1. Exactly describe why we cannot use the CIDR notation for the following blocks in Table 12.1:
   a. AD HOC block with the range 224.0.2.0 to 224.0.255.255.
   b. The first reserved block with the range 224.3.0.0 to 231.255.255.255.
   c. The second reserved block with the range 234.0.0.0 to 238.255.255.255

Step 1/7

CIDR:

• This stands for Classless Inter-Domain Routing.

• CIDR is a set of standard internet protocol that can be used to give unique identification number to the network as well as to devices.

• In the CIDR standard, the first block of an IP address is prefix in order to identify the network address.

• Before CIDR, a DNS (Domain Name System) was established for classful routing systems were used to an IP address in order to identify the network address. After that CIDR was discovered.

• The prefix part is used by host computer for transmitting the packets to its destination computer.

• CIDR removed early version of the classes which name is as follows:

• There are five classes defined in computer networking and using the three classes and remaining two classes is for future use and their range which are as follows:

• **Class A:** This has the range 0-127.

• **Class B:** This has the range 128-191.

• **Class C:** This has the range 192-223.

• **Class D:** This has the range 224-239. This can be used for multicasting.

• **Class E:** This has the range 240-255.This is reserved for future use.

• From the above class range can be identified from which class the IP address is belongs.

• A CIDR IP address can be look like a normal IP address that ends with followed by a number which are as follows:

• 178.204.4.6/32.

• In this the last 32 tells that prefix IP network.

• The prefix IP network specify that how many addresses are covered by the CIDR.

Step 2/7

CIDR Blocks:

• CIDR blocks can be used to group the blocks addresses into a single routing network address.

• CIDR prefix IP network is used for interpreting the IP addresses.

• CIDR blocks distribute the first blocks of bit sequences which consist of binary representation of IP address and blocks can be identified through the decimal dot notation that can be used for IPV4 address.

• In CIDR blocks, an address which has the unique prefixes and the same number of bits always related to the same blocks.

• CIDR blocks assignment can be managed by the IANA (Internet Assigned Number Authority).

• The main purpose of the IANA is to provide the large block of IP addresses to the RIRs (Regional Internet Registries).

• So, the large blocks can be used for geographical area which is as follows:

• North America, Australia, Africa and Europe etc.

• The main purpose of each RIRs is to assign smaller blocks, but it is still used to create larger blocks of IP addresses to the LIRs (Local Internet Registries).

• Depending upon the organization of regional and Local Internet Registries blocks can be divided further.

• CIDR can also be used for newer IPv6 standard.

Step 3/7

CIDR notation cannot be used for the blocks because of following reasons:

• In order to find the CIDR notation for a range of addresses while the first and last block addresses are given.

• There is need to find the prefix length which can be denoted as n (value of n).

• In order to find the maximum number of same right most bits in Left address and right address.

• Suppose that the first block is prefix. In the first address, right most bits (suffix) should be all 0's and in the last address, right most bits (suffix) should be all 1's.

• Suppose above test matches in first and last addresses then find the value of n (prefix length) and the block can be used for CIDR notation.

• The above test guarantees that the first address can be divided into present block number of addresses.

Step 4/7

• The AD-HOC block that has the range: 224.0.2.0 to 224.0.255.255.

• From the above discussion, first address which is in decimal is 224.0.2.0 that can be represented in binary such as:

224.0.2.0: 1 1 1 0 0 0 0 0.0 0 0 0 0 0 0 0.0 0 0 0 0 0 1 0.0 0 0 0 0 0 0 0

• Last Address which is in decimal is 224.0.255.255 that can be represented in binary such as:

224.0.255.255: 1 1 1 0 0 0 0 0.0 0 0 0 0 0 0 0.1 1 1 1 1 1 1 1.1 1 1 1 1 1 1 1

• From the above CIDR notation concept, it is clear that in first address, the suffix should be all 0's and in last address all suffix should be all 1's.

• But in the first address the rightmost block (suffix) has 1's in the second block from the right which can be seen in the above first address which is represented in the binary. So, this block does not match with the condition which has been discussed above for the CIDR.

• And this block can be divided into many blocks for the future purpose.

Step 5/7

• The first reserved block which has the range 224.3.0.0 to 231.255.255.255

• From the above discussion it has the first and last address which is as follows:

• First Address which is in decimal is 224.3.0.0 that can be represented in binary which is as follow:

224.3.0.0: 1 1 1 0 0 0 0 0.0 0 0 0 0 1 1 1.0 0 0 0 0 0 0 0.0 0 0 0 0 0 0 0

• Last Address which is in decimal is 231.255.255.255 that can be represented in binary which is as follow:

231.255.255.255: 1 1 1 0 0 1 1 1.1 1 1 1 1 1 1 1.1 1 1 1 1 1 1 1.1 1 1 1 1 1 1 1

•

Step 6/7

From the above CIDR notation concept, it is clear that in first address the suffix should be all 0's and in last address all suffix should be all 1's.

• But in the first address the rightmost block (suffix) has two 1's in the third block from the right which can be seen in the above first address which is represented in the binary. So, this block does not match with the condition which has been discussed above for the CIDR.

• And this block can be divided into many blocks in the future purpose.

Step 7/7

• The second reserved block which has the range 234.0.0.0 to 238.255.255.255

• From the above discussion it has the first and last address which is as follows:

• First Address which is in decimal is 234.0.0.0 that can be represented in binary which is as follow:

234.0.0.0: 1 1 1 0 1 0 1 0.0 0 0 0 0 0 0 0 .0 0 0 0 0 0 0 0.0 0 0 0 0 0 0 0

• Last Address which is in decimal is 238.255.255.255 that can be represented in binary which is as follow:

238.255.255.255: 1 1 1 0 1 1 1 0.1 1 1 1 1 1 1.1 1 1 1 1 1 1 1.1 1 1 1 1 1 1 1

• From the above CIDR notation concept, it is clear that in first address the suffix should be all 0's and in last address all suffix should be all 1's.

