

## 1. Is registration required if the mobile host acts as a foreign agent? Explain your answer.

### Step 1/3

- The **registration request** is the request which is sent to the foreign agent from the mobile host to register its care of address.
- It also announces address of the home agent and its home address.

### Step 2/3

- A mobile host can move from one place to another place. In this case, the address of IP needs to be changed.
- The most suitable approach for mobile host is to use two addresses: original address of mobile host i.e. home address and temporary address of mobile host i.e. care-of-address.
- When host or node moves to another place the care-of-address must be changed. It is related to foreign network, and determines moved host.
- To make the address changes transparent to the users, the network user uses: foreign agent and home agent.
- Router attached to home address of home agent and router connected to foreign address which is the foreign agent.
- The foreign agent accepts and transfers packet to the mobile host which is sent by the home agent.
- Mobile host must act as foreign agent.
- However, to act as foreign agent, mobile host must receive care-of-address by itself with the help of DHCP.
- Mobile host needs extra software to communicate with the home agent.

### Step 3/3

**Yes, registration is required if mobile acts as foreign agent it must register itself.**

- Mobile host, to act as foreign network, needs to communicate with home agent and also communicate with home address and care-of-address.
- Registration is required for the mobile host because mobile host needs to identify itself to the home agent.

## 2. Redraw Figure 10.7 if the mobile host acts as a foreign agent.

### Step 1/3

Refer to figure 10.7 of chapter 10 from the textbook.

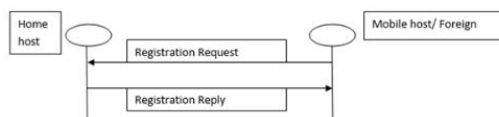
### Step 2/3

- The figure sends packet from remote host to home agent.
- Remote host uses its address as source address and home address of mobile as destination address.
- After receiving the packet from remote host, the home agent sends the packet to foreign agent using tunneling concept.
- After receiving packet from home agent, the foreign agent removes the original packet and finds the care-of-address.
- The mobile host sends the packet to remote host in a normal way.

### Step 3/3

If the mobile acts as foreign agent, it removes the foreign network between the mobile host and remote host. Then mobile host can send request directly to the next host.

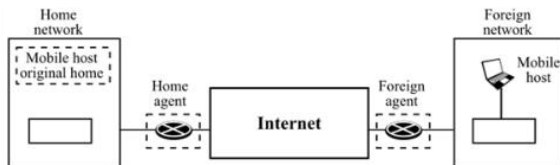
**Thus, after removing all except home host or mobile host (foreign), the figure is shown below:**



3. Create a home agent advertisement message using 1456 as the sequence number and a lifetime of 3 hours. Select your own values for the bits in the code field. Calculate and insert the value for the length field.

Step 5/7

Home Agent and Foreign Agent Diagram:



Step 6/7

Agent Advertisement Format:

ICMP Advertisement Message			
Type	Length	Sequence number	
Lifetime		Code	Reserved
Care of addresses (foreign agent only)			

Step 7/7

As per given details there is home agent advertisement has the sequence number 1456 and has the lifetime 3 hours. The description of the all fields of home agent with corresponding value which is as follows:

- The first field tells about the ICMP advertisement that will be used for both home agent as well as foreign agent.
- The second field tells about the type that takes the 8-bit field that has the value 16.
- Then next field tells about the length that takes the 8-bit length and has the value 8.
- Then next field tells about the sequence number as per given detail the value is 1456 and takes the 16-bits field.
- Then next field tells about the lifetime and as per given details the value is 3 hours

1 minute = 60 seconds

since, 1 hour = 60 minute

then 60 minute =  $60 \times 60 = 3600$  seconds = 1 hours

then 3 hours =  $3600 \times 3 = 10800$  seconds

- Then next field tells about the code and it takes the 8-bit flag that means 1 is use for set and 0 for reset that has the table value 0.

- And the last field that can be used for Reserved purpose in the home agent.

- This does not contain the care of address.

