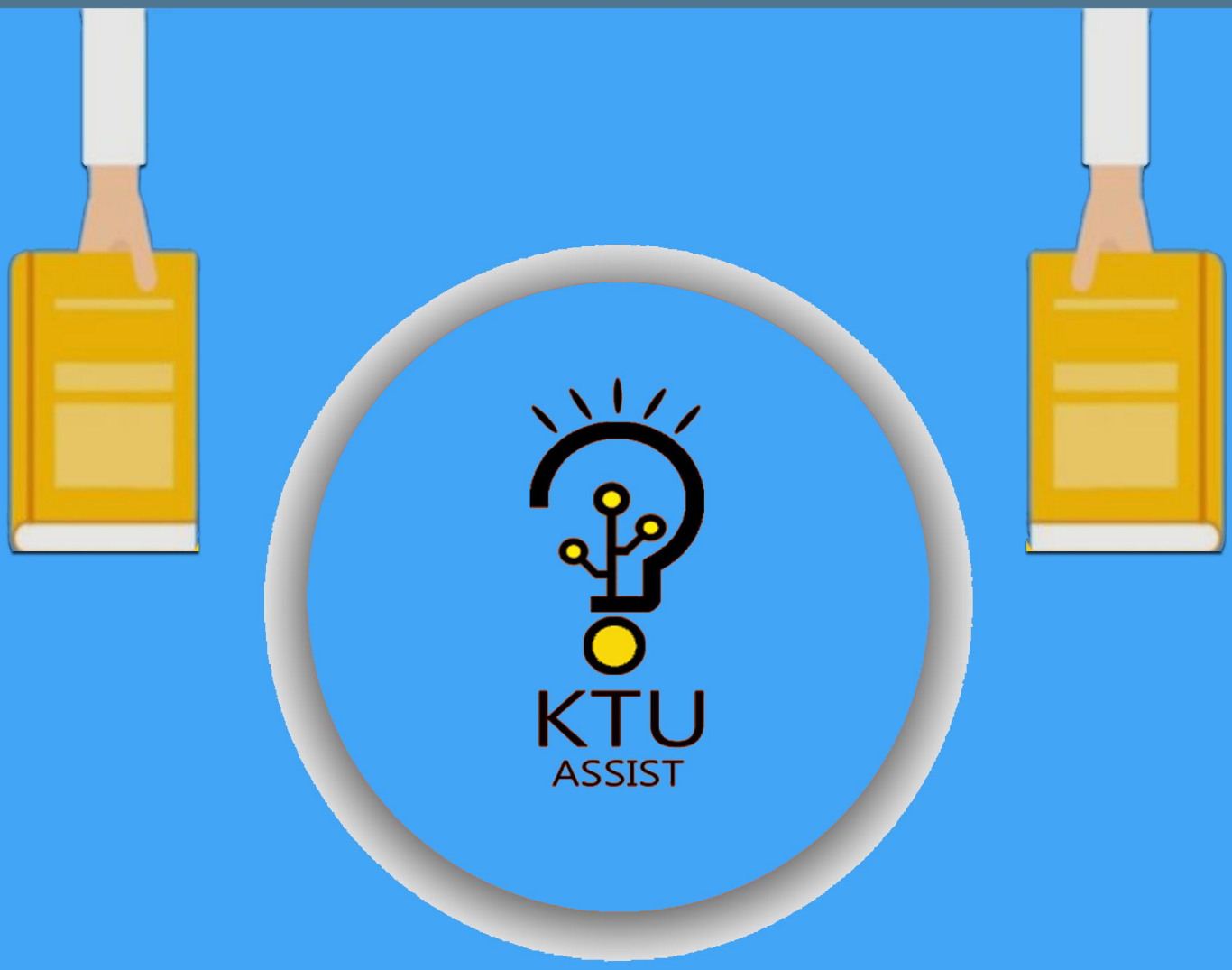
APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

STUDY MATERIALS



INTERNET CONTROL PROTOCOLS

Ques 1) What are the internet control protocols? List them.

