Computer Networks Assignment 2

IGMP, ICMP, RARP

Submitted by:
Srividya Krishnakumar
CS6A
55

IGMP

The Internet Group Messaging protocol (IGMP) is one of the necessary, but not sufficient, protocols that is involved in multicasting. IGMP is a companion to the IP protocol.

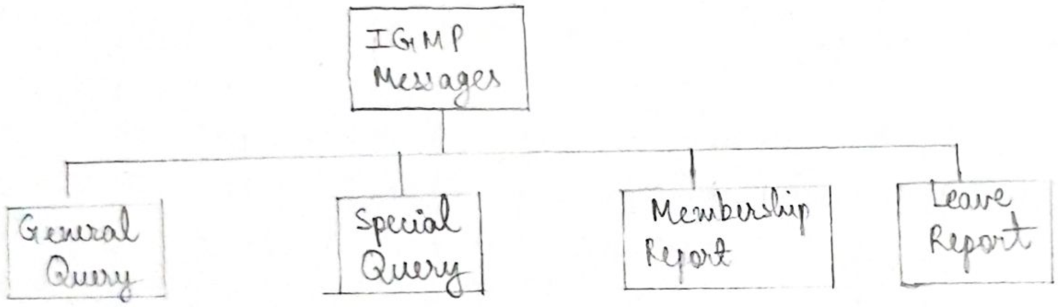
Group Management

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 that distribute multicast packets to hosts or other routers. IGMP gives the multicast routers information about the membership status of hosts (routers) connected to the network.

IGMP Messages

IGMPv2 has 3 types of messages – the query
- membership report
- leave report.

There are 2 types of query messages – general.
- Special.



Message Format

← 8 bits → ← 8 bits → ← 8 bits → ← 8 bits →

Type	Max. Response Time	Checksum
Group address in membership & leave reports and query; all 0s in general query.		

- **Type** – this 8 bit field defines the type of message.

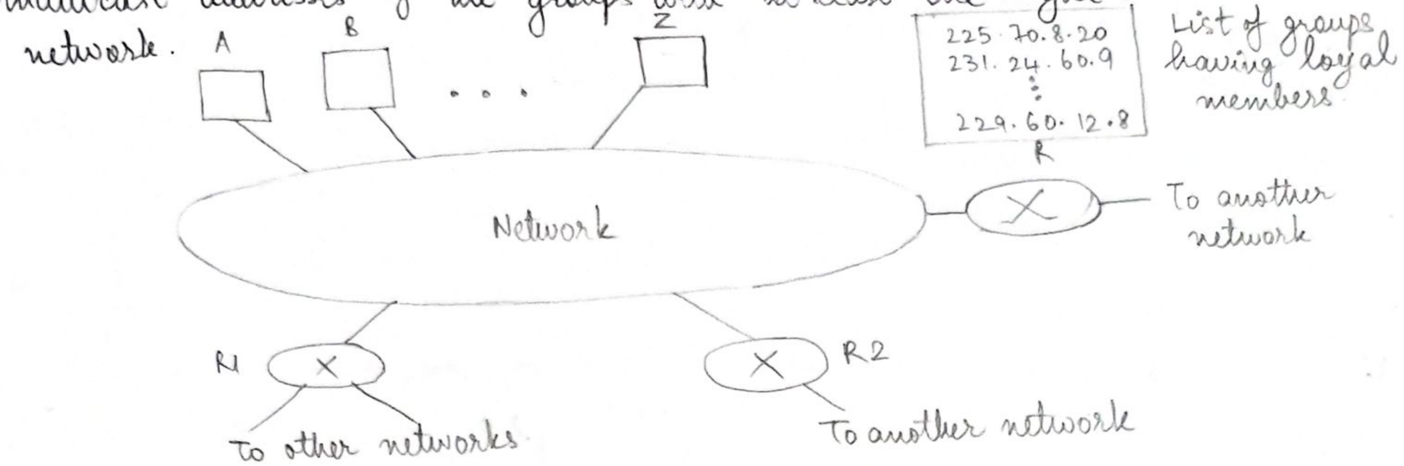
Type	Value
General or Special Query	0x11 or 0001 0001
Membership Report	0x16 or 0001 0110
Leave report	0x17 or 0001 0111

- **Maximum Response Time** – this 8 bit field defines the amount of time in which a query must be answered.

- Checksum- is a 16 bit field carrying the checksum.
- Group Address- value of this field is 0 for a general query message. The value defines the group id (multicast address of the group) in the special query, membership report & leave report.

IGMP Operation

IGMP operates locally. A multicast router connected to a network has a list of multicast addresses of the groups with at least one loyal member in that network.



For each group, there is 1 router that has the duty of distributing the multicast packets destined for that group. This means that if there are 3 multicast routers connected to a network, their lists of group ids are mutually exclusive.

A host/multicast router can have membership in a group. When a host has membership, it means that 1 of its processes (an applicⁿ program) receives multicast packets from some group. When a router has membership, it means that a network connected to 1 of its other interfaces receives these multicast packets. In both cases, the host & the router keep a list of group ids & relay their interest to the distributing router.

