IGMP Tutorials.

**What is IGMP?**

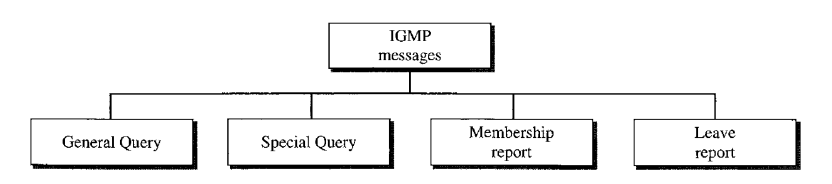
* The IP protocol can be involved in two types of communication :unicasting and multicasting.
* Uni-casting is the communication between one sender and one receiver. It is a one-to-one communication . However, some processes sometimes need to send the same message to a large number of receivers simultaneously. This is called multicasting, which is a one-to-many communication.
* For example, multiple stock brokers can simultaneously be informed of changes in a stock price, or travel agents can be informed of a plane cancellation. Some other applications include distance learning and video-on-demand.

**Group Management?**

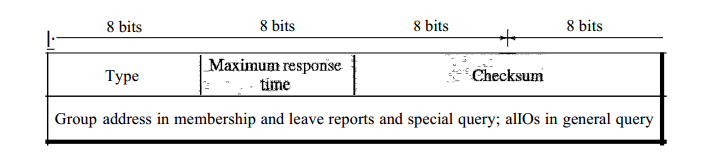
* IGMP is not a multicasting routing protocol; it is a protocol that manages group membership. In any network , there are one or more multicast routers(Let’s say tehr are souces ) that distribute multicast packets to hosts or other routers. The IGMP protocol gives the multi cast routers information about the member ship status of hosts(routers) connected to the network.
* What is the problem ? A multicast router may receive thousands of multi cast packets every day for different groups. If a router has no knowledge about the membership status of the hosts, it must broad cast all these packets.
* Lot of traffic and consumes bandwidth
* Solutions: A better solution is to keep a list of groups in the network for which there is atleast one loyal member
* IGMP is a group management protocol, Which helps a multi cast router create and update a list of loyal members related to each router interface.

IGMP Message:

* 4 Diffenet messages are trsamited to achive this group management.

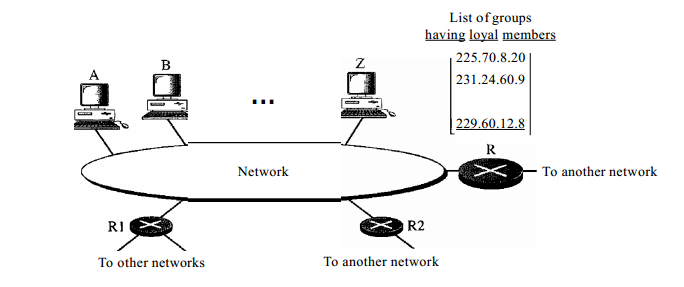


**IGMP Message format:**



* Type – Indiacte What type of meessge it is.
* MRT : is the maximum allowed time, the quesry must be answered/
* Checksum – just a check sum
* Group Address – Define Group ID

**IGMP Operations :**



**Problem Definitions:**

**R is a multi cast router which has a list of all host in the network. It is getting multicust traffic from outside and it suppose to forword the trffic to desire host rather than broadcasting it. How it will do that ?**

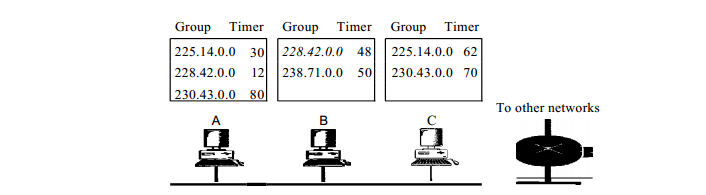
**4 steps, as below:**

1. **Joing a group , When a process(say VLC) want to listen a mustccast packets for goup G , it notify the host, then host send a member ship report message. It sent it twice with assumption that if first one lost , second one will take care. After gtting this message an entry got created in the R.**
2. **Leaving a Group. If no process in the host want to listen the multicast packets he can send a leave request.**
3. **When R recv this leave request, it will not immediately delete the entry form the Table, as other hose might listen this multicast,, thus it send a special query message asking “Is there are anyone is listing this multicast ?” . In a particular time , no resp (memmbehip request) received than it will delete it.**
4. **Above three kind of message is not enough. What happen if host is down or remove from system without a leave report ? Multicast router has the reposibility to handle and keep updated the multicast table. In perticualt time interval it send the General Query message (GID = 0.0.0.0). Router expect an ans within 100. Hist send a memenrship report if it is interested**