ICMP Advertisement Message			
16	8	1456	
10800		0	Reserved

4. Create a foreign agent advertisement message using 1672 as the sequence number and a lifetime of 4 hours. Select your own values for the bits in the code field. Use at least three care-of addresses of your choice. Calculate and insert the value for the length field.

Step 7/7

As per given details there is foreign agent advertisement has the sequence number 1672 and has the lifetime 4 hours. The description of the all fields of foreign agent with corresponding value which is as follows:

- The first field tells about the ICMP advertisement that will be used for both home agent as well as foreign agent.
- The second field tells about the type that takes the 8-bit field that has the value 16.
- Then next field tells about the length that takes the 8-bit length and has the value 20.
- Then next field tells about the sequence number as per given detail the value is 1672 and takes the 16-bits field.
- Then next field tells about the lifetime and as per given details the value is 4 hours and has the value 14400 in seconds which can be computed as follows:

1 minute = 60 seconds

since, 1 hour = 60 minutes

then 60 minutes =  $60 \times 60 = 3600$  seconds = 1 hour

then 4 hours =  $3600 \times 4 = 14400$  seconds

- Then next field tells about the code and it takes the 8-bit flag that means 1 is used for set and 0 for reset that has the table value 0.
- And the next field that can be used for Reserved purpose in the foreign agent.
- And the last field tells about the care-of-address that has the address which is as follows:
- 128.1.1.2
- 128.1.1.3

ICMP Advertisement Message			
16	20	1672	
14400		0	Reserved
128.1.1.12			
128.1.1.13			
128.1.1.14			

- 128.1.1.4

## 5. Discuss how the ICMP router solicitation message can also be used for agent solicitation. Why are there no extra fields?

### Step 1/2

There are three phases is used in mobile communication, first phase is agent discovery, second phase is registration, and third phase is data transfer.

**Agent discovery** defines two types of discovery first is solicitation and advertisement. Mobile host discover home agent and home agent discover the foreign agent.

- Agent solicitation is initiated if the host moves to a new network and has not received agent advertisement.
- Agent solicitation uses Internet Control Message Protocol (ICMP) to inform that needs assistance or help.

### Step 2/2

**There are no extra fields because the agent looks for the information and agents own address is included in the message.**

- If the mobile host acts as agent, it does not use any new packet type of agent solicitation then it uses ICMP message solicitation packet.

## 6. Which protocol is the carrier of the agent advertisement and solicitation messages?

### Step 1/5

There are three phases is used in mobile communication, first phase is agent discovery, second phase is registration, and third phase is data transfer.

### Step 2/5

**Agent discovery** have two phases, first, before leaving its home network, the mobile host must determine the home agent.

- Second, after it has been moved to foreign network, the mobile host must determine foreign agent.
- The discovery contains two types of messages: advertisement and solicitation.

### Step 3/5

The router advertises its presence on network using Internet Control Message Protocol (ICMP) router advertisement.

- It can also make changes to the agent advertisement to the packets if, it acts as an agent.

### Step 4/5

**Agent solicitation** is initiated if the host moves to a new network and has not received agent advertisement.

- Agent solicitation uses ICMP to inform that needs assistance or help.

### Step 5/5

**Hence, the carrier of the agent solicitation and advertisement message is Internet Control Message Protocol (ICMP).**



7. Show the encapsulation of the advertisement message in Exercise 3 in an IP data-gram. What is the value for the protocol field?

Step 2/4

The format of agent advertisement of Internet Control Message Protocol (ICMP) is as follows:

ICMP Advertisement Message			
Type	Length	Sequence Number	
Lifetime		Code	Reserved
Care-of-address (foreign agent only)			

- The 8-bit Type field is set 16.
- The 8-bit length field represents extension message's length.
- Message number is hold by the 16-bit Sequence Number field.
- The number of seconds during which agent will accept the request is defined by Lifetime.
- The 8-bit Code field is either set 0 or 1.
- Care-of-address shows the list of address used as care-of-address.

