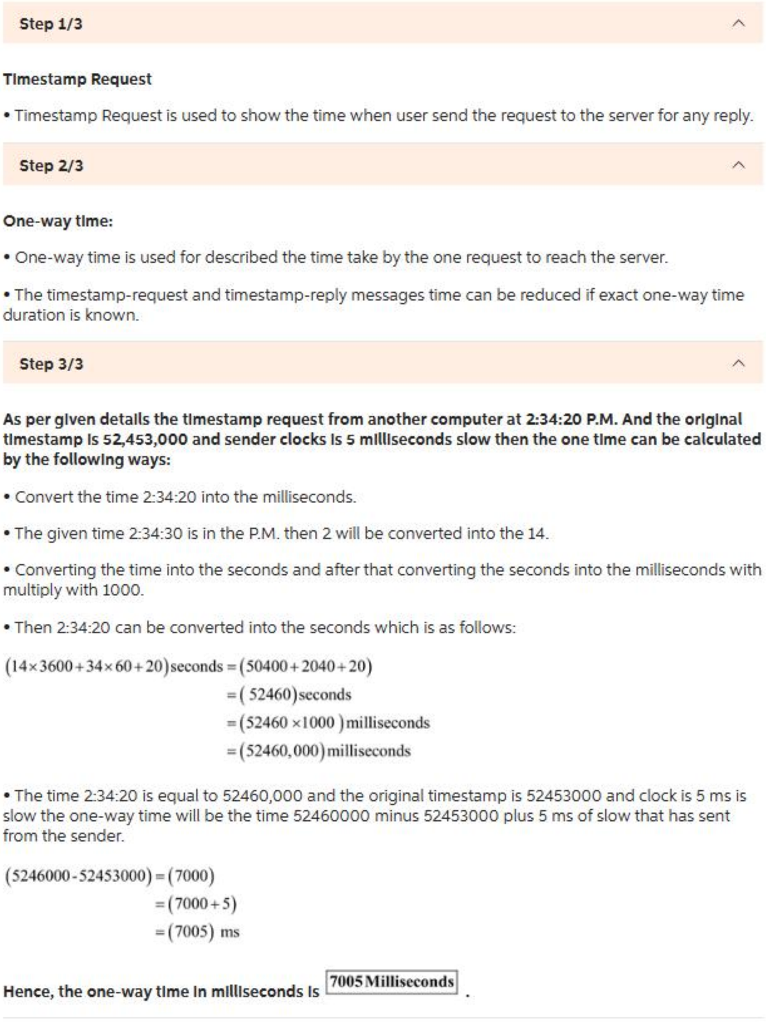
$$\begin{aligned}(15\times3600+40\times60+30)\text{seconds} &= (54000+2400+30)\\ &= (\ 56430)\text{seconds}\\ &= (56430\ \times1000\ )\text{milliseconds}\\ &= (56430,000)\text{milliseconds}\end{aligned}$$

• And the remaining two fields as Receive timestamp and Transmit timestamp will be feed with the 0 that has exhibited in the diagram just because of the request.



13	0	Checksum
Identifier		Sequence number
56,430,000		
0		
0		

21. A computer receives a timestamp request from another computer at 2:34:20 P.M. The value of the original timestamp is 52,453,000. If the sender clock is 5 ms slow, what is the one-way time?



Step 1/3

Timestamp Request

- Timestamp Request is used to show the time when user send the request to the server for any reply.

Step 2/3

One-way time:

- One-way time is used for described the time take by the one request to reach the server.

- The timestamp-request and timestamp-reply messages time can be reduced if exact one-way time duration is known.

Step 3/3

As per given details the timestamp request from another computer at 2:34:20 P.M. And the original timestamp is 52,453,000 and sender clocks is 5 milliseconds slow then the one time can be calculated by the following ways:

- Convert the time 2:34:20 into the milliseconds.

- The given time 2:34:30 is in the P.M. then 2 will be converted into the 14.