**UseFul Concept :**

1. **Delayed Reponce: In general query message , all memner In that group, must repond , if A and B are belonging to group G, then both of them need to send a memeship report to Router and it’s an overhead , so only one respond is send to privent unnecessary traffic. To achiev that , they don’t send respoce immediactly biut wait for some random time, and wait fro random time to send the response. As report is broadcast hence if A get a report message from B, then A will not send the respoce again**

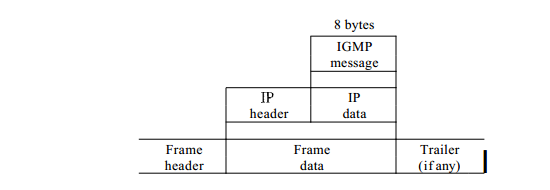
**Question :**



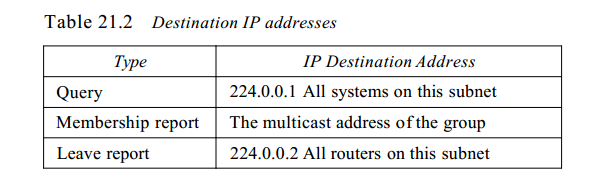
Find out which of the who will send the membership-report when they recv general query from router

1. Query Router: Query messages may create a lot of responses. To prevent unnecessary traffic, IGMP designate sone router as the query router for each network, while other are passive

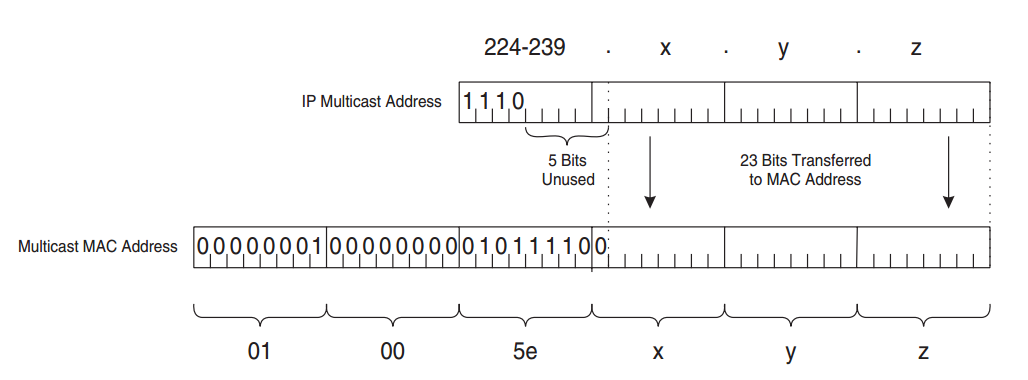
IP datagram for IGMP.

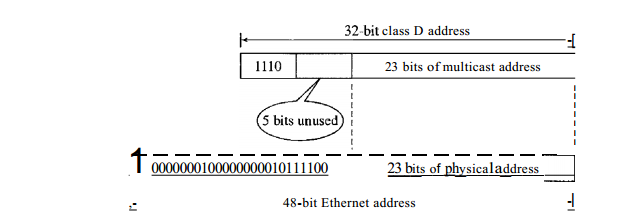


* The IP packet that carries an IGMP packet has a value of 1 in its TTLfield.
* IP multicast or Class D addresses begin with 1110 in the most significant address bits—Addresses within the range 224.0.0.0 to 239.255.255.255.
* Hosts anywhere in the network can register to join a multicast group defined by a specific multicast IP address \_ which basically treaded as group ID
* IP multicast addresses 224.0.0.1 (all hosts on a subnet) and 224.0.0.2 (all routers on a subnet) are well known and don’t require registration



**Pysical multi cast support:**

* Multicast also uses Ethernet or MAC addresses beginning with 01-00-5e. (The least significant bit of the high-order byte is always 1.) The multicast IP addresses must be translated into multicast MAC addresses in this fashion
* Mac Address 48 bit longs
* First 25 bit indicate Pysical multicast address
* Last 23 bit is used to defibe the group.
* How to convert Multicast IP address to Multi cast Mac adreess. ? Multicast router extract the lease 23 bit’s in clss D IP address and insirt them multicast Ethernet frome.
* 



* The 25 most-significant bits in the MAC address are always 01-00-5e.
* The 23 lowest-significant bits are copied from the 23 lowest-significant bits of the IP address.
* Is the address translation is Unique ? The address translation is not unique; 5 bits of the IP address are not used, therefore, 32 different IP addresses can all correspond to a single multicast MAC address.