Ans: Internet Control Protocols

At the network layer (or, more accurately, the internetwork layer), TCP/IP supports the internetwork protocol (IP). IP contains four supporting protocols:

1) Address Resolution Protocol(ARP)
2) Reverse Address Resolution Protocol (RARP)
3) Internet Control Message Protocol(ICMP)
4) Internet Group Message Protocol(IGMP)
5) BOOTP

Ques 2) Discuss about Internet Control Message Protocol (ICMP)?

Ans: Internet Control Message Protocol (ICMP)

The internet control message protocol (ICMP) is a mechanism used by hosts and routers to send notification of datagram problems back to the sender. ICMP uses echo test/reply to test whether a destination is reachable and responding.

It also handles both control and error messages, but its sole function is to report problems, not correct them. Responsibility for correction lies with the sender.

A datagram carries only the addresses of the original sender and the final destination. It does not know the addresses of the previous router(s) that passed it along. For this reason, ICMP can send messages only to the source, not to an intermediate router. ICMP is often considered part of the IP layer.

It communicates error messages and other conditions that require attention. ICMP messages are usually acted on by either the IP layer or the higher layer protocol (TCP or UDP). Some ICMP messages cause errors to be returned to user processes. ICMP messages are transmitted within IP datagrams, as shown in **figure 5.1**:

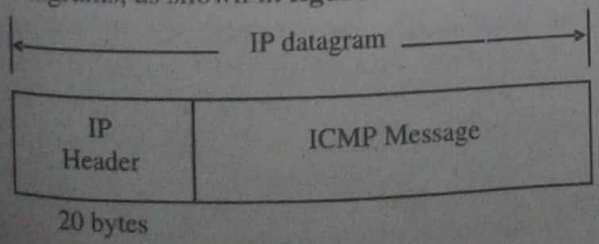


Figure 5.2 shows the format of an ICMP message. The first 4 bytes have the same format for all messages, but the remainder differs from one message to the next.

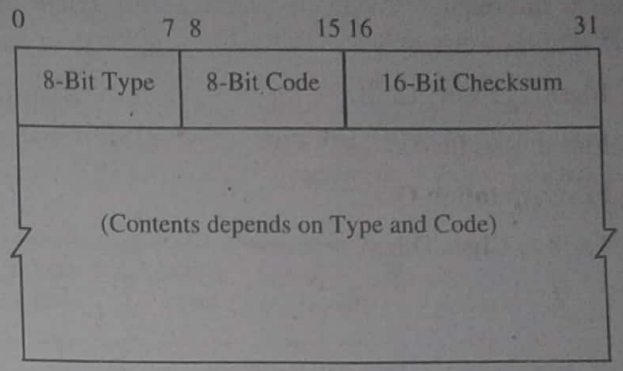


Figure 5.2: ICMP Message

There are 15 different values for the type field, which identify the particular ICMP message. Some types of ICMP messages then use different values of the code field to further specify the condition.

The checksum field covers the entire ICMP message. The ICMP checksum is required.

Ques 3) Discuss how error reporting happens in ICMP?

Ans: Error Reporting

ICMP always reports error messages to the original source. Five types of errors are handled (**figure 5.3**):

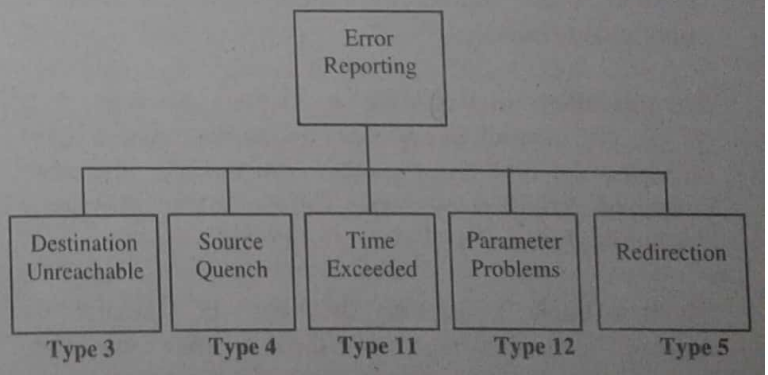


Figure 5.3: Error Reporting Messages

The following are important points about ICMP error messages:

1) No ICMP error message will be generated in response to a datagram carrying an ICMP error message.
2) No ICMP error message will be generated for a fragmented datagram that is not the first fragment.