- Converting the time into the seconds and after that converting the seconds into the milliseconds with multiply with 1000.

- Then 2:34:20 can be converted into the seconds which is as follows:

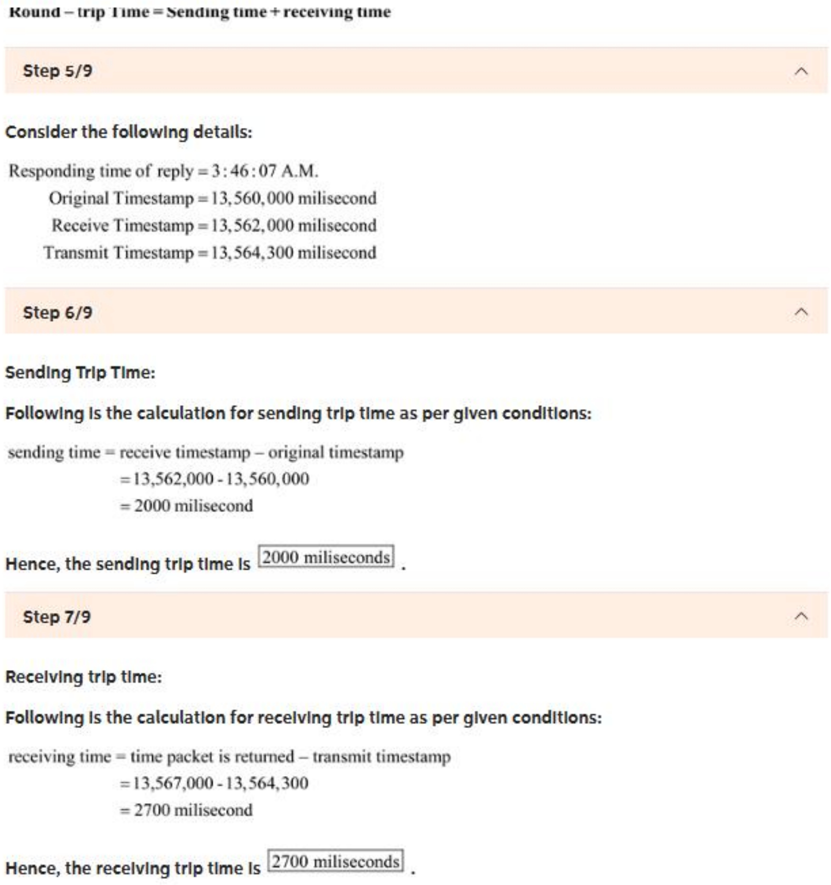
$$\begin{aligned}(14\times3600+34\times60+20)\text{seconds} &= (50400+2040+20)\\ &= (\ 52460)\text{seconds}\\ &= (52460\times1000\ )\text{milliseconds}\\ &= (52460{,}000)\text{milliseconds}\end{aligned}$$

- The time 2:34:20 is equal to 52460,000 and the original timestamp is 52453000 and clock is 5 ms is slow the one-way time will be the time 52460000 minus 52453000 plus 5 ms of slow that has sent from the sender.

$$\begin{aligned}(5246000-52453000) &= (7000)\\ &= (7000+5)\\ &= (7005)\ \text{ms}\end{aligned}$$

Hence, the one-way time in milliseconds is $\boxed{\textbf{7005 Milliseconds}}$.

22. A computer sends a timestamp request to another computer. It receives the corresponding timestamp reply at 3:46:07 A.M. The values of the original timestamp, receive timestamp, and transmit timestamp are 13,560,000, 13,562,000, and 13,564,300, respectively. What is the sending trip time? What is the receiving trip time? What is the round-trip time? What is the difference between the sender clock and the receiver clock?