**IGMP Snooping ?**

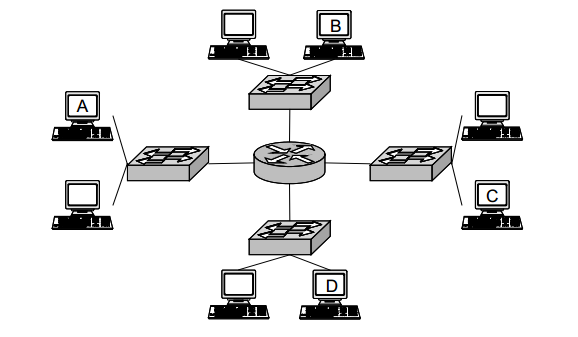
IGMP is a session-layer (Layer 3) protocol used to establish membership in a Multicast group and can register a router to receive specific Multicast traffic. The main aim is to avoid flooding in the network, which basically restricted by Layer3 filtering. But Problem happenes when number of host connected to a router through a layer-2 switch. As a IGMP is a layer 3 protocol, it can not restrict the flooding the traffic in layer-2 lavel, That means, all the host connected to Layer-2 Switch, will get the multicast packet,still it is intened fro only one.

A Layer 2 switch supporting IGMP Snooping can passively snoop on IGMP Query, Report, and Leave (IGMP version 2) packets transferred between IP Multicast routers/switches and IP Multicast hosts to determine the IP Multicast group membership. IGMP snooping checks IGMP packets passing through the network, picks out the group registration, and configures Multicasting accordingly.

Without IGMP Snooping, Multicast traffic is treated in the same manner as a Broadcast transmission in a Switch, which forwards packets to all ports on the network. With IGMP Snooping, Multicast traffic is only forwarded to ports that are members of that Multicast group. IGMP Snooping generates no additional network traffic, which significantly reduces the Multicast traffic passing through your switch.

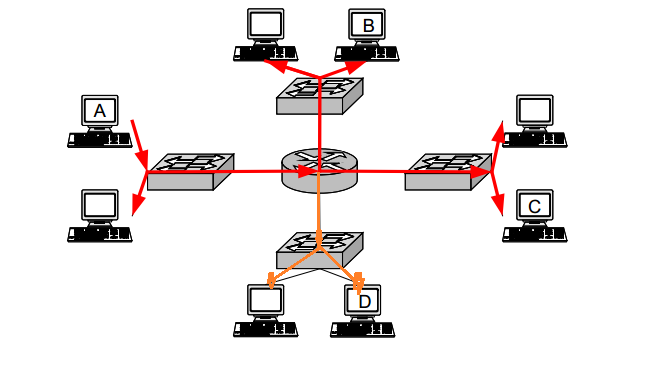
By listening to and analyzing IGMP messages, a Layer 2 device running IGMP Snooping establishes mappings between **ports and multicast MAC** addresses and forwards multicast data based on these mappings.

**An Example of IGMP Snooping:.**

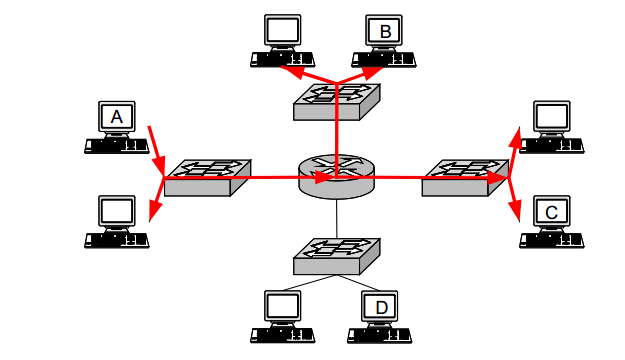


* 8 Host is connected through 4 lyer 2 switch, connected to one router in middle
* A is multicast trsamitter and B and C want to get it.

Without IGMP :



With IGMP but doesn’t have IGMP Snooping



With IGMP Snooping :