• But in the first address the rightmost block (suffix) has one 1 in the fourth block from the right which can be seen in the above first address which is represented in the binary and in the Last address the fourth block from the right which has one 0. So, this block does not match with the condition which has been discussed above for the CIDR.

• And this block can be divided into many blocks in the future purpose.

2. **The AS number in an organization is 24101. Find the range of multicast addresses that the organization can use in the GLOP block.**

Step 1/4

AS Number:

- This stands for Autonomous System Number.
- Autonomous system is sometimes introduced to the routing domain.
- In this type of system, networks can communicate routing information in the group via the IGP (Interior Gateway Protocol).
- This distributes the routing information to the other autonomous system with the help of BGP (Border Gateway Protocol).
- EGP (Exterior Gateway Protocol) was used previously. BGP can be used for future.
- This sets the globally unique number referred to as an autonomous system number.
- With the help of an autonomous system, a single network or group of networks can be controlled by the network administrator or a group of administrators.
- An AS number is available globally and can be used to identify the autonomous system.
- In autonomous system number has the limited number.
- Every AS can be assigned the 16-bit number.

Step 2/4

Multicast Address:

- Multicast address is a type of logical identifier which is related to datagram or frames that process the datagram or frames for a specific network service.
- Multicast addressing is handled in the OSI layer 2 which name is:
- DataLink Layer
- Multicast address has some range which is as follows:
- 224.0.0.0.0 to 239.255.255.255
- In this the starting range 224.0.0.0.0 is used to reserve base address.
- The second range 224.0.0.1 is used to multicast the computer groups.
- The third range 224.0.0.2 is used to subnet all router.
- If the datagrams with multicast address then the all datagrams simultaneously transmitted to every computer of multicast address.

Step 3/4

GLOP Block:

- The block has the address 233.0.0.0/8 is called the GLOP block.
- This block can be used for an autonomous system.
- Every AS can be assigned the 16-bit number.
- In order to insert the autonomous system number, then in the middle of GLOP block two octets can be filled to create the multicast address.
- This has the range 233.x.y.0 to 233.x.y.255 to create the 256 multicast addresses.
- In this x.y is the AS number.

Step 4/4

In the organization an AS number is 24101 in order to the find the multicast address. The calculation can be done in the following way:

- The AS number is 24101 and there are the 256 base addresses.
- First divide the 24101 by 256 in order to find the value of x and y, where x is quotient and y is remainder.
- If dividing the 24101 to 256 gets the 94 as quotient and 37 as remainder.
- Then fill the value of x as 94 and y as 37.
- Then address will be for GLOP block is 233.94.37.0

Hence, the range of multicast address is 233.94.37.0 to 233.94.37.255.

3. A multicast address for a group is 232.24.60.9. What is its 48-bit Ethernet address for a LAN using TCP/IP?

Step 1/3

Multicast Address:

• Multicast address is a type of logical identifier which is related to datagram or frames that process the datagram or frames for a specific network service.

• Multicast addressing is handled in the OSI layer 2 that's name is Datalink Layer.

• Multicast address has some range which is as follows:

• 224.0.0.0.0 to 239.255.255.255

• In this the starting range 224.0.0.0.0 is used to reserve base address.

• The second range 224.0.0.1 is used to multicast the computer groups.

• The third range 224.0.0.2 is used to subnet all router.

• If the datagrams with multicast address then the all datagrams simultaneously transmitted to every computer of multicast address.

Step 2/3

Ethernet Address:

• Ethernet address is also known as wireless hardware address.

• Ethernet address contains a number and this number is assigned by a manufacturer of that Ethernet.

• The assigned number will be in 6-byte hexadecimal number.

• For example, the number is 092007B10A6DE.

• The above hex digit number can be 0 to 9 and can be any letter from A to F in uppercase or lower case.

• In some places used prefix 0x to tell that the number is in hexadecimal and do not interpret the 0x value for the number.

• The above 6 byte hexadecimal, each 2 byte can be written as two hexadecimal which is as follows:

• 09:20:07:B10:A6:DE

Step 3/3

Suppose a group has 232.24.60.9 as multicast address then 48-bit Ethernet address for a LAN using TCP/IP can be calculated by the following way:

• First convert the multicast address into binary form as follows:

• The binary number will be: 11101000.00011000.00111100.00001001

• In the multicast address, there are 6 octets in which 3 octets are reserved.

• From the reserved octets, the prefix 3 octet is 01:00:5E that means 24 bits are reserved for layer 2 and this octet starts from octet0, octet1, ..., octet5 and 1 bit is also reserved in octet4. Only 23 bits can multicast for layer 2.

• Thus, the 3 octet has the prefix value is 01:00:5E and the remaining can be calculated as:

• The prefix value is 01:00:5E where E represents the 14 in decimal which is as follows: 5E has the 94 in decimal $\left(\left(5\times16^1+14\times16^0\right)=80+14=94\right)$.

Binary digits for 01: 00000001

Binary digits for 00: 00000000

Binary digits for 94: 01011110

• To perform operation for 48-bit Ethernet address, 232 is the first octet of the given IP address and this will match with prefix ethernet address 94 which is in third octets.