3) No ICMP error message will be generated for a datagram having a multicast address.
4) 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.

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. The original datagram header is added to give the original source, which receives the error message, information about the datagram itself.

The 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 (**figure 5.4**).

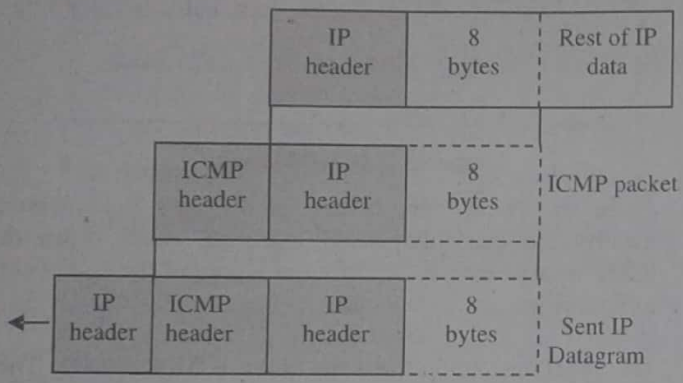


Figure 5.4: Contents of Data Field for the Error Messages

Ques 4) Explain about the ICMP timestamp request and reply?

Ans: ICMP Timestamp Request and Reply
The ICMP timestamp request allows a system to query another for the current time. The recommended value to be returned is the number of milliseconds since midnight coordinated Universal Time.

The **advantage** of this ICMP message is that it provides millisecond resolution, whereas some other methods for obtaining the time from another host (such as the rdate command provided by some Unix systems) provide a resolution of seconds.

The **drawback** is that only the time since midnight is returned – the caller must know the date from some other means.

Figure 5.5 shows the format of the ICMP timestamp request and reply messages:

The requestor fills in the originate timestamp and sends the request. The replying system fills in the receive timestamp when it receives the request, and the transmit timestamp when it sends the reply.

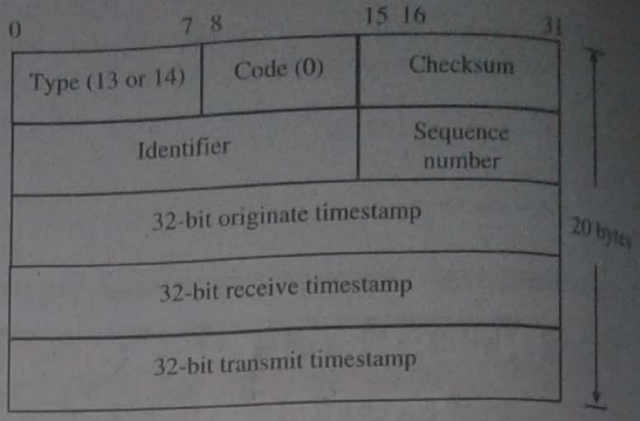


Figure 5.5: ICMP Timestamp Request and Reply Messages

In actuality, however, most implementations set the latter two fields to the same value. (The reason for providing the three fields is to let the sender compute the time for the request to be sent and separately compute the time for the reply to be sent).

Ques 5) What is Address Resolution Protocol (ARP)? Explain its working.

Ans: Address Resolution Protocol (ARP)
ARP is used to find the physical address of the node when its Internet address is known. Anytime a host, or a router needs to find the physical address of another host on its network, it formats an ARP query packet that includes the IP address and broadcasts in over the network.

Every host on the network receives and processes the ARP packet, but only the intended recipient recognizes its internet address and sends back its physical address.

The host holding the datagram adds the address of the target host both to its cache memory and to the datagram header, then sends the datagram on its way.

ARP is a low level protocol that uses the services of the MAC (Data Link) Layer, and as with all protocols, is then encapsulated in a physical network frame.