Step 3/4

The fields are fill with specified values:

4	5	0	44	
42			0	0
15	1		Header Checksum	
Source Address				
Destination Address				
ICMP				
Advertisement Message				
16	8		1456	
10800			0	Reserved

- Version field uses IP4.
- The length of header is 5.
- The type is service is 0.
- Identification is 42 and length of message is 44.
- Flag is 0 (reserved) and fragment offset is 0.
- Time to live for a message on a network is 15 sec.
- In the given question, Sequence number is 1456 and Lifetime is 3 hours or 10800 seconds.
- Code is 00 because registration is required.
- Type is set to be 16. Size of length is 8-bit.
- Since, agent itself acts as home agent there is no foreign address.

Step 4/4

Hence, the value of protocol field is set to 1 which indicates ICMP.

8. Explain why the registration request and reply are not directly encapsulated in an IP datagram. Why is there a need for the UDP user datagram?

Step 1/5

- A **registration request** is transfer to the foreign agent from the mobile host to register its care-of address. It also announces home agent address and its home address.
- A **registration reply** is sent to the foreign agent from the home agent and then conveyed to the mobile host. It approves or disapprove the registration request.

Step 2/5

**UDP** is an unreliable, connectionless, transport layer protocol. It stands for user datagram protocol (UDP).

- It is used for the process with the mechanism of error control and flow control.
- UDP uses 69 port number for the Trivial File Transfer Protocol
- The sender sends the data packets to the receiver while receiver does not send acknowledgement to the sender. That's why it is an unreliable protocol.

Step 3/5

**User datagram** is the UDP packet, it contains 8 bytes of header and data which is sending to the receiver side.

- The length of UDP packet is maximum to 65535 bytes.
- UDP packets are encapsulated with IP datagram with length 65535bytes. IP fields consist header length and total length.
- At the receiver side, to calculate the UDP length of the data from provided information of UDP user datagram.

Step 4/5

**The registration request and reply are not directly encapsulated in the program because:**

- The agent runs the server program that is running continuously while waiting for registration message.

Step 5/5

**There is a need of UDP user datagram because:**

- This type of server programs needs a well-known port and transport layer protocols to support it. These well-known port and transport layer protocols are available in UDP.

9. We have the following information shown below. Show the contents of the IP datagram header sent from the remote host to the home agent.

**Mobile host home address: 130.45.6.7/16**  
**Mobile host care-of address: 14.56.8.9/8**  
**Remote host address: 200.4.7.14/24**  
**Home agent address: 130.45.10.20/16**  
**Foreign agent address: 14.67.34.6/8**

#### Step 1/2

The general format of IP datagram format is as follows:

Version	Header	Type of Service	Length	
Identification			Flags	Fragment Offset
Time to live	Protocol		Header Checksum	
Source Address				
Destination Address				
Data				

- Version field defines the version of IP used.
- Header field specifies the length of header in 32-bit words.
- The type of service field provides information about the quality of service.
- The 16-bit length field gives the length of datagram
- The 16-bit identification field contains fragment common to particular message.
- Flags specifies whether the fragment is reserved or DF (should not be fragmented) or MF (tells about the last message).
- The fragment offset indicates offset when message is fragmented.
- Time to live field represents the time that is allowed to live in the network.
- The protocol specifies the protocol used.
- Basic protection against corruption in transmission is provided by header checksum.
- Source address is the 32-bit field specifies the origin of the message.
- Destination message gives the address of the destination.

#### Step 2/2

The format of the IP datagram header sent from the remote host to home agent is as follows:

4	5	0	Length	
42			0	0
15	Protocol		Header Checksum	
200.4.7.14				
130.45.10.20				
Data				

- Since, the source address is remote host address 200.4.7.14 and destination address is home agent 130.45.10.20.

- Version 4 is used Internet protocol. Header uses 32-bit words.