$\textbf{Round} - \textbf{trip Time} = \textbf{Sending time} + \textbf{receiving time}$

Step 5/9

Consider the following details:

$$\begin{aligned} \text{Responding time of reply} &= 3:46:07 \text{ A.M.} \\ \text{Original Timestamp} &= 13,560,000 \text{ milisecond} \\ \text{Receive Timestamp} &= 13,562,000 \text{ milisecond} \\ \text{Transmit Timestamp} &= 13,564,300 \text{ milisecond} \end{aligned}$$

Step 6/9

Sending Trip Time:

Following is the calculation for sending trip time as per given conditions:

$$\begin{aligned} \text{sending time} &= \text{receive timestamp} - \text{original timestamp} \\ &= 13{,}562{,}000 - 13{,}560{,}000 \\ &= 2000 \text{ milisecond} \end{aligned}$$

Hence, the sending trip time is $\boxed{2000 \text{ miliseconds}}$.

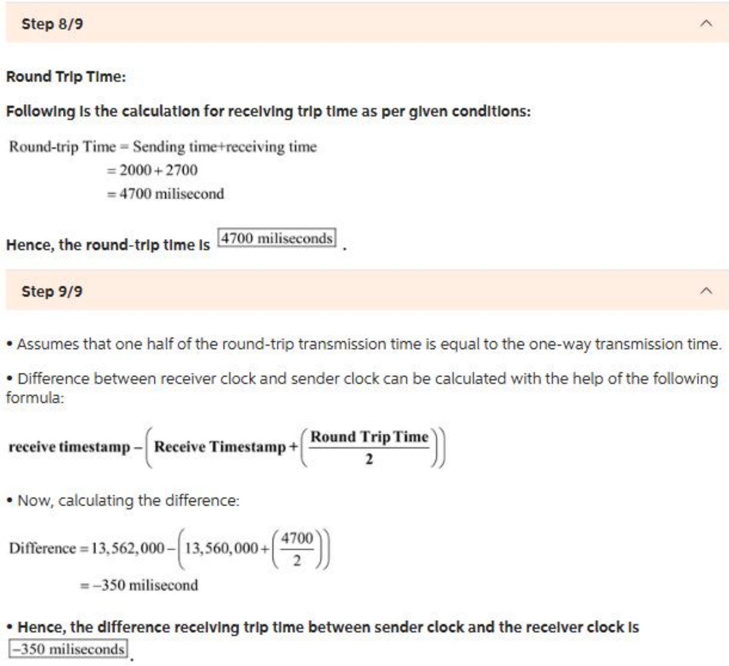
Step 7/9

Receiving trip time:

Following is the calculation for receiving trip time as per given conditions:

$$\begin{aligned} \text{receiving time} &= \text{time packet is returned} - \text{transmit timestamp} \\ &= 13{,}567{,}000 - 13{,}564{,}300 \\ &= 2700 \text{ milisecond} \end{aligned}$$

Hence, the receiving trip time is $\boxed{2700 \text{ miliseconds}}$.



Step 8/9

Round Trip Time:

Following is the calculation for receiving trip time as per given conditions:

$$\begin{aligned} \text{Round-trip Time} &= \text{Sending time} + \text{receiving time} \\ &= 2000 + 2700 \\ &= 4700 \text{ milisecond} \end{aligned}$$

Hence, the round-trip time is $\boxed{4700 \text{ miliseconds}}$.

Step 9/9

- Assumes that one half of the round-trip transmission time is equal to the one-way transmission time.
- Difference between receiver clock and sender clock can be calculated with the help of the following formula:

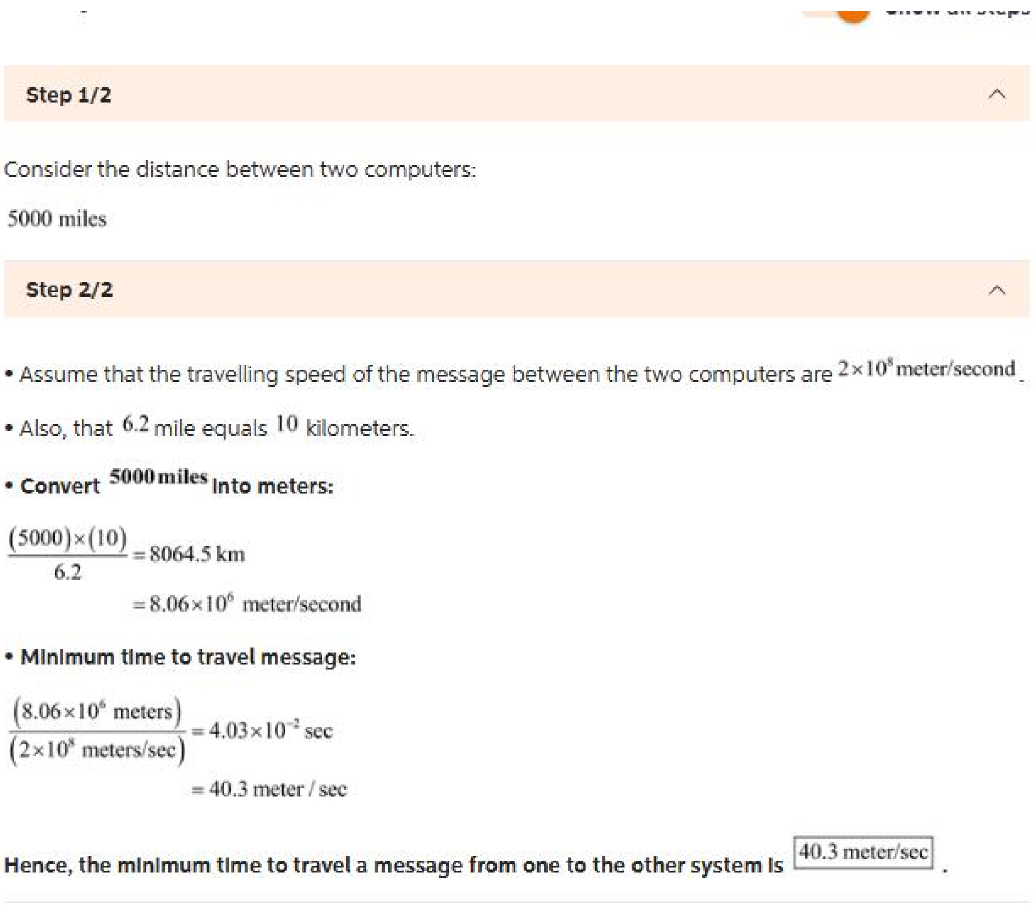
$$\textbf{receive timestamp} - \left(\textbf{Receive Timestamp} + \left(\frac{\textbf{Round Trip Time}}{\textbf{2}}\right)\right)$$

- Now, calculating the difference:

$$\begin{aligned} \text{Difference} &= 13{,}562{,}000 - \left(13{,}560{,}000 + \left(\frac{4700}{2}\right)\right) \\ &= -350 \text{ milisecond} \end{aligned}$$

- **Hence, the difference receiving trip time between sender clock and the receiver clock is** $\boxed{-350 \text{ miliseconds}}$.

23. If two computers are 5000 miles apart, what is the minimum time for a message to go from one to the other?



Step 1/2

Consider the distance between two computers:

5000 miles

Step 2/2

- Assume that the travelling speed of the message between the two computers are 2×10^8 meter/second.
- Also, that 6.2 mile equals 10 kilometers.
- **Convert 5000 miles into meters:**

$$\frac{(5000)\times(10)}{6.2}=8064.5\text{ km}$$

$$=8.06\times10^6\text{ meter/second}$$

- **Minimum time to travel message:**

$$\frac{(8.06\times10^6\text{ meters})}{(2\times10^8\text{ meters/sec})}=4.03\times10^{-2}\text{ sec}$$

$$=40.3\text{ meter / sec}$$

Hence, the minimum time to travel a message from one to the other system is $\boxed{40.3\text{ meter/sec}}$.