• The resultant value will not change and has the same value for third octets and remaining value 24.60.9 will be:

Binary form of (232.24.60.9): 11101000.00011000.00111100.00001001

Binary form of (01:00:94): 00000001.00000000.01011110

• The resulting address will be 1.0.94.24.60.9 for the three octets.

• 1.0.94 that has been reserved for the three octets and remaining in the from 24.60.9.

• Hence, the resulting value can be in hexadecimal 01:00:5E:24:3C:09.

4. Change the following IP multicast addresses to Ethernet multicast addresses. How many of them specify the same Ethernet address?

a. 224.18.72.8

b. 235.18.72.8

c. 237.18.6.88

d. 224.88.12.8

Step 7/11

a.

• In this IP multicast address: **224.18.72.8**, firstly find the right most 3 digits and substract the 8 from the left most digits and suppose if it is greater than 8, then add the result the starting of the ethernet address.

• The above IP address can be represented in the following ways:

11100000.00010010.01001000.00001000

• The above binary can be represented in hexadecimal like this:

E0.12.48.08

• So, from the above IP multicast address, the changed (in hexadecimal) address is as follows:

IP address:				E0:	12:	48 :	08
Subtract 8					12:	48 :	08
Result	01:	00:	5E		12:	48 :	08

• After that the last result is 01:00:5E: 12:48:08

Step 8/11

b.

• In this IP multicast address: **235.18.72.8**, firstly find the right most 3 digits and substract the 8 from the left most digits and suppose if it is greater than 8, then add the result the starting of the ethernet address.

• The above IP address can be represented in the following ways:

11101011.00010010.01001000.00001000

• The above binary can be represented in hexadecimal like this:

EB.12.48.08

• So, from the above IP multicast address, the changed (in hexadecimal) address is as follows:

IPAddress:	EB:12:48:08
Subtract 8:	12:48:08
Result:	01:00:5E:12:48:08

• After that the last result is 01:00:5E: 12:48:08

Step 9/11

c.

• In this IP multicast address: **237.18.6.88**, firstly find the right most 3 digits and substract the 8 from the left most digits and suppose if it is greater than 8, then add the result the starting of the ethernet address.

• The above IP address can be represented in the following ways:

11101101.00010010.00000110.01011000

• The above binary can be represented in hexadecimal like this:

ED.12.48.08

• So, from the above IP multicast address, the changed (in hexadecimal) address is as follows:

IP address:			ED: 12: 06: 58
Subtract 8:			12 :06: 58
Result:	01:	00:	5E: 12: 06 :08

• After that the result is 01:00:5E: 12:06:08

Step 10/11

d.

• In this IP multicast address: **224.88.12.8**, firstly find the right most 3 digits and substract the 8 from the left most digits and suppose if it is greater than 8, then add the result the starting of the ethernet address.

• The above IP address can be represented in the following ways:

11100000. 01011000.00001100.00001000

• The above binary can be represented in hexadecimal like this:

E0.58.0C.08

• So, from the above IP multicast address, the changed (in hexadecimal) address is as follows:

IP address:	94: 58: 0C: 08
Subtract 8	58:0C:08
Result	01:00: 5E: 58:0C:08

• After that result is 01:00:5E: 58:0C:08.

Step 11/11

From the above, it is clear that two ethernet multicast address is same which address is as follows:

• **224.18.72.8:** For this IP multicast address, the ethernet address is 01:00:5E: 12:48:08 for option (a).

• **235.18.72.8:** For this IP multicast address the ethernet address is 01:00:5E: 12:48:08 for option (b)

• Hence, the above two option (a) and (b) represents the same ethernet address.

5. Why is there no need for the IGMP message to travel outside its own network?

Step 1/2

IGMP:

• This stands for Internet Group Management Protocol.

• Protocol is a set of rules and regulations that determine how communication can be happen between the computers.

• IGMP is discussed in RFC 1112 for the IP multicast addressing in the internet.

• This is an Internet Protocol that gives the route to its multicast (Multicast is a type of communication where can be one sender and multiple receiver) group membership to its adjacent routers.

• Multicasting defines that in network one computer can send content to the multiple computer that can be identified by the receiver computer from where this content is coming.

• IGMP is discussed on network layer.

• IGMP can be used to exchange the information on the basis of status of membership in the multicast addressing to the router on the network.

• For Example, suppose a router is aware from the host that is privately attached to the network for a specific multicast group address then the router sends this information to the other router on the internetwork in order that multicast information can be send to the suitable routers.

• In IGMP, the host always inform to its local router.

• In order to join the multicast group, a host must report to its local router on the network for a membership.

• These routers intermittently survey the host in their privately connected network for checking its membership status.

• Suppose a host wants to join multicast group, then it sends the IGMP message means a host membership report that has the address 244.0.0.1 .This address contains the multicast address that recognize the group for which the host wants to join.

Step 2/2

There is no need for IGMP in order to travel outside of its own network because:

• The main purpose of IGMP is only to tell the other routers in the spanning tree (it has the minimum edges suppose there are n vertices then there must be n-1 edges) of membership group.

• The purpose of IGMP message to survey the network for membership for any groups.

6. Answer the following questions:

a. What is the size of a general query message in IGMPv3?

b. What is the size of a group-specific message in IGMPv3?

c. What is the size of a group-and-source-specific message in IGMPv3 if it contains 10 source addresses?