- Joining a Group-

A host or router can join a group. A host maintains a list of processes that have membership in a group. When a process wants to join a new group, it sends its request to the host. The host adds the name of the process & the name of the requested group to its list. If this is the 1st entry for this particular group, the host sends a membership report message.

- Leaving a Group

When a host sees that no process is interested in a specific group, it sends a leave report. Similarly, when a router sees that none of the networks connected to its interfaces is interested in a specific group, it sends a leave report about that group.

- **Monitoring Membership.**

A host or router can join a group by sending a membership report message. It can leave a group by sending a leave report message. However, sending these 2 types of messages is not enough. The multicast router is responsible for monitoring all the hosts or routers in a LAN to see if they want to continue their membership in a group.

- **Delayed Response.**

To prevent unnecessary traffic, IGMP uses a delayed response strategy. when a host or router receives a query message, it does not respond immediately; it delays the response. Each host or router uses a random no. to create a timer, which expires between 1 & 10s. A timer is set for each group in the list. Each host or router waits until its timer has expired before sending a membership report message. During this waiting time, if the timer of another host or router, for the same group, expires earlier, that host or router sends a membership report.

- **Query Router**

Query messages may create a lot of reesponses. to prevent unnecessary traffic, IGMP designates 1 router as query router for each network. Only this designated router sends the query message & the other routers are passive.

ICMP

The IP protocol has no error-reporting or error-correcting mechanism. It also lacks a mechanism for host & management queries.

The Internet Control Message Protocol (ICMP) has been designed to compensate for the above 2 deficiencies. It is a companion to the IP protocol.

Types of Messages

ICMP messages are divided into 2 broad categories:

(i) Error-reporting messages - report problems that a router or a host may encounter when it processes an IP packet.

(ii) Query messages - occur in pairs; help a host or network manager get specific information from a router or another host.

Message Format

An ICMP message has an 8-byte header and a variable size data section. Although the general format of the header is different for each message type, the 1st 4 bytes are common to all.

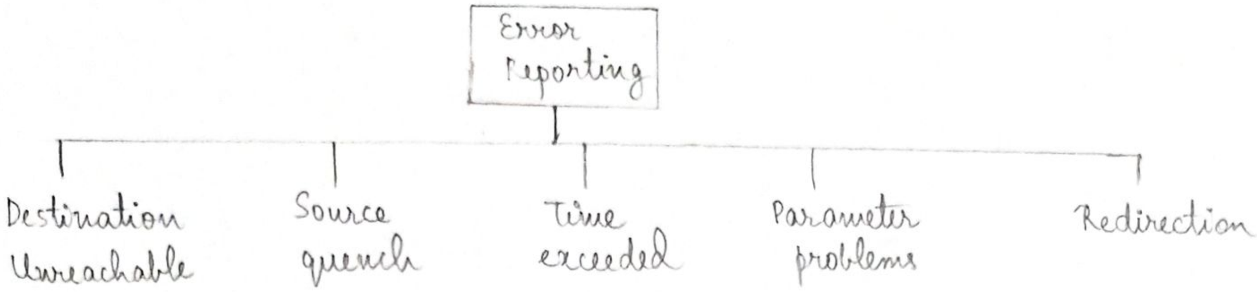
8 bits	8 bits	8 bits	8 bits
Type	Code	Checksum	
Rest of the header			
Data section			

The 1st field, ICMP type, defines the type of the message.
The code field specifies the reason for the specific message type.
The last common field is the checksum field.
The rest of the header is specific for each message type.

(i) Error reporting

One of the main responsibilities of ICMP is to report errors. However, ICMP doesn't correct errors - it simply reports. Error correction is left to the higher level protocols.

ICMP uses the source IP address to send the error message to the source (originator) of the datagram.



(a) Destination Unreachable

When a router cannot route a datagram or a host cannot deliver a datagram, the datagram is discarded & the router or the host sends a destination-unreachable message back to the source host that initiated the datagram.

(b) Source Quench

The source quench message in ICMP was designed to add a kind of control to the IP. When a router or host discards the datagram, due to congestion, it sends a source quench message to the sender of the datagram.

(c) Time Exceeded

This message is generated in 2 cases:

(i) when the time-to-live value reaches 0. after decrementing, the router discards the datagram. However, when the datagram is discarded, a time exceeded message must be sent by the router to the original source.

