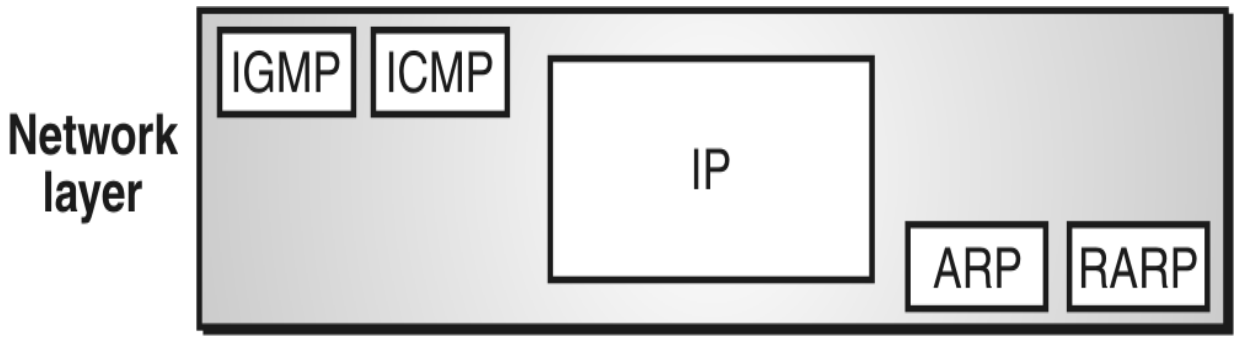
Computer Network(CSC 503)

Shilpa Ingoley

Lecture 29 and 30

- 4.3 **Protocols** - ARP,RARP, ICMP, IGMP



Address Resolution Protocol (ARP)

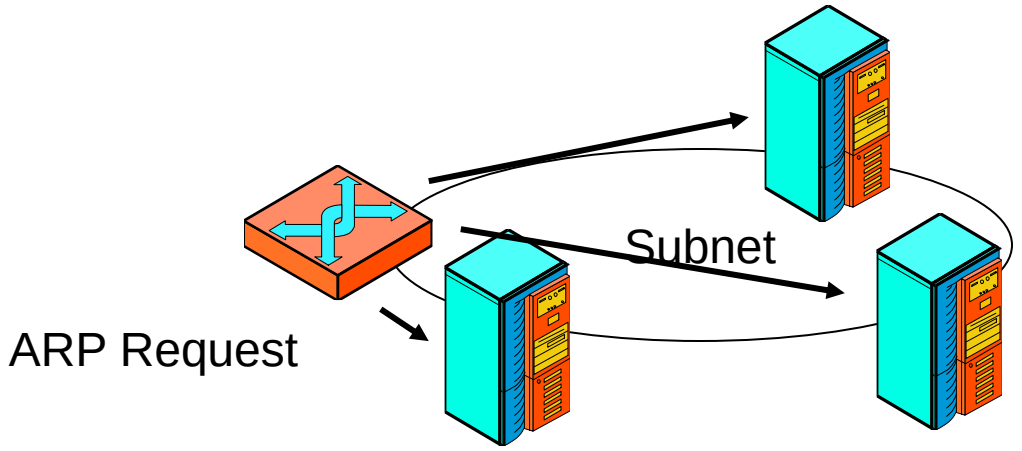
- For sending packet on internet IP address is not sufficient.
- DLL NIC does not understand IP address.
- Therefore, We need to address the problem of mapping IP address to NIC address.
- The address resolution protocol (ARP) is a protocol used by the Internet Protocol (IP), specifically IPv4, to map IP network addresses to the hardware addresses used by a data link protocol.

- **IP address(input) → ARP → Physical (NIC's/Ethernet) address (output)**

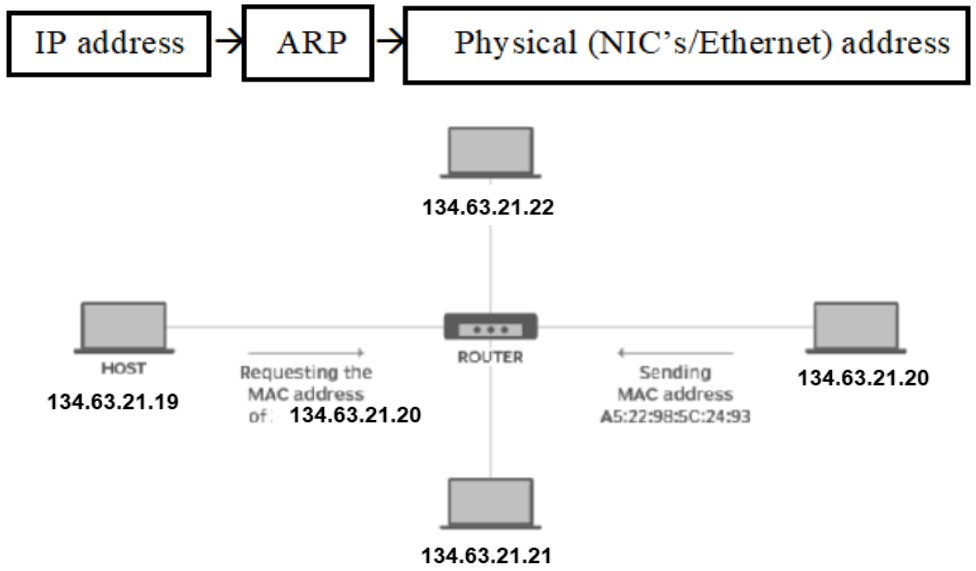
- The term address resolution refers to the process of finding an address of a computer in a network.

Address Resolution Protocol (ARP)

- Router creates an ARP Request message to be sent to all hosts on the subnet.
  - Address resolution protocol message asks “Who has IP address 134.63.21.20?”
  - Passes ARP request to data link layer process for delivery



Working of ARP



Address resolution protocol message asks "Who has IP address 134.63.21.20?"