Step 3/7

1. Membership query message format:

|<--------8-bit-------->|<--------8-bit------->|<---------------16-bit------------------>|

Type:0x11			Response Code	Checksum
Group Address				
Resv	S	QRV	QQIC	Number of Sources (N)
Source Address (1)				
Source Address (2)				

Source Address (N)				

Step 4/7

- **Type.** It defines message type and its field consists 8-bit.
- **Response Code.** It defines response time of the recipient and its field consists 8-bit.
- **Checksum.** It is calculated according to complete IGMP message.
- **Group Address.** Its field size is 32-bit. For general query message this field set to 0 and for group specific or group-and source specific, it is set to IP multicast.
- **Resv**. it consists 4-bit of fields and reserved for the future use.
- **S**. it is a suppress flag of 1-bit field.
- **QRV.** Its field is 3-bit and it is also called querier's robustness variable.
- **QQIC.** Its field is 8-bit and it is also called querier's query interval code.
- **Number of sources(N).** this field size is 16-bit and it defines the unicast source address of 32-bit.
- This value is set to zero for the group-specific query and general query.
- It sets non-zero for the group-and-source-specific query.

Step 5/7

a.

In IGMPv3, the size of the general query message is 12 bytes long.

Step 6/7

b.

In IGMPv3, the size of the group specific message is 16 bytes long.

Step 7/7

c.

The size of group-source-specific message, if IGMPv3 contains 10 addresses can be calculated as follows:

- In the IGMPv3, there are 3 records and each record have the 10 addresses, for IGMPv3 there is a membership query table.
- The size of report message can be calculated like this:
- There are 3 records while each record has 10 addresses then the report size will be:

$$\begin{aligned}10+3\times(10+5\times4) &= 10+3\times(10+20)\\ &= 10+3\times30\\ &= 10+90\\ &= 100 \text{ bytes}\end{aligned}$$

The size is 100 bytes of the group-source-specific message if there are 10 source addresses.

7. What is the size of a report message in IGMPv3 if it contains 3 records and each record contain 5 source addresses (ignore auxiliary data)?

Step 1/2

IGMPv3:

• This is the third version of IGMP.

• IGMPv3 is discussed in the RFC 3376 after that IGMPv3 has been modified and discussed in RFC 4604.

• IGMPv3 is used for source filtering.

• Source filtering empowers the multicast receiver host for giving the signal to a router from which groups it wants to traffic and also empowers for which source this traffic is expected.

• IGMPv3 supports two mode which is as follows:

• **INCLUDE Mode:** In this, receiver declares the enrollment to a host group and gives the collection of IP addresses from which it needs to traffic.

• **EXCLUDE Mode:** In this, receiver declares the participation to a host group and gives the collection of IP addresses from which it does not want to traffic.

Step 2/2

Consider the details provided in the textbook.

The size of a report message in IGMPv3 will be:

$$\begin{aligned} 8+3\times(8+5\times4) &= 8+3\times(8+20) \\ &= 8+3\times(28) \\ &= 8+84 \\ &= 92 \end{aligned}$$

Hence, the size of a report message in IGMPv3 is $\boxed{\text{92 bytes}}$.

8. Show the socket state table (similar to Figure 12.11) for a host with two sockets: S1 and S2. S1 is the member of group 232.14.20.54 and S2 is the member of the group 232.17.2.8. S1 likes to receive multicast messages only from 17.8.5.2; S2 likes to receive multicast messages from all sources except 130.2.4.6.

Step 2/3

As per given details there is two socket S1 and S2 for a host. S1 has the member group address 232.14.20.54 and can receive the multicast messages from the 17.8.5.2 and S2 has the member group address 232.17.2.8 and can receive the multicast message from the all source excepting the 130.2.4.6

- In the below diagram, firstly header and group record message has been discussed according to given details.
- The field 0x22 can be used for group record while another field like Reserved that takes 8-bit field.
- And the next field tell about the checksum that takes 16-bit fields.
- In this diagram the record type 6 is using in order to exclude mode that means any messages from the only source declares the source address that has been discussed in Exercise 9 report.
- As per given details the two socket S1 and S2 and S1 is the member group has the address 232.14.20.54 and Socket S1 wants to receive the message only from the address 17.8.5.2 for multicast messages.
- And in this Socket S2 has the member group address 232.17.2.8 and Socket S2 wants to receive the message from all the sources excepting from the address 130.2.4.6 that has been exhibited in the socket table.

0 8 16 31

0x22	Reserved	Checksum
Reserved		2
1	0	1
232.14.20.54		
17.8.5.2		
6	0	1
232.17.2.8		
130.2.4.6		

Step 3/3

Socket State Table:

Socket	Multicast Group	Filter	Source Address
S1	232.14.20.54	Include	17.8.5.2
S2	232.17.2.8	Exclude	130.2.4.6

9. Show the interface state for the computer in Exercise 8.

Step 2/2

Interface state of the computer which is given in the below table which is as follows:

Multicast Group	Timer	Filter	Source address
232.14.20.54	12:00	Include	17.8.5.2
232.17.2.8	12:05	Exclude	130.2.4.6

10. Show the group record sent by the host in Exercise 9 if socket S1 declares that it likes also to receive messages from the source 24.8.12.6.

Step 2/2

As per given details the below is the group record sent with the help of computer for exercise 9 in this socket S1 defines that it wants to receive the message that has the address 24.18.12.6

- In the below diagram, firstly header and group record message has been discussed according to given details.
- The field 0x22 can be used for group record while another field like Reserved that takes 8-bit field.
- And the next field tell about the checksum that takes 16-bit fields.
- In this diagram the record type 6 is using in order to exclude mode that means any messages from the only source declares the source address that has been discussed in Exercise 9 report.
- As per given details the two socket S1 and S2 and S2 is the member group has the address 232.17.2.8 and Socket S2 wants to receive the message only from the address 130.2.4.6 for multicast messages.
- And this Socket S1 wants to receive the messages from the source that has the address 24.8.12.6 and Socket S1 has the member group address is 232.14.20.54.