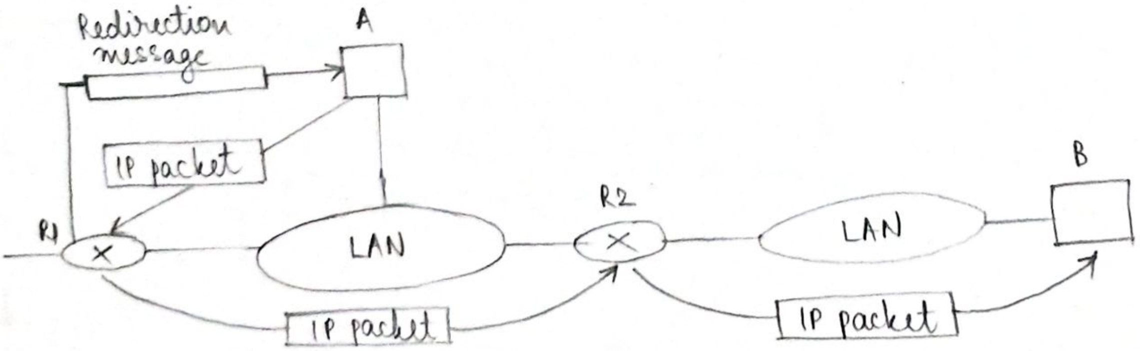
(ii) when not all fragments that make up a message arrive at the destination host within a certain time limit.

(d) Parameter Problem

If a router or the destination host discovers an ambiguous or missing value in any field of the datagram, it discards the datagram & sends a parameter problem message back to the source.

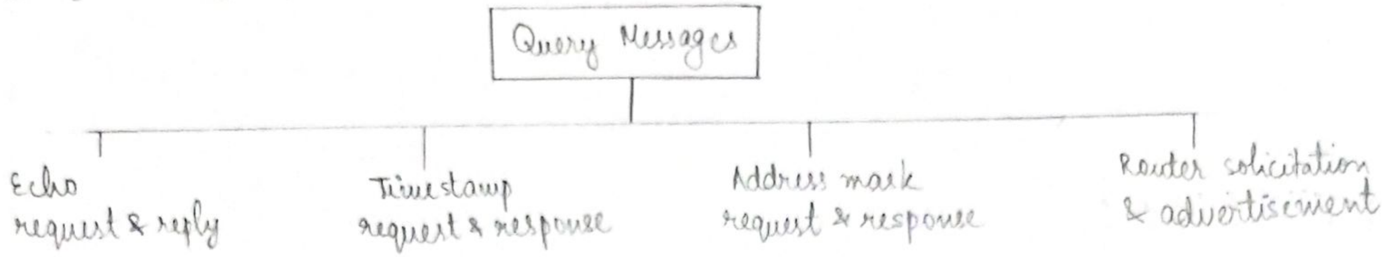
(e) Redirection

The host may send a datagram, which is destined for another network to the wrong router. In this case, the router that receives the datagram will forward the datagram to the correct router.
However, to update the routing table of the host, it sends a redirection message to the host.



(ii) Query

In this type of ICMP message, a node sends a message that is answered in a specific format by the destination node.


Query Messages
Echo request & reply
Timestamp request & response
Address mask request & response
Router solicitation & advertisement

(a) Echo request & reply.

The echo request & echo reply messages are designed for diagnostic purposes. Network managers & users utilize the pair of messages to identify network problems.

(b) Timestamp request & reply

2 machines (hosts or routers) can use the timestamp request & timestamp reply messages to determine the round-trip time needed for an IP datagram to travel between them.

(c) Address-Mask request & reply

A host may know its IP address, but not the corresponding mask. To obtain its mask, a host sends an address-mask-request message to a router on the LAN.

The router receiving the address-mask-request message responds with an address-mask-reply message, providing the necessary mask for the host.

(d) Router solicitation & Advertisement.

A host that wants to send data to a host on another network needs to know the address of routers connected to its own network. The router-solicitation & router-advertisement messages can help in this situation.

RARP.

The Reverse Address Resolution Protocol (RARP) allows a host to discover its Internet address when it knows only its physical address. It is used when a computer is connected to a network for the 1st time, or when a diskless computer is booted.

Mapping Physical to Logical Address.

There are occasions in which a host knows its physical address, but needs to know its logical address. This may happen in 2 cases:

1. A diskless station is just booted. The station can find its physical address by checking its interface, but does not know its IP address.
2. An organization doesn't have enough IP addresses to assign to each station; it needs to assign IP addresses on demand. The station can send its physical address & ask for a short-time lease.

RARP finds the logical address for a machine that knows only its physical address. Each host or router is assigned 1 or more logical (IP) addresses, which are unique & independent of the physical (hardware) address of the machine. To create an IP datagram, a host or a router needs to know its own IP address(es). The IP address of a machine is usually read from its configuration file stored on a disk.

However, a diskless machine is usually booted from ROM, which has minimum booting information. The ROM is installed by the manufacturer. It cannot include the IP address because the IP addresses on a network are assigned by the network administrator.

The machine can get its physical address (by reading its NIC, for example), which is unique locally. It can then use the physical address to get the logical address by using the RARP protocol. A RARP request is created and broadcast on the local network.
Another machine on the local network that knows all the IP addresses will respond with a RARP reply. The requesting machine must be running a RARP client program; the responding machine must be running a RARP server program.

There is a serious problem with RARP. Broadcasting is done at the data link layer. The physical broadcast address, all 1s in the case of Ethernet, does not pass the boundaries of a network. This means that if an administrator has several networks or several subnets, it needs to assign a RARP server for each network or subnet. This is the reason that RARP is almost obsolete.