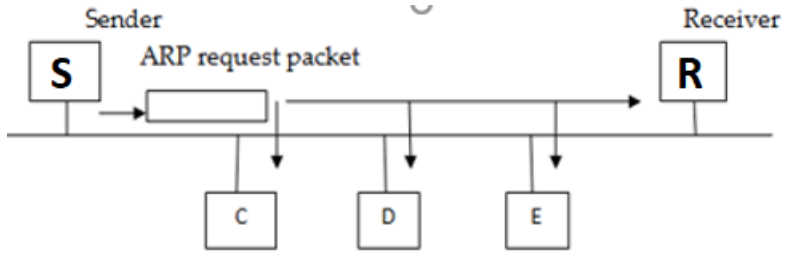
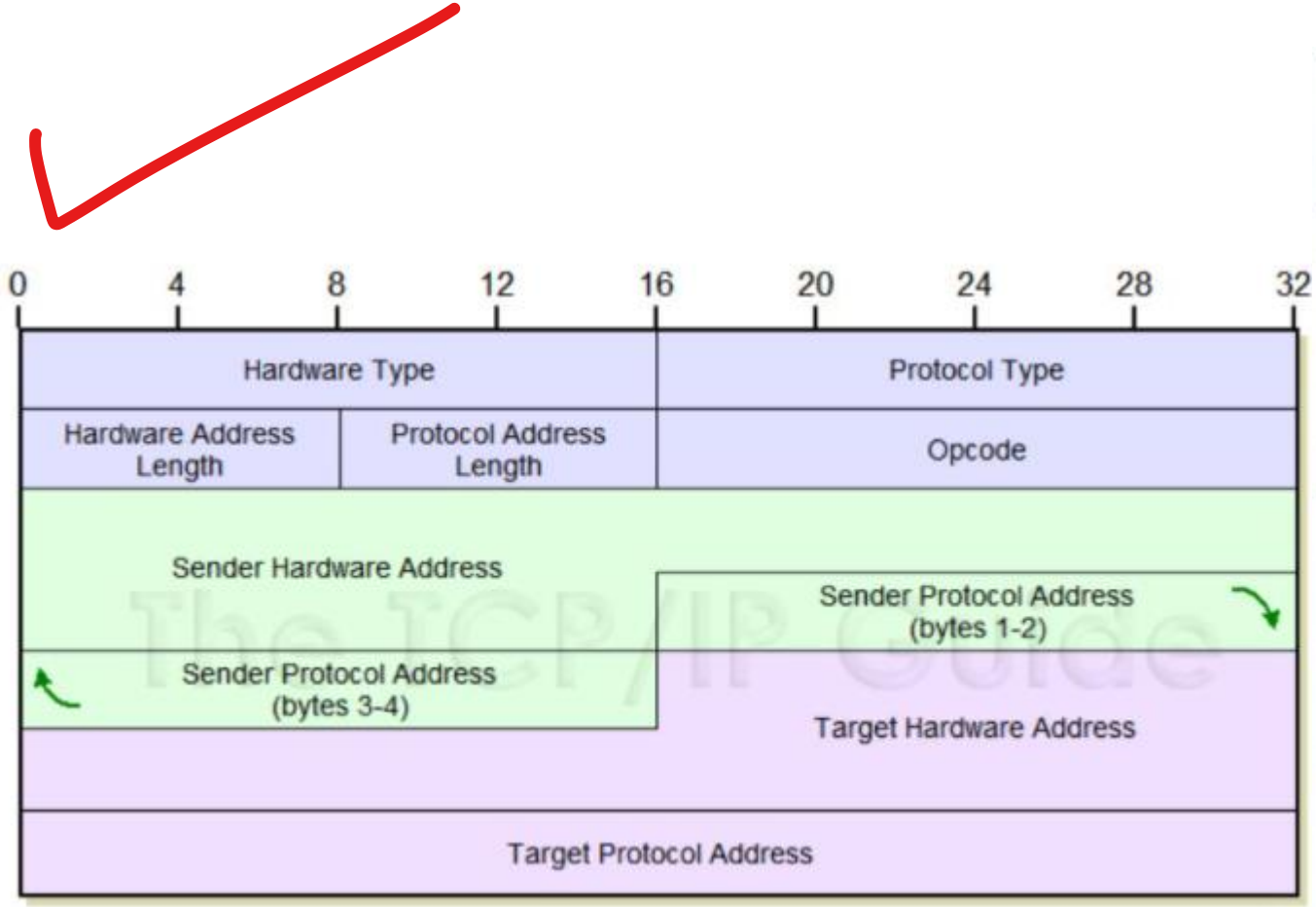
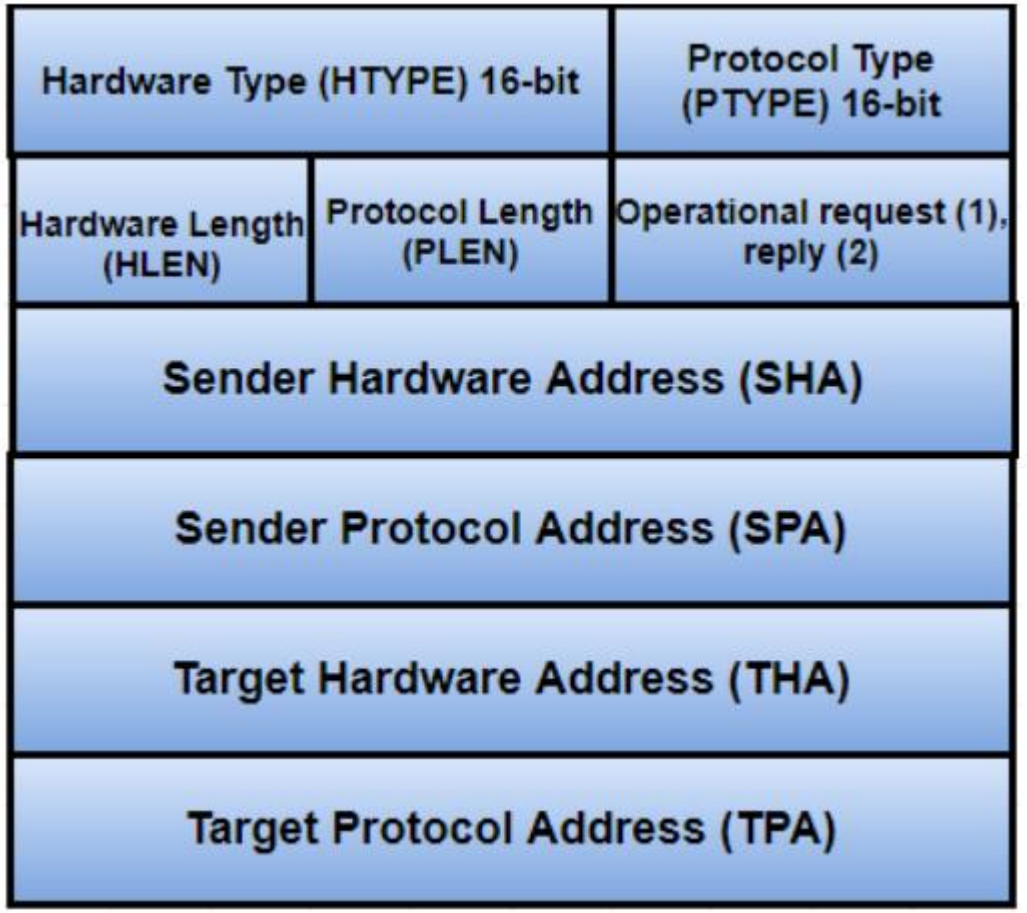


Fig : ARP request packet is broadcasted over the network

- All the hosts on network receivers and processes ARP request packet. Only host with IP address recognizes its IP address and sends back ARP response as its Physical address(MAC).
- The response is unicast and will receive by sending host only.

Packet Structure of ARP





Contd...

1. HTYPE (Hardware Type : 16 bits) : This field specifies the network link protocol type. Ex: Ethernet is 1.

2. Protocol type (PTYPE) PTYPE (Protocol Type : 16 bits): This field specifies the internetwork protocol for which the ARP request is intended. For IPv4, this has the value 0x0800.

3.Hardware length (HLEN) HLEN (Hardware Length: 8 bits) : Length (in octets) of a hardware address. Ethernet address length is 6.

4. Protocol length (PLEN) PLEN (Protocol Length : 8 bits) : Length (in octets) of internetwork addresses. The internetwork protocol is specified in PTYPE. Example: IPv4 address length is 4.

5. Operation OPER (Operation: 16 bits) : Specifies the operation that the sender is performing:

- 1 for request
- 2 for reply.

6. Sender hardware address (SHA) SHA (Sender Hardware Address: 6 bytes) : Media address of the sender. In an ARP request this field is used to indicate the address of the host sending the request.

- In an ARP reply, this field is used to indicate the address of the host that the request was looking for.

7.SPA (Sender Protocol Address: 4 bytes) : Internetwork address of the sender.

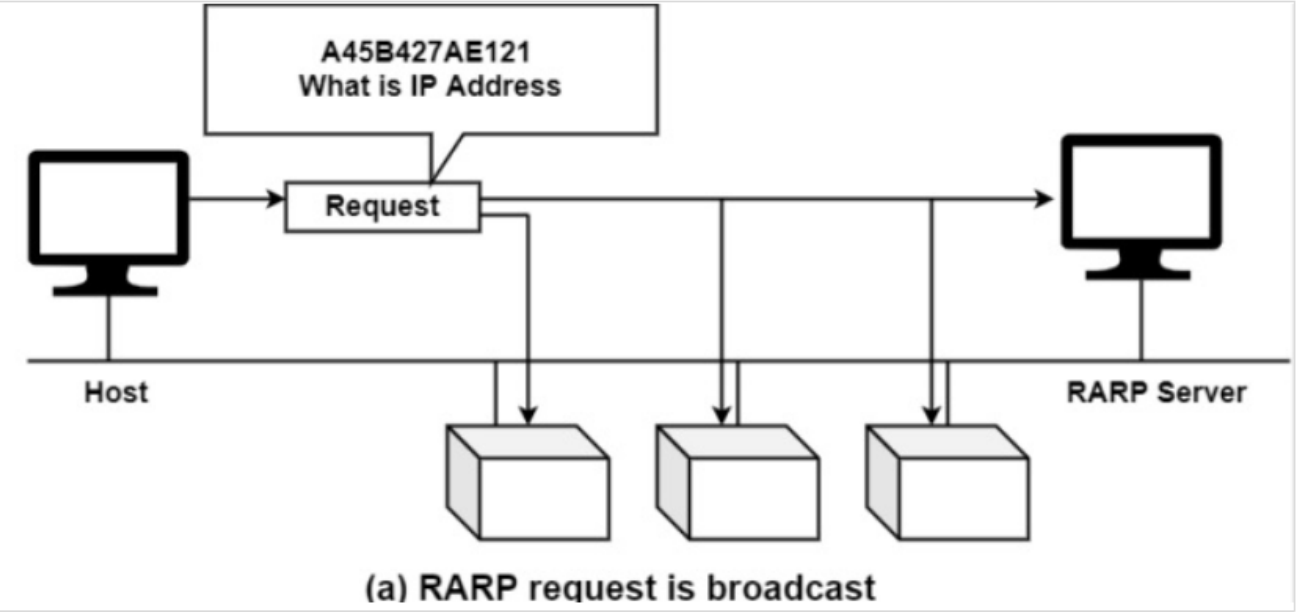
8. THA (Target Hardware Address : 6 bytes): Media address of the intended receiver. In an ARP request this field is ignored. In an ARP reply this field is used to indicate the address of the host that originated the ARP request.

9.TPA (Target Protocol Address : 4 bytes) : Internetwork address of the intended receiver.

Reverse Address Resolution Protocol (RARP)

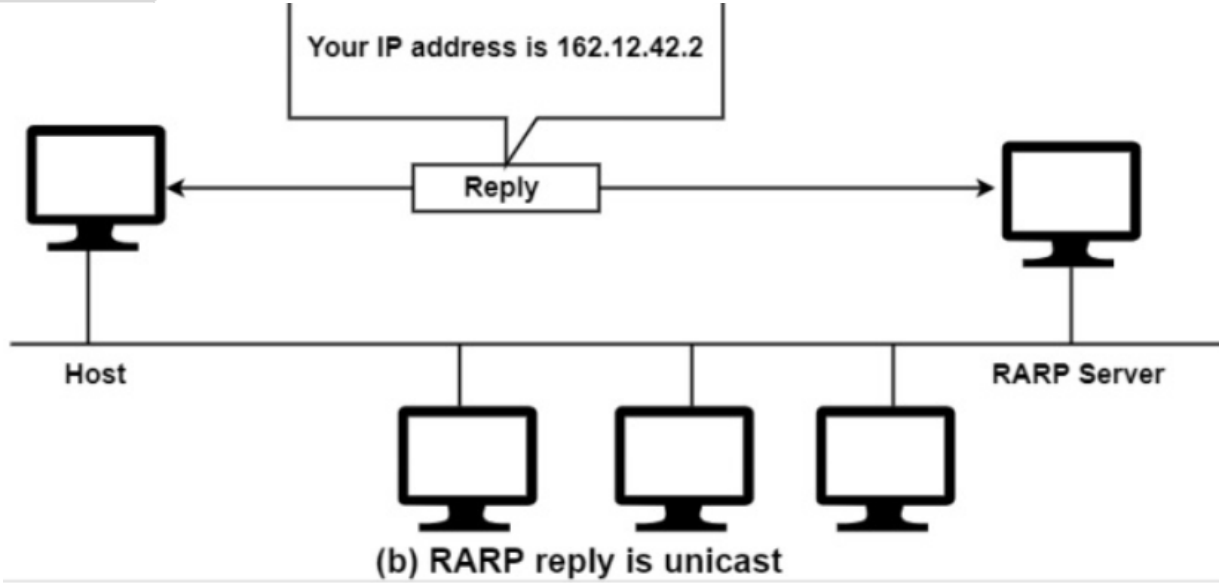
- The Reverse Address Resolution Protocol (RARP) is used by a client computer to request its Internet Protocol (IPv4) address from a computer network, when all it has available is its hardware address-a MAC address.
- Some network hosts, such as a diskless workstation, do not know their own IP address when they are booted. To determine their own IP address, they use a mechanism similar to ARP, but now the hardware address of the host is the known parameter, and the IP address is the queried parameter.
- The reverse address resolution is performed the same way as the ARP address resolution. The same packet format is used for the ARP.
- An exception is the operation code field that now takes the following values−
  - 3 for RARP request
  - 4 for RARP reply
- The client broadcasts the request
- RARP requires one or more server hosts to maintain a database of mappings of Link Layer addresses to their respective protocol addresses.
- Media Access Control (MAC) addresses need to be individually configured on the servers by an administrator. RARP is limited to serving only IP addresses.
- It has been made obsolete by the Bootstrap Protocol (BOOTP) and the modern Dynamic Host Configuration Protocol (DHCP), both of which support a much greater feature set than RARP.

Working of RARP



(a) RARP request is broadcast

ARP only assumes that every host knows the mapping between its own hardware address and protocol address. RARP requires one or more server hosts in the network to maintain a database of mapping between hardware address and protocol address so that they will be able to reply to requests from client hosts.



(b) RARP reply is unicast

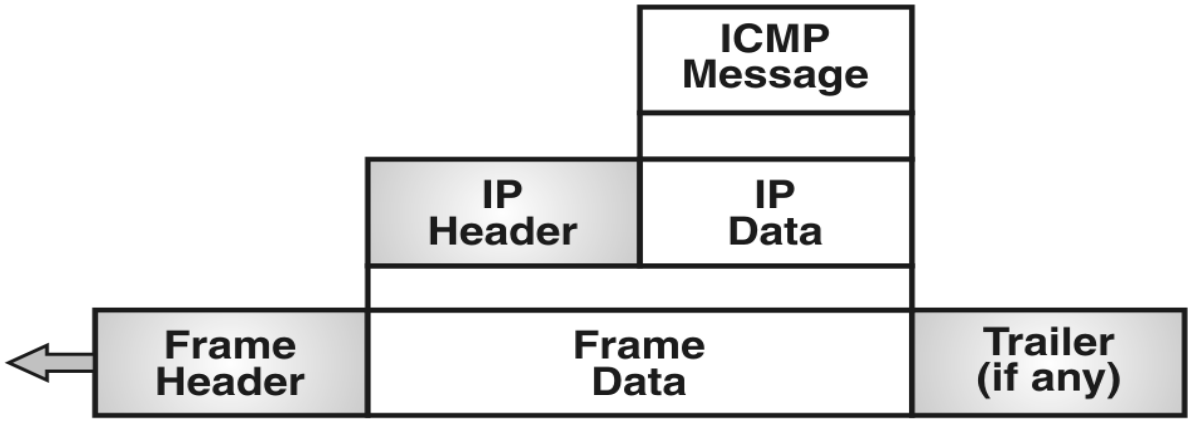
Internet Control Message Protocol (ICMP)

- The IPv4 has **no error-reporting** or error-correcting mechanism.
  - If an error has occurred, IP protocol has no built-in mechanism to notify the original host.
- The IP protocol also lacks a mechanism for **host and management queries.**
  - A **host** sometimes needs to determine if a router or another **host is alive**.
  - And sometimes a **network manager** needs information from another **host or router.**

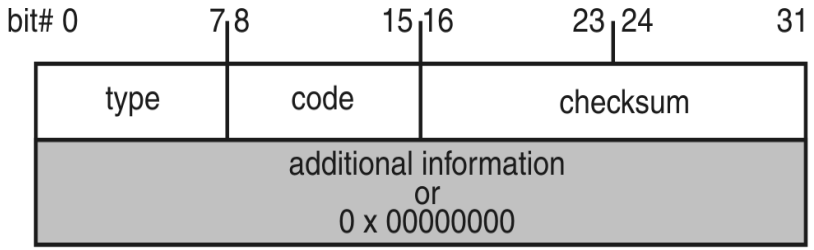
- The **ICMPv4** has been designed to compensate for the above two deficiencies

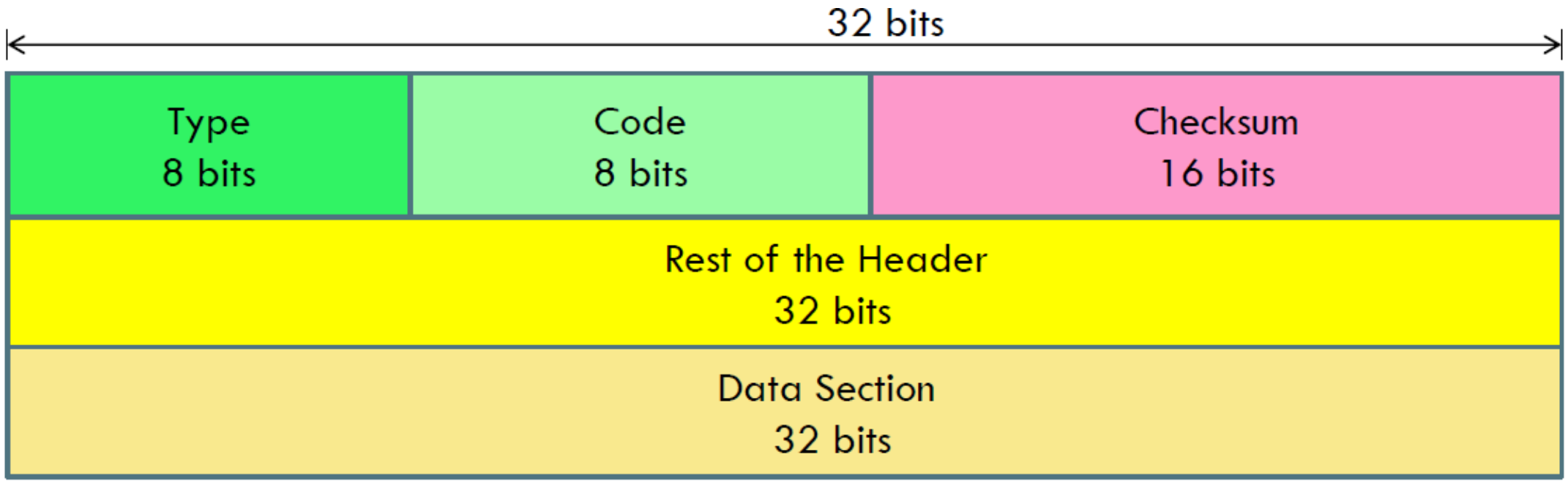
Contd...

- It is a companion to the IP protocol. ICMP itself is a network-layer protocol.
- The messages are first encapsulated inside IP datagrams before going to the lower layer.
- When an IP datagram encapsulates an ICMP message, the value of the protocol field in the IP datagram is set to 1 to indicate that the IP payroll is an ICMP message.



ICMP Header Format



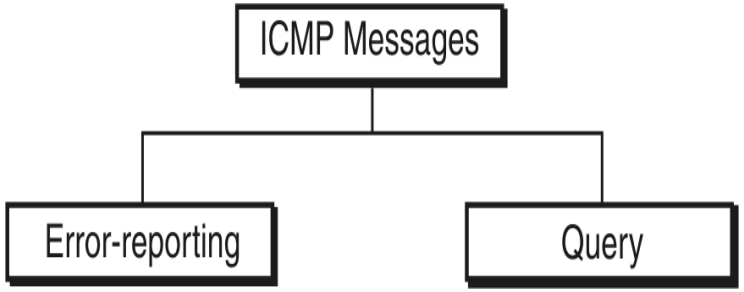


An ICMP message has an 8-byte header and a variable-size data section.
The general format of the header is different for each message type, the first 4 bytes are common to all.

Contd...

- **Type:** It is the first field that defines the **type of the message.**
- **Code:** This field specifies the **reason** for the particular message type.
- **Checksum:** The last common field is the checksum field. The checksum is calculated over the **entire message** (header and data).

  - The rest of the header is specific for each message type.
- **Data Section/Additional information:** If there is no additional data, there are 4 bytes set to zero. Each ICMP messages is at **least 8 bytes** long.
  - The data section in **error messages** carries information for finding the **original packet that had the error.**
  - In **query messages,** the data section carries extra information based on the **type of query.**

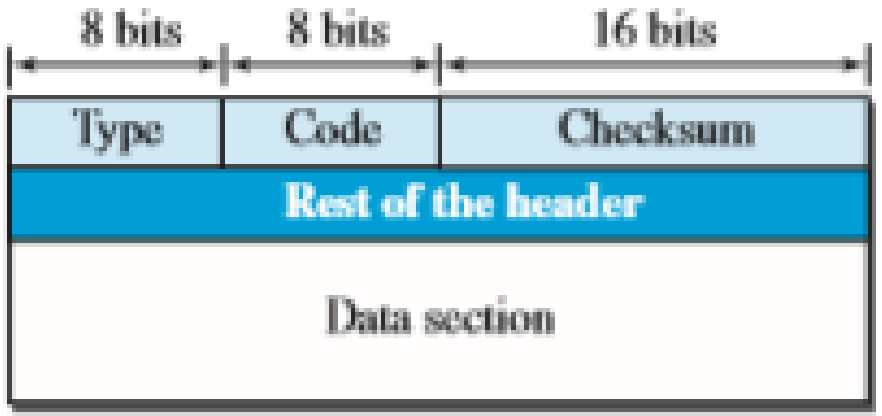


ICMP messages are divided into **two** broad categories:

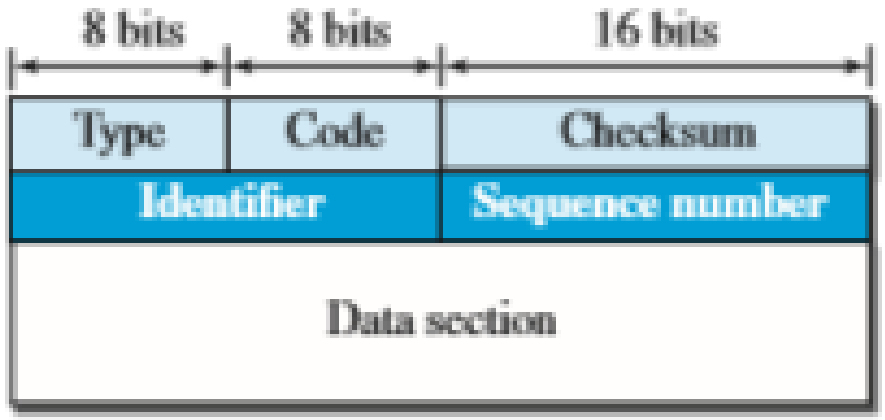
- **1. Error-reporting messages :** The error-reporting messages report problems that **a router or a host** (destination) may encounter when it processes an IP packet.
- **2. Query messages:** The query messages, which occur **in pairs**, help a host or a network manager get specific information from a router or another host.

Category	Type	Message
Error-reporting message	3	Destination unreachable
	4	Source quench
	11	Time exceeded
	12	Parameter problem
	5	Redirection
Query message	8 or 0	Echo request or reply
	13 or 4	Timestamp request or reply

Contd...



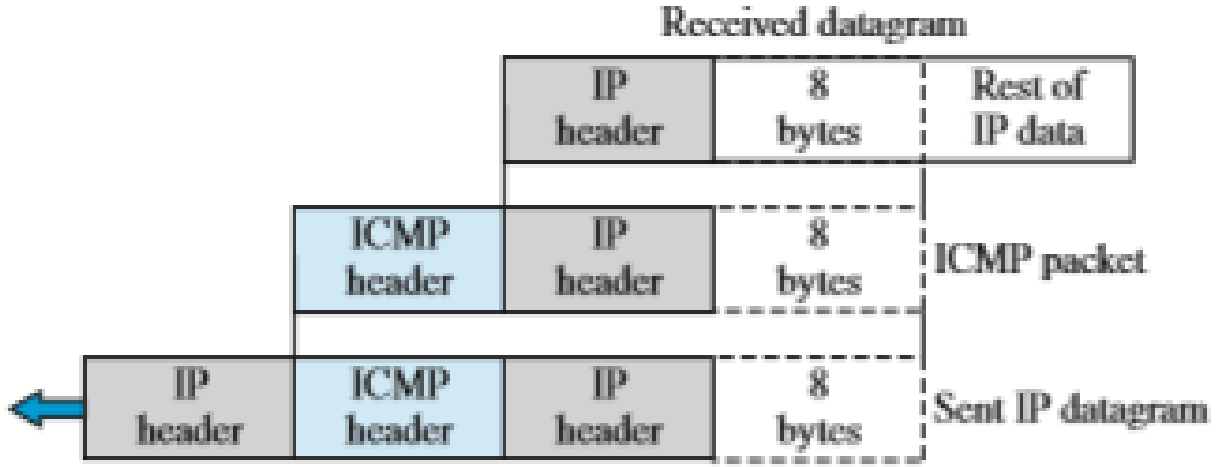
Error-reporting messages



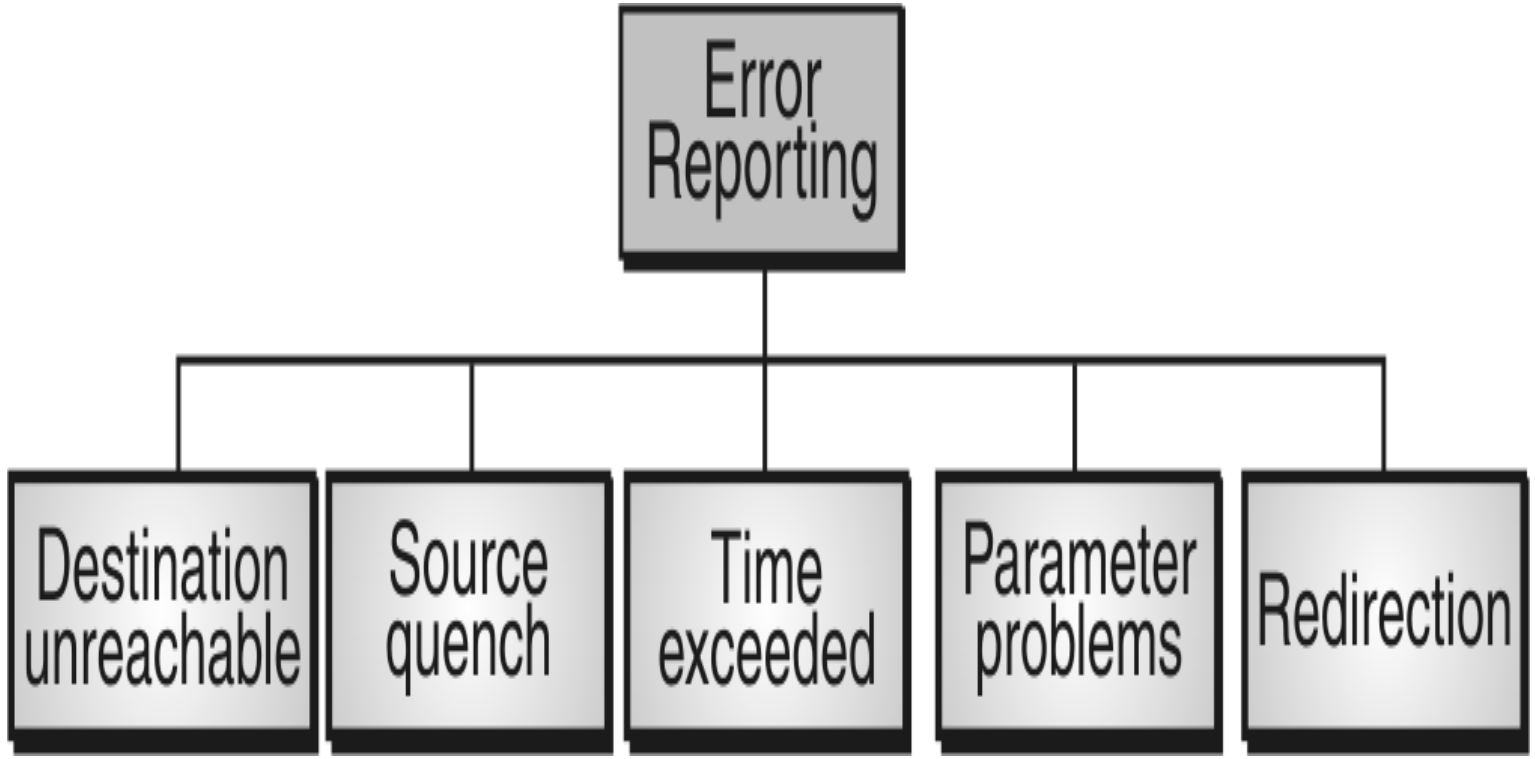
Query messages

ICMP Error Messages

- All error messages contain a data section that includes the **IP header of the original datagram plus the first 8 bytes** of data in that datagram.
- These 8 bytes of data are included because the first 8 bytes provide information about the port numbers (UDP and TCP) and sequence number (TCP). This information is needed so the source can inform the protocols (TCP or UDP) about the error
- ICMP forms an error packet, which is then encapsulated in an IP datagram



Error Reporting Messages



Contd…

Destination Unreachable (type 3) :

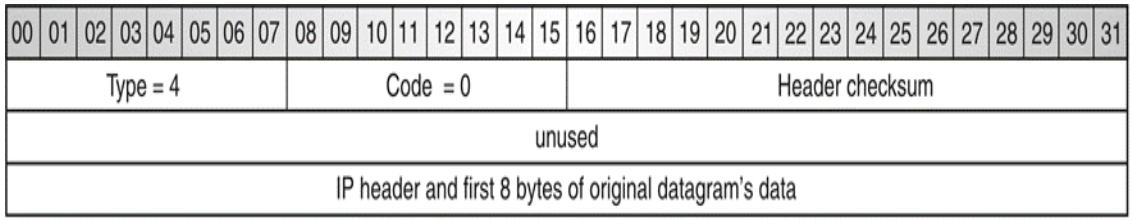
- It is most widely used error message
- This message uses different codes (0 to 15) to define the type of error message and the reason why a datagram has not reached its final destination.
- For example, code numbers tells the source that a host is unreachable. This may happen when we use the HTTP protocol to access a web page, but the server is down. The message “destination host is not reachable” is created and sent back to the source

Code	Description
0	Network unreachable error.
1	Host unreachable error.
2	Protocol unreachable error (the designated transport protocol is not supported).
3	Port unreachable error (the designated protocol is unable to inform the host of the incoming message).
4	The datagram is too big. Packet fragmentation is required but the 'don't fragment' (DF) flag is on.
5	Source route failed error.
6	Destination network unknown error.
7	Destination host unknown error.
8	Source host isolated error.
9	The destination network is administratively prohibited.
10	The destination host is administratively prohibited.
11	The network is unreachable for Type of Service.
12	The host is unreachable for Type of Service.
13	Communication administratively prohibited (administrative filtering prevents packet from being forwarded).
14	Host precedence violation (indicates the requested precedence is not permitted for the combination of host or network and port).
15	Precedence cutoff in effect (precedence of datagram is below the level set by the network administrators).

Contd...

Source Quench (type 4) :

- It informs the sender that the network has encountered congestion and the datagram has been dropped; the source needs to slow down sending more datagrams.



00 01 02 03 04 05 06 07	08 09 10 11 12 13 14 15	16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
Type = 4	Code = 0	Header checksum
unused		
IP header and first 8 bytes of original datagram's data		

Parameter Problem (type 12):

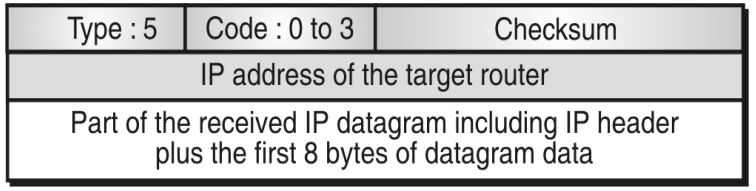
- It can be sent when either there is a problem in the header of a datagram (code 0) or some options are missing or cannot be interpreted (code 1).

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 of datagram data		

Contd…

Redirection Message (type 5):

- It is used when the source uses a wrong router to send out its message. The router **redirects the message to the appropriate router**, but informs the source that it needs to change its default router in the future. The IP address of the default router is sent in the message.



Time Exceeded:

- The TTL field prevents a datagram from being aimlessly circulated in the Internet. When the **TTL value becomes 0, the datagram is dropped** by the visiting router and a time exceeded message (type 11) with code 0 is sent to the source to inform it about the situation. The time-exceeded message (with code 1) can also be sent when not all fragments of a datagram arrive within a predefined period of time.

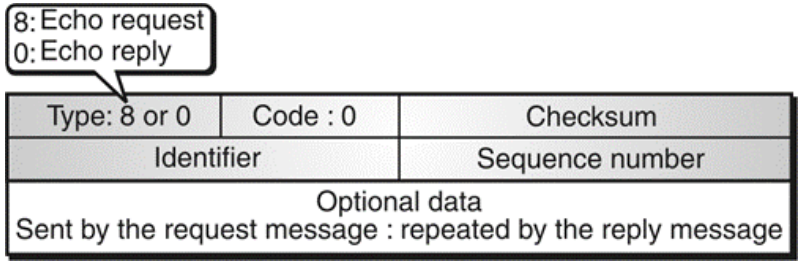
Code	Description
0	Time-to-live exceeded in transit.
1	Fragment reassembly time exceeded.

Contd...

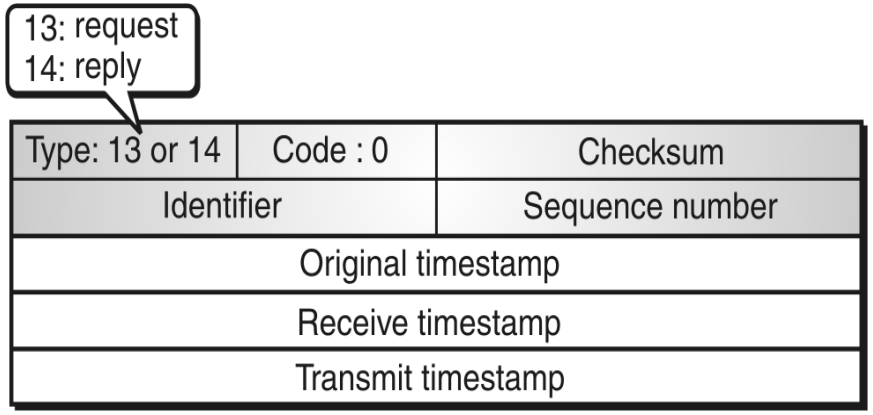
- No ICMP error message will be generated in response to a datagram carrying **an ICMP error message.**
- No ICMP error message will be generated for a **fragmented datagram that is not the first fragment.**
- No ICMP error message will be generated for a datagram having a **multicast address**.
- No ICMP error message will be generated for a datagram having **a special address such as 127.0.0.0 or 0.0.0.0.**

ICMP Query Messages

- Query messages in ICMP can be used independently without relation to an IP datagram.
- Query messages are used to
  - **Probe or test** the liveliness of hosts or routers in the Internet,
  - Find the **one-way or the round-trip time** for an IP datagram between two devices,
  - Find out whether the **clocks in two devices are synchronized**.
- Query messages come in pairs: **request and reply.**
  - Example: The **echo request (type 8)** and the **echo reply (type 0)** pair of messages are used by a host or a router to test the liveliness of another host or router.



Timestamp Request Reply



- Sending time = receive timestamp - original timestamp
- Receiving time = returned time - transmit time
- Round-trip time = sending time + receiving time

ICMP For Debugging (Debugging Tools)

Tools that use ICMP for debugging:

- **ping**
- **traceroute or tracert**

Ping (Packet Internet Groper)

- The ping program is used to find if a **host is alive and responding**.
- The source host sends ICMP **echo-request messages**
- The destination, **if alive**, responds with ICMP **echo-reply messages**.
- The ping program sets the identifier field in the echo-request and echo-reply message and starts **the sequence number** from **0**;
- This number is **incremented by 1 each time a new message** is sent.
- Ping can calculate the **round-trip** time.
- It inserts the **sending time** in the **data section** of the message.
- When the packet arrives, it subtracts the arrival time from the departure time to get the **round-trip time (RTT)**.

Traceroute

- The traceroute program in UNIX or tracert in Windows can be used to trace the path of a packet from a source to the destination.
- It can find the IP addresses of all the routers that are visited along the path.
- The program is usually set to check for the maximum of 30 hops (routers) to be visited.
- The number of hops in the Internet is normally less than this.
- **Difference between Traceroute and Tracert:** The tracert program in windows behaves differently. The tracert messages are encapsulated directly in IP datagrams. The tracert, like traceroute, sends echo-request messages. However, when the last echo request reaches the destination host, an echo replay message is issued.

Internet Group Management Protocol (IGMP)

- IGMP is an integral part of **IP multicast**.
- IGMP is a communications protocol used by **hosts and adjacent routers** on IPv4 networks to establish **multicast group memberships**.
- IGMP is a protocol defined at the network layer
- It is one of the auxiliary protocols, like ICMP, which is considered part of the IP.
- IGMP messages, like ICMP messages, are **encapsulated in an IP datagram**.
- IGMP can be used for one-to-many networking applications such as **online streaming video and gaming**, and allows more efficient use of resources when supporting these types of applications.

Contd...

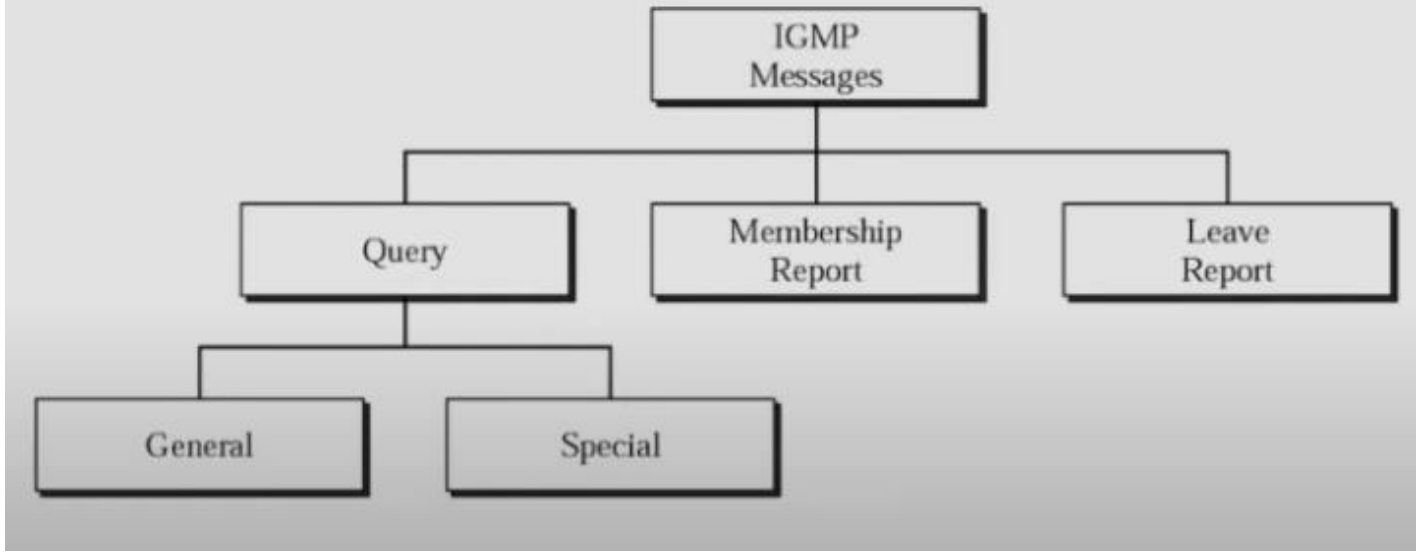
Following are versions of IGMP :

- IGMPv1
- IGMPv2
- IGMPv3

Contd…

- There are only **different** types of messages in IGMP
  - **Query Message**: A query message is **periodically** sent by a router to all hosts attached to it to ask them to report their interests about membership in groups
  - **Report messages**: A report message is sent by a host as a response to a query message.

IGMP MESSAGES



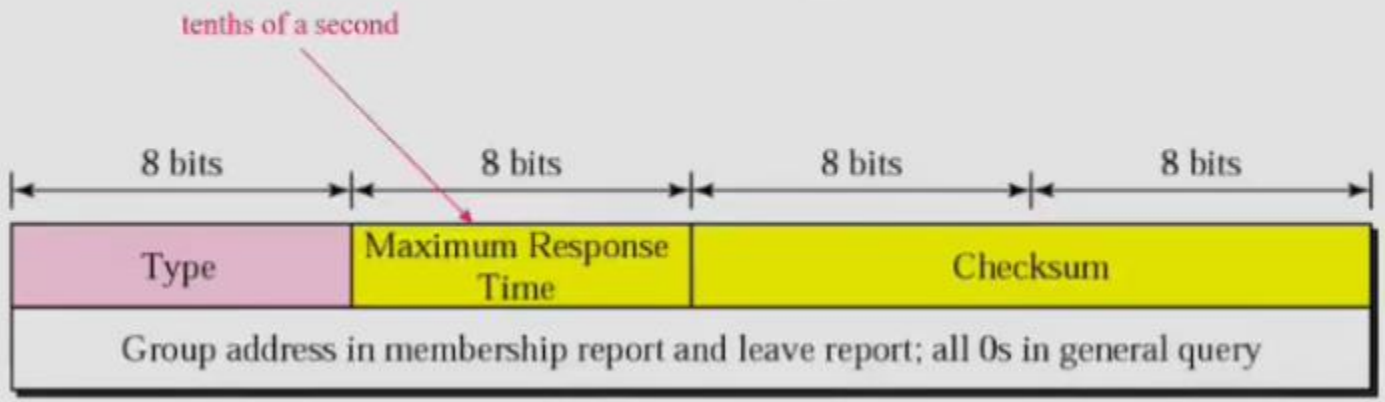
IGMP Query Message

- The query message is **sent by a router to all hosts** in each interface to collect information about their membership.
- There are three versions of query messages:
- **General Query Message:** It is sent about membership in any group.
  - It is encapsulated in a datagram with the destination address 224.0.0.1 (all hosts and routers).
  - All routers attached to the same network receive this message to inform them that this message is already sent and that they should refrain from resending it.

IGMP Messages

- There are several types of IGMP messages:
  - **General membership queries :** Sent by multicast routers to determine which multicast addresses are of interest to systems attached to the network(s) they serve to refresh the group membership state for all systems on its network.
  - **Group-specific membership queries :** Used for determining the reception state for a particular multicast address
  - **Group-and-source-specific queries :** Allow the router to determine if any systems desire reception of messages sent to a multicast group from a source address specified in a list of unicast addresses
  - **Membership reports :** Sent by multicast receivers in response to a membership query or asynchronously when first registering for a multicast group
  - **Leave group messages :** Sent by multicast receivers when specified multicast transmissions are no longer needed at the receiver.

IGMP message format



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

IGMPv2 packet structure

bit offset	0–7	8–15	16–31
0	Type	Max Resp Time	Checksum
32	Group Address		

1. Type :Indicates the message type as follows

Message	Type value
Membership Query	0x11
IGMPv1 Membership Report	0x12
IGMPv2 Membership Report	0x16
IGMPv3 Membership Report	0x22
Leave Group	0x17

2. Max Resp Time

- Specifies the required responsiveness of replies to a Membership Query (0x11).
- This field is meaningful only in Membership Query; in other messages it is set to 0 and ignored by the receiver.
- The field specifies time in units of 0.1 second (a field vale of 10 specifies 1 second).
- Larger values reduce IGMP traffic burstiness and smaller values improve protocol responsiveness when the last host leaves a group.

3. Group Address

- This is the **multicast address** being queried when sending a Group-Specific or Group-and-Source-Specific Query.
- The field is zeroed when sending a General Query.

Contd…

- **Group-Specific query message:** It is sent from a router to ask about the membership related to **a specific group**.
- This is sent when a router **does not receive a response about a specific group** and wants to be sure that there is **no active member of that group** in the network.
- The group identifier (multicast address) is mentioned in the message.
- The message is encapsulated in a datagram with the destination address set to the corresponding multicast address.
- Although all hosts receive this message, those **not interested drop it**.

Contd…

- **Source-and-group-specific query message:** It is sent from a router to ask about the **membership related to a specific group** when the message comes from a **specific source or sources**.
- Again the message is sent when the router **does not hear** about a specific group related to a **specific host or hosts**.
- The message is encapsulated in a datagram with the destination address set to the corresponding multicast address.
- Although all hosts receive this message, those **not interested drop it**.

IGMP Report Message

- A report message is **sent by a host as a response to a query** message.
- The message contains a list of records in which each record gives **the identifier of the corresponding group (multicast address)** and the addresses of all sources that the host is interested in receiving messages from **(inclusion).**
- The record can also mention the source addresses from which the host does not desire to receive a group message **(exclusion).**
- The message is encapsulated in a datagram with the multicast address 224.0.0.22 (multicast address assigned to IGMPv3).

Contd…

- In IGMPv3, if a host needs to join a group, it **waits until** it receives a query message and then sends a report message.
- If a host **needs to leave a group**, it does **not respond to a query message**.
- If **no other host responds** to the corresponding message, **the group is removed** from the router database.