0	8	16 31
0x22	Reserved	Checksum
Reserved		2
1	0	1
232.17.28		
130.2.4.6		
6	0	1
232.14.20.54		
24.8.12.6		

11. Show the group record sent by the host in Exercise 9 if socket S2 declares that it wants to leave the group 232.17.2.8.

Step 2/2

As per given details the below is the group record sent with the help of computer for exercise 9 in this socket S2 defines that it wants to left out the group that has the address 232.17.2.8

- In the below diagram, firstly header and group record message has been discussed according to given details.
- The field 0x22 can be used for group record while another field like Reserved that takes 8-bit field.
- And the next field tell about the checksum that takes 16-bit fields.
- In this diagram the record type 6 is using in order to exclude mode that means any messages from the only source declares the source address that has been discussed in Exercise 9 report.
- As per given details the two socket S1 and S2 and S1 is the member group has the address 232.14.20.54 and Socket S1 wants to receive the message only from the address 17.8.5.2 for multicast messages.
- And this Socket S2 wants to left out the group that has the address 232.17.2.8 and Socket S2 wants to receive the message only from the address 130.2.4.6 for multicast messages.

0	8	16 31
0x22	Reserved	Checksum
Reserved		2
1	0	1
232.14.20.54		
17.8.5.2		
6	0	1
232.17.28		
130.2.4.6		

12. Show the group record sent by the host in Exercise 9 if socket S1 declares that it wants to join the group 232.33.33.7 and accept any message from any source.

Step 2/2

As per provided details the below is the group record sent with the help of computer for exercise 9 in this socket S1 defines that it wants to join the group that has the address 232.33.33.7

• In the below diagram, firstly header and group record message has been discussed according to given details.

• The field 0x22 can be used for group record while another field like Reserved that takes 8-bit field.

• And the next field tell about the checksum that takes 16-bit fields.

• In this diagram the record type 6 is using in order to exclude mode that means any messages from the only source declares the source address that has been discussed in Exercise 9 report.

• As per given details the two socket S1 and S2 and S2 is the member group has the address 232.17.2.8 and Socket S1 wants to receive the message from the all source excepting the address 130.2.4.6 multicast messages.

• And this Socket S1 wants to join the group that has the address 232.33.33.7 and Socket S1 wants to receive the message from the address 17.8.5.2 for multicast messages.

0	8	16	31
0x22	Reserved	Checksum	
Reserved		2	
1	0	1	
232.17.2.8			
130.2.4.6			
6	0	1	
232.33.20.33.7			
17.8.5.2			

13. In Figure 12.14, show the state for interface m1 if the router receives a report with the record telling a host wants to join the group 232.77.67.60 and accept the messages from any source.

Step 3/3

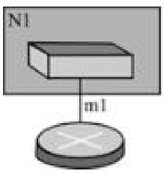
As per given details there is interface m1 if the router gets the report with the joining of group with the IP 232.77.67.60 and admitted the messages from any sources.

• In the diagram, there is the interface which name is m1 within network with router.

• This diagram has the interface m1 that has the multicast group address which has the value 232.77.67.60.

• This has the group time that is discussed above.

• The below diagram has the Filter as well as Source address that is also discussed above.



State for interface m1

Multicast group	Timer	Filter	Source addresses
232.77.67.60		Include	

14. Show the value of MRT in second if the Max Response Code is:

a. 125

b. 220

MRT:

• This stands for Maximum Response Time.

• The MRT is the highest time that can be declared before forwarding a report in response to a query.

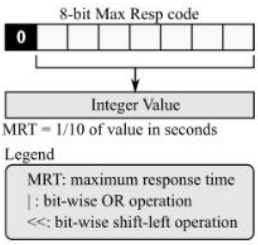
• The MRT can be performed by the 8 -bit MRC (Maximum Response Code) field in the query.

• Below is the diagram, with the help of MRC calculation can be performed which is as follows:

• In order to calculate MRT follow the following conditions which is as follows:

• Suppose there is the MRC value is less than 128 that means the left most bit value will be 0.

• Then take 7 bits value in decimal and multiply with 1/10 to get MRT.

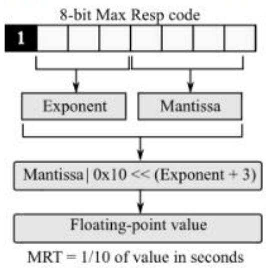


Step 2/5

• In order to calculate MRT follow the following conditions which is as follows:

• Suppose there is the MRC value is greater than 128 that means the left most bit value will be 1.

• Then take 3 bits as Exponents and 5 bits as Mantissa value calculated in floating value then multiply with 1/10 that is exhibited in the diagram.



Step 3/5

As per given details the MRC has the value 125 and 220 then this can be calculated by the following ways which is as follows:

• The MRC value is 125.

• Firstly, convert this 125 into the binary value.

$\textbf{Binary Value of } 125 = (01111001)_2$.

• From the left side the left most bit is 0 that means 125 is less than 128 already.

• Take the 7 bits from the left to right and convert it into decimal.

• After taking 7 bits and converting the value will be as it is 125.

• Then MRT value will be in seconds by the following way:

$$\begin{aligned} 125 \times 1 \div 10 &= 125 \div 10 \\ &= 1.25 \text{second} \end{aligned}$$

Hence, the MRT value is $\boxed{1.25\text{seconds}}$.

Step 4/5

b.

• The MRC value is 220.

• Firstly, convert this 220 into the binary value.

$\textbf{Binary Value of 220} = (11011100)_2$.

• The value of MRC is greater than 128 that means the left most bit is 1.