Then, length of header is h:

$$2^h = 32$$

$$= 2^5$$

Thus,

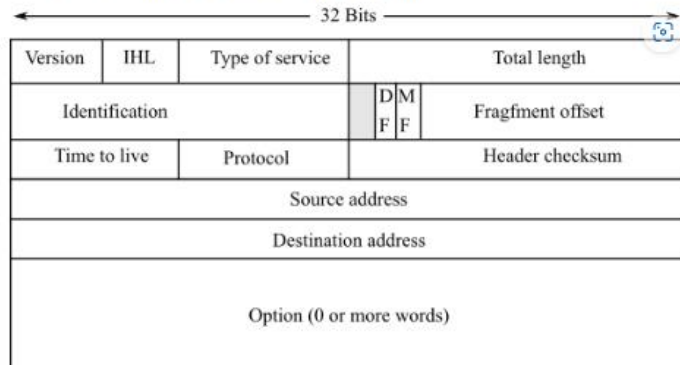
$$h = 5$$

- Time to live on network is 15 seconds.
- Type of service is 0.
- Identification used is 42.

**10.** Using the information in Exercise 9, show the contents of the IP datagram sent by the home agent to the foreign agent. Use tunneling.

**IP datagram Diagram:**

- This is the complete structure of the IP datagram.



**Step 7/9**

As per given details the from the exercise 9 the Information is as follows:

Consider the Information:

Mobile host home address: 130.45.6.7/16

Mobile host care-of-address: 14.56.8.9/8

Remote host address: 200.4.7.14/24

Home agent address: 130.45.10.20/16

Foreign agent address: 14.67.34.6/8

**Step 8/9**

• Before starting, in the IP datagram there is only two main fields which is **IP header** and **data** and IP header will be divided into many parts which description is as follows:

- In the below table the first field tells about the version which has the value 4.
- The next field tells about the header length and has the value 5.
- The next field tells about the type of services and has the value 0.
- The next field tells about the total length.
- The next field tells about the identification and has the value 107 that recognize the datagram.
- The next field tells about the DF (Do Not Fragment) and MF (More Fragment) and has the value 0.
- The next field tells about the Fragment offset and that has the value 0.
- The next field tells about the Time to live and has the value 15.
- The next field tells about the Protocol.
- The next field tells about the header checksum.
- The next field tells about the home agent address which is 130.45.10.20/16.
- The next field tells about the foreign agent address which is 14.67.34.6/8.
- first field tells about the version which has the value 4.
-



**Step 9/9**

The next field tells about the header length and has the value 5.

- The next field tells about the type of services and has the value 0.
- The next field tells about the total length.
- The next field tells about the identification and has the value 42 that recognize the datagram.
- The next field tells about the DF (Do Not Fragment) and MF (More Fragment) and has the value 0.
- The next field tells about the Fragment offset and that has the value 0.
- The next field tells about the Time to live and has the value 15.
- The next field tells about the Protocol.
- The next field tells about the header checksum.
- The next field tells about the remote host address which is 200.4.7.14/24.
- The next field tells about the mobile host home address which is 130.45.6.7/16.
- And the last field tells about the only data.

4	5	0	length	
107			0	0
15	Protocol		Header Checksum	
130.45.10.20				
14.67.34.6				
4	5	0	length	
42			0	0
15	Protocol		Header Checksum	
200.4.7.14				
130.45.6.7				
Data				

11. Using the information in Exercise 9, show the contents of the IP datagram sent by the foreign agent to the mobile host.

Step 7/9

As per given details the from the exercise 9 the information is as follows:

Consider the information:

Mobile host home address: 130.45.6.7/16

Mobile host care-of-address: 14.56.8.9/8

Remote host address: 200.4.7.14/24

Home agent address: 130.45.10.20/16

Foreign agent address: 14.67.34.6/8

Step 8/9

• Before starting, in the IP datagram there are only two main fields which are **IP header** and **data** and the IP header will be divided into many parts whose description is as follows:

- In the below table the first field tells about the version which has the value 4.
- The next field tells about the header length and has the value 5.
- The next field tells about the type of services and has the value 0.
- The next field tells about the total length.
- The next field tells about the identification and has the value 207 that recognizes the datagram.
- The next field tells about the DF (Do Not Fragment) and MF (More Fragment) and has the value 0.
- The next field tells about the fragment offset and that has the value 0.
- The next field tells about the time to live and has the value 15.
- The next field tells about the protocol.
- The next field tells about the header checksum.
- The next field tells about the address which is 14.67.34.30.
- The next field tells about the mobile host care-of-address which is 14.56.8.9/8.
- The first field tells about the version which has the value 4.
- The next field tells about the header length and has the value 5.
- 

Step 9/9

The next field tells about the type of services and has the value 0.