In this case the Source Address field of the physical frame will indicate the station that is requesting the address resolution, while the Destination Address field will contain the broadcast address. Where a Type field is present, this will contain a code to indicate the ARP protocol, so that receiving stations will be able to correctly process the frame. **For example,** in the case of Ethernet, the Type field will contain 0x0806.

Working of Address Resolution Protocol (ARP)
Step 1: When a source device want to communicate with another device, source device checks its Address Resolution Protocol (ARP) cache to find if already has a resolved MAC address of the destination device.

If it is there, it will use that address for communication. To view your Local Address

Resolution Protocol (ARP) cache, Open Command Prompt and type command "arp a" (Without double quotes using Windows Operating Systems).

Step 2: If ARP resolution is not there in local cache, the source machine will generate an Address Resolution Protocol (ARP) request message, it puts its own data link layer address as the Sender Hardware Address and its own IP address as the Sender Protocol Address.

It fills the destination IP address as the Target Protocol Address. The Target Hardware Address will be left blank, since the machine is trying to find that.

Step 3: The source broadcast the Address Resolution Protocol (ARP) request message to the local network.

Step 4: The message is received by each device on the LAN since it is a broadcast. Each device compare the Target Protocol Address (IP Address of the machine to which the source is trying to communicate) with its own Protocol Address (IP Address). Those who do not match will drop the packet without any action.

Step 5: When the targeted device checks the Target Protocol Address, it will find a match and will generate an Address Resolution Protocol (ARP) reply message.

It takes the Sender Hardware Address and the Sender Protocol Address fields from the Address Resolution Protocol (ARP) request message and uses these values for the Targeted Hardware Address and Targeted Protocol Address of the reply message.

Step 6: The destination device will update its Address Resolution Protocol (ARP) cache, since it need to contact the sender machine soon.

Step 7: Destination device send the Address Resolution Protocol (ARP) reply message and it will not be a broadcast, but a unicast.

Step 8: The source machine will process the Address Resolution Protocol (ARP) reply from destination, it store the Sender Hardware Address as the layer 2 address of the destination.

Step 9: The source machine will update its Address Resolution Protocol (ARP) cache with the Sender Hardware Address and Sender Protocol Address it received from the Address Resolution Protocol (ARP) reply message.

Ques 6) What do you understand by Gratuitous and proxy ARP?

Ans: Gratuitous ARP
Gratuitous ARP is used when a node (end system) has selected an IP address and then wishes to defend its chosen address on the local area network (i.e. to check no other node is using the same IP address).
It can also be used to force a common view of the node's IP address (e.g. after the IP address has changed). Use of this is common when an interface is first configured, as the node attempts to clear out any stale caches that might be present on other hosts. The node simply sends an ARP request for itself.

Proxy ARP
Proxy ARP is the name given when a node responds to an ARP request on behalf of another node. This is commonly used to redirect traffic sent to one IP address to another system.

Proxy ARP can also be used to subvert traffic away from the intended recipient. By responding instead of the intended recipient, a node can pretend to be a different node in a network, and therefore force traffic directed to the node to be redirected to itself.

The node can then view the traffic (e.g. before forwarding this to the originally intended node) or could modify the traffic. Improper use of Proxy ARP is therefore significant security vulnerability and some networks therefore implement systems to detect this. Gratuitous ARP can also help defend the correct IP to MAC bindings.

Ques 7) Define Reverse Address Resolution Protocol (RARP)?

Ans: Reverse Address Resolution Protocol (RARP)
RARP works much like ARP. The host wishing to retrieve its internet address broadcasts an RARP query packet that contains its physical address to every host on its physical network.

A server on the network recognizes the RARP packet and returns the host's internet address.
The TCP/IP protocol that allows a computer to obtain its IP address from a server is known as the Reverse Address Resolution Protocol (RARP).

RARP is adapted from the ARP protocol and uses the same message format. Like an ARP message, a RARP message is sent from one machine to another encapsulated in the data portion of a network frame.

For example, an Ethernet frame carrying a RARP request has the usual preamble, Ethernet source and destination addresses, and packet type fields in front of the frame. The frame type contains the value 8035 to identify the contents of the frame as a RARP message. The data portion of the frame contains the 28-octet RARP message.

Figure 5.6 shows how a host uses RARP. The sender broadcasts a RARP request that specifies itself as both the sender and target machine, and supplies its physical network address in the target hardware address field. All computers on the network receive the request, but only those authorized to supply the RARP service process the request and send a reply; such computers are known

informally as RARP servers. For RARP to succeed, the network must contain atleast one RARP server:

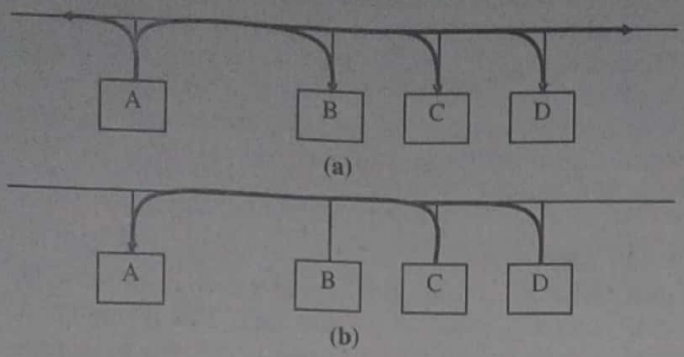


Figure 5.6: Example Exchange using the RARP Protocol, (a) Machine A Broadcasts a RARP Request specifying itself as a Target, and (b) Those Machines Authorized to Supply the RARP Service (C and D) Reply Directly to A.

Servers answer requests by filling in the target protocol address field, changing the message type from request to reply, and sending the reply back directly to the machine making the request. The original machine receives replies from all RARP servers, even though only the first is needed.

Ques 8) Write short note on BOOTP.

Ans: BOOT Strap Protocol

To overcome some of the drawbacks of RARP, researchers developed the BOOT strap Protocol (BOOTP). Later, the Dynamic Host Configuration Protocol (DHCP) was developed as a successor to BOOTP. Because the two protocols are closely related.

Because it uses UDP and IP, BOOTP can be implemented with an application program. Like RARP, BOOTP operates in the client-server paradigm and requires only a single packet exchange.

However, BOOTP is more efficient than RARP because a single BOOTP message specifies many items needed at start-up, including a computer's IP address, the address of a router, and the address of a server.

BOOTP also includes a vendor-specific field in the reply that allows hardware vendors to send additional information used only for their computers.

BOOTP places all responsibility for reliable communication on the client. Because UDP uses IP for delivery, messages can be delayed, lost, delivered out of order, or duplicated. Furthermore, because IP does not provide a checksum for data, the UDP datagram could arrive with some bits corrupted.

To guard against corruption, BOOTP requires that UDP use checksums. It also specifies that requests and replies should be sent with the do not fragment bit set to accommodate clients that have too little memory to re-assemble datagrams. BOOTP is also constructed to allow multiple replies; it accepts and processes the first.

To handle datagram loss, BOOTP uses the conventional technique of timeout and re-transmission. When the client transmits a request, it starts a timer.

If no reply arrives before the timer expires, the client must re-transmit the request. Of course, after a power failure all machines on a network will re-boot simultaneously, possibly over-running the BOOTP server(s) with requests.

If all clients use exactly the same re-transmission timeout, many or all of them will attempt to re-transmit simultaneously. To avoid the resulting collisions, the BOOTP specification recommends using a random delay.

In addition, the specification recommends starting with a random timeout value between 0 and 4 seconds, and doubling the timer after each re-transmission.

After the timer reaches a large value, 60 seconds, the client does not increase the timer, but continues to use randomization. Doubling the timeout after each re-transmission keeps BOOTP from adding excessive traffic to a congested network; the randomization helps avoid simultaneous transmissions.

Ques 9) What is Internet multicasting? What are the applications of multicasting?

Ans: Multicasting

In multicast communication, there is one source and a group of destinations. The relationship is one-to-many. In this type of communication, the source address