• Ignore the first bit and see the second diagram, then take 3 bits from left for exponent and another remaining 4-bit as for Mantissa.

• That means the exponent value is 101 has the value 5 in decimal and mantissa value is 1100 has the 12 in decimal.

• Then MRT value will be in seconds by the following way:

$$(\textbf{Mantissa} | \textbf{0x10} << (\textbf{exponent} + 3))$$

• So, the calculated value of Mantissa is 12 and exponent is 5.

• And 0x10 is in hexadecimal and has the decimal value with 10.

• Putting the value of all variable in the formula which is as follows:

• Then MRT value will be in seconds by the following ways and performing the bitwise OR operation and bitwise left shift that can be performed with multiply by 2 with power of given exponent:

$$(\textbf{Mantissa} | \textbf{0x10} << (\textbf{exponent} + 3))$$

$$\begin{aligned}&(12|10 << (5+3)) = (14 << 8)\\&= (14 \times 2^8) = 3584\\&= (3584 \times 1/10) = 358.4\,\textbf{seconds}\end{aligned}$$

Step 5/5

Hence, the MRT value is $\boxed{358.4\,\textbf{seconds}}$.

15. The contents of an IGMP message in hexadecimal notation are:

11 03 EE FF E8 0E 15 08

Answer the following questions:

a. What is the type?

b. What is the checksum?

c. What is the groupid?

Step 6/9

The IGMP message which has the hexadecimal representation which is as follows:

11 03 EE FF E8 0E 15 08

• The above message type is query message because this has the value 11 in the starting which is given in above IGMP message and that has been discussed above in the Type that 0x11 is used for query message.

Step 7/9

• For the above hexadecimal notation 11 03 EE FF E8 0E 15 08 the checksum will be as follows:

• The checksum for 11 03 EE FF E8 0E 15 08 will be from the left the octets 3 and octets 4 which is in hexadecimal 0x EE FF.

• The 0x EE FF can be represented in this way $(14141515)_{16}$ because the E has value 14 and F has value 15 in the decimal.

• The above value will in decimal:

Step 8/9

$$\begin{aligned}\left(14\times16^1+14\times16^0\ \ 15\times16^1+15\times16^0\right)&=(224+14\ \ 240+15)\\&=(238\ \ 255)\end{aligned}$$

• The above value is in decimal which can be represented as $(238\,255)_{10}$.

• The above can be represented in binary which is as follows:

$(1110\ 1110\ 1111\ 1111)_2$

• The checksum is (1110 1110 1111 1111)2.

Step 9/9

• For the above hexadecimal notation 11 03 EE FF E8 0E 15 08 the group addresses are as follows:

• In the given address 11 03 EE FF E8 0E 15 08, from the right, 8 bytes which is each has 2-byte address.

• The group address is $(E80E1508)_{16}$ and this can be separated in order to get the group address $(E8.0E.15.08)_{16}$ which can be converted in decimal as follows:

• E has the value 14 in decimal, $(148.014.15.08)_{16}$.

• This can be calculated in decimal:

$$\begin{aligned}\begin{pmatrix}14\times16^1+8\times16^0 & 0\times16^1+14\times16^0\\ 1\times16^1+5\times16^0 & 0\times16^1+8\times16^0\end{pmatrix}&=(224+8\ \ 0+14\ \ 16+5\ \ 0+8)\\&=(232\ \ 14\ \ 21\ \ 8)\end{aligned}$$

• The calculated value can be represented in decimal like this $(232.14.21.8)_{10}$.

• The group id will be 232.14.21.8.

16. The contents of an IGMP message in hexadecimal notation are:

22 00 F9 C0 00 00 00 02

Answer the following questions:

a. What is the type?

b. What is the checksum?

c. What is the number of records?

The IGMP message which has the hexadecimal representation which is as follows:

22 00 F9 C0 00 00 00 02

a.

• The above message type is used for Membership report. Because this has the value 22 in the starting which is given in the above IGMP message and that has been discussed above in the Type that 0x22 (22) is used for Membership report.

Step 8/10

b.

For the above hexadecimal notation **22 00 F9 C0 00 00 00 02** the checksum will be as follows:

•

Step 9/10

The checksum for **22 00 F9 C0 00 00 00 02** will be from the left the octets 3 and octets 4 which is in hexadecimal 0xF9 C0.

• The 0x EE FF can be represented in this way $(15\ \ 9\ \ 12\ \ 0)_{16}$.

• The above value will in decimal:

$$\begin{aligned}\left(15\times16^1+9\times16^0\ \ 12\times16^1+0*16^0\right)&=\left(240+9\ \ 192+0\right)\\&=\left(249\ \ 192\right)\end{aligned}$$

• The calculated value can be represented in the decimal like this $(249\ \ 192)_{10}$.

• The above can be represented in binary which is as follows:

$(1111\ \ 11001\ \ 1100\ \ 0000)_2$

• And the checksum is $(1111\ \ 11001\ \ 1100\ \ 0000)_2$.

Step 10/10

c.

• For the above hexadecimal notation **22 00 F9 C0 00 00 00 02** the group addresses is as follows.

• In the given address **22 00 F9 C0 00 00 00 02**, from the right, 8 bytes which is each has 2 byte address.

• The group address is $(00000002)_{16}$ and this can be separated in order to get the group address $(00.00.00.02)_{16}$ which can be converted in decimal like this which is as follows:

• $(00.00.00.02)_{16}$

• This can be calculated in decimal:

$$\begin{aligned}\begin{pmatrix}0\times16^1+0\times16^0\ \ 0\times16^1+0\times16^0\\ 0\times16^1+0\times16^0\ \ 0\times16^1+2\times16^0\end{pmatrix}&=(0+0\ \ 0+0\ \ 0+0\ \ 0+2)\\&=(0\ \ 0\ \ 0\ \ 2)\end{aligned}$$

• The calculated value can be represented in the decimal like this $(0\ \ 0\ \ 0\ \ 2)_{10}$.