- The next field tells about the total length.
- The next field tells about the identification and has the value 42 that recognizes the datagram.
- The next field tells about the DF (Do Not Fragment) and MF (More Fragment) and has the value 0.
- The next field tells about the fragment offset and that has the value 0.
- The next field tells about the time to live and has the value 15.
- The next field tells about the protocol.
- The next field tells about the header checksum.
- The next field tells about the remote host address which is 200.4.7.14.
- The next field tells about the mobile host home address which is 130.45.6.7.
- And the last field tells about the only data.

4	5	0	length	
207			0	0
15	Protocol		Header Checksum	
14.67.34.30				
14.56.8.9				
4	5	0	length	
42			0	0
15	Protocol		Header Checksum	
200.4.7.14				
130.45.6.7				
Data				

**12. Using the information in Exercise 9, show the contents of the IP datagram sent by the mobile host to the remote host.**

**Step 1/3**

Refers to the exercise 9 of chapter of the textbook to complete information.

**Step 2/3**

The general format of IP datagram format is as follows:

Version	Header	Type of Service	Length	
Identification			Flags	Fragment Offset
Time to live	Protocol		Header Checksum	
Source Address				
Destination Address				
Data				

- Version field defines the version of IP used.
- Header field specifies the length of header in 32-bit words.
- The type of service field provides information about the quality of service.
- The 16-bit length field gives the length of datagram
- The 16-bit identification field contains fragment common to particular message.
- Flags specifies whether the fragment is reserved or DF (should not be fragmented) or MF (tells about the last message).
- The fragment offset indicates offset when message is fragmented.
- Time to live field represents the time that is allowed to live in the network.
- The protocol specifies the protocol used.
- Basic protection against corruption in transmission is provided by header checksum.
- Source address is the 32-bit field specifies the origin of the message.
- Destination message gives the address of the destination.
- The data field contains the data sent or received.

**Step 3/3**

The format of the IP datagram header sent from the mobile host to remote host is as follows:

4	5	0	Length
42	0	0	
15	Protocol	Header Checksum	
130.45.6.7			
200.4.7.14			
Data			

- Since, the destination address is remote host address 200.4.7.14 and source address is mobile host home 130.45.6.7.
- Time to live on network is 15 seconds. Version 4 is used and header is 5.
- Type of service is 0. Identification used is 42.

**13. What type of inefficiency do we have in Exercise 9? Explain your answer.**

**Step 1/3**

Refers to the exercise 9 of the chapter 10 of the textbook.

**Step 2/3**

- Inefficiency in mobile IP are of two types: double crossing (2X) and triangle routing and this routing is also called dog-leg routing.
- Double crossing inefficiency arises if remote host established connection with a mobile host then this mobile host has placed to same network like remote host.
- Triangle routing comes in less severe case.
- It occurs if remote host established connection with mobile host which is not attached to different network.
- In this case, if mobile host sends data packet to remote host that means efficiency does not exist in it.
- But, if remote host sends data packet to the mobile host, then data packet first received by the home agent and after that it received by the mobile host.

**Step 3/3**

**Hence, the user has triangle routing types of Inefficiency in exercise 9 because:**

- Whenever mobile host sends data packets towards the remote host, it goes normally.
- But, if remote host sends data to next host i.e. mobile host, then data received by the home agent and then it received by the mobile host.
- This inefficiency is triangle or dog leg routing.
- The packet has to travel the extra distance of two sides of triangle than one side of the triangle. This give rise to the inefficiency.