• The group id is 0.0.0.2. and in this 0.0.0.2 number of records tells the source address. From the left it has the 0 means it is general and specific group.

18. In Figure 12.18, find the unicast routing tables for routers R2, R3, and R4. Show the shortest path trees.

Step 4/8

Unicast routing table for the router R2 means R2 is a root, and directly connected networks to this root is represented by the dashed (-).

- Network N1 is directly connected to the router R2 (root) so, it is represented by dashed.
- Network N2 is directly connected to the router R2 (root) so, it is represented by dashed.
- Network N3 is directly connected to the router R2 (root) so, it is represented by dashed.
- Router R2 connected to the router R3 and then router R3 connected to the network N4.
- Router R2 connected to the router R1 and then router R1 connected to the network N5.
- Router R2 connected to the router R1, R1 connected to R4 and then router R4 connected to the network N6.

The shortest path tree for the unicast routing of router R2 is as given below:

Step 5/8

	Destination	Next-hop
Shortest path →	N1	—
—	N2	—
—	N3	—
	N4	R3
—	N5	R1
Shortest path →	N6	R1

Shortest path tree

Step 6/8

Unicast routing table for the router R3 means R3 is a root, and directly connected networks to this root is represented by the dashed (-).

- Router R3 connected to the router R2, R2 connected to the network N1.
- Router R3 connected to the router R2, R2 connected to the network N2.
- Network N3 is directly connected to the router R3 (root) so, it is represented by dashed.
- Network N4 is directly connected to the router R3 (root) so, it is represented by dashed
- Router R3 connected to the router R2, R2 connected to R1 and then router R1 connected to the network N5.
- Router R3 connected to the router R2, R2 connected to R1, R1 is connected to the R4 and then router R4 connected to the network N6.

The shortest path tree for the unicast routing of router R3 is as given below:

Step 7/8

	Destination	Next-hop
Shortest path →	N1	R2
—	N2	R2
—	N3	—
	N4	—
—	N5	R2
Shortest path →	N6	R2

Shortest path tree

Step 8/8

Unicast routing table for the router R4 means R4 is a root, and directly connected networks to this root is represented by the dashed (-).

• Router R4 connected to the router R1 and then router R1 connected to the network N1.

• Router R4 connected to the router R1, R1 connected to R2 and then router R2 connected to the network N2.

• Router R4 connected to the router R1, R1 connected to R2 and then router R2 connected to the network N3.

• Router R4 connected to the router R1, R1 connected to R2, R2 is connected to the R3 and then router R3 connected to the network N4.

• Network N5 is directly connected to the router R4 (root) so, it is represented by dashed.

• Network N6 is directly connected to the router R4 (root) so, it is represented by dashed.

The shortest path tree for the unicast routing of router R4 is as given below:

	Destination	Next-hop
Shortest path →	N1	R1
—	N2	R1
—	N3	R1
—	N4	R1
—	N5	—
Shortest path →	N6	—

Shortest path tree

19. In Figure 12.19, find the multicast routing tables for routers R2, R3, and R4.

Step 4/6

In order to find the multicast routing tables, there is the following routing table for routers R2, R3, R4 which is as follows:

• The first routing table for routers R2 from the figure 12.19 in the book. In this there are group like G1, G2,...... etc.

Destination	Next-Hop
G1	R1, R3
G2	R3
G3	R1
G4	R1, R3
G5	R1

Step 5/6

• The second routing table for routers R3 from the figure 12.19 in the book. In this there are group like G1, G2,...... etc.

Destination	Next-Hop
G1	R2
G2	R2
G3	R2
G4	R2
G5	R2

Step 6/6

• The third routing tables for routers R4 from the figure 12.19 in the book. In this there are group like G1, G2,...... etc.

Destination	Next-Hop
G1	R1
G2	R1
G3	R1
G4	R1
G5	R1

20. A router using DVMRP receives a packet with source address 10.14.17.2 from interface 2. If the router forwards the packet, what are the contents of the entry related to this address in the unicast routing table?

Step 7/9

As per given details router is using the DVMRP (Distance Vector Multicast Routing Protocol) gets the packet with the starting address 10.14.17.2 from interface 2.the contents of this address have the following information in the unicast routing table which is as follows:

• This uses the DVMRP (Distance Vector Multicast Routing Protocol).

DVMRP:

• This stands for Distance Multicast Routing Protocol.

• DVMRP is a type of interior gateway protocol.

• DVMRP is developed of Multicast routing protocol.

• DVMRP is based on source routing protocol

• DVMRP can only rotes the multicast packets.

•

Step 8/9

For router there is additional information is required for the non-multicast routing protocol while DVMRP can be extended for the non-multicast routing protocol (Unicast Routing).

• The below diagram can be used for MBONE (Multicast Backbone).

• The MBONE use the backbone with the help of mesh topology that is utilized by the server in order to redistribute the multicast address in the star topology.

• The below is the format of MBONE on the basis of internet.

8 bits	8 bits		16 bits
Type(0X 13)	Code(0X 1)		Checksum
Reserved	Capabilities	minor version	Major version
Generation ID			
Neighbour IP1			
....			
Neighbours IP N			

Step 9/9

Diagram:

• The below diagram can be used for MBONE as well as unicast routing table.

• In this table, the DVMRP (Distance Vector Multicast Routing Protocol) informs the packet in order to find neighbors to path for the sender.

• DVMRP utilizes the hop count with the help of Metric.

• This diagram has the list of networks and metrices.

8 bits	8 bits		16 bits
Type(0X 13)	Code(0X 1)		Checksum
Reserved	Capabilities	minor version	Major version
Mask 1 (Oct 2)	Mask 1 (Oct 3)	Mask 1 (Oct 4)	Src Net 11
Src Net 11	Metric 11		Src Net 12
Src Net 12	Metric 12		--------
	---------------		Mask 2 (Oct 2)
Mask 2 (Oct 3) | Mask 2 (Oct 4)	Src Net 21		
Src Net 21	Metric 21	----------------	

21. Router A sends a unicast RIP update packet to router B that says 134.23.0.0/16 is 7 hops away. Network B sends an update packet to router A that says 13.23.0.0/16 is 4 hops away. If these two routers are connected to the same network, which one is the designated parent router?

Step 4/4

In this router A sends the RIP packet to router B that has the address 134.23.0.0/16 and network B sends then updated packet to the router A which has the address 13.23.0.0/16.

• These above two addresses 134.23.0.0/16 and 13.23.0.0/16 belongs to same network.

• And in this network router B sends an updated packet to the router A.

• So, the router B should be designated to the parent router.

22. Does RPF actually create a shortest path tree? Explain.

Step 3/3

RPF:

• This stands for Reverse Path Forwarding.

• RPF is the modified concept of flooding.

• RPF is the family of RPB, TRPB and RPM algorithm.

• In the RPF, in order to prevent the loops only one copy is sended and other copy will be discard.

• In RPF, router sends only that packet that has been traveled through the shortest path tree from the source to the router.

• In order to find this packet, RPF uses the concept of unicast routing table.

• Suppose that a unicast packet enters into the router interface firstly router will receive the packet and extract the unicast address.

• In order to send the packet to its source address, it determines from the unicast routing table.

• With the help of routing table, can be identify the next hop in the network.

• Suppose that a multicast packet enters into router interface that means that packet has traveled the shortest path from the router to the source address in network because shortest path is uses the concept of reciprocal in UDVR(Unicast Distance Vector Routing) protocol.

• Reciprocal means from A to B can be like B to A. Suppose that a path is shortest path from A to B then the path must be shortest path from B to A.

• If the packet has traveled from router to its source from the shortest path router sends that packet otherwise it will discard that packet.

• RPF avoids the loop because the in the RPF, always only one shortest path from its router to the source.

• Suppose that a packet left out the router and come back again with the help of another interface or identify router that means the packet has not traveled the shortest path.

Hence, RPF creates always only one shortest path from the router to its source.

23. Does RPB actually create a shortest path tree? Explain. What are the leaves of the tree?

Step 1/2

Shortest Path Tree:

• Suppose that there is connected, undirected graph S, then a shortest path tree will be rooted at vertex v will be spanning tree of S then the vertex v to any other vertex v1 in the spanning tree will be shortest path.

• Spanning tree has n vertices and n-1 edges in the shortest path.

• There are many shortest path algorithms by which shortest path tree can be construct which name is as follows:

• Dijkstra's algorithm

• Bellman-Ford algorithm.

Step 2/2

RPB:

• This stands for Reverse Path Broadcasting.

• This has the many types of algorithm which belongs to the same family of algorithm which name is follows:

• **TRBP:** This stands for Truncated Reverse Path Broadcasting's can be used to overcome the limitation of RBP.

• **RPM:** This stands for Reverse Path Multicasting. This is the extension of RPB and TRBP.

• In order to avoid the routing loops in multicasting group, RPB algorithm can be used.

• The RPB algorithm makes the shortest spanning tree and packets can be forwarded optimally.

• RPB can be used for shortest path between sender and every receiver for multicast packets to deliver and it guarantees that multicast packets will be deliver as fast as possible.

• In the RPB, multicast packet reaches at every network and that network will receive the single copy of that packets. So, it creates the spanning tree.

Hence, RPB creates the shortest path tree and the network Is the only leaves of the tree.

24. Does RPM actually create a shortest path tree? Explain. What are the leaves of the tree?

Step 2/3

RPM:

• This stands for Reverse Path Multicasting.

• This is the extended implementation of RPB (Reverse Path Broadcasting) and TRBP (Truncated Reverse Path Broadcasting).

• In RPB (Reverse Path Broadcasting), it broadcast the packets not multicast the packets.

• The RPB was not efficient for broadcasting.

• In order to increase the efficiency, the multicast packet must be arriving at those networks who are the active member of particular group. This process is called the Reverse Path Multicasting

• This allows the source-based shortest path tree to be pruned in order that packets can be forwarded for only those branches which is the active members of the particular group.

• In order to convert the broadcast to multicast, protocol uses two methods in the RPM which is follows:

• **Pruning:** In the pruning, the router sends the prune messages to the it's above router in order that it can prune the equivalent interface.

So, the above router can stop forwarding the multicast messages for the particular group with the help of that interface.

• **Grafting:** Suppose that there is a last router in the network which is a leaf router has forwarded the prune message but instantly noticed with the help of IGMP that one of its networks once more is interested for receiving the multicast packets. In order to do above process the graft message is requires.

• Grafting can be used to forces the upstream router for resuming the send multicast messages.

Step 3/3

From the above it is clear that RPM does not create shortest path directly which adds the shortest path tree by the following ways which is as follows:

• The RPM creates the shortest path tree with the help of Pruning and Grafting process in the RPB which has been discussed above.

Hence, RPM creates the shortest path tree and leaves of the tree are the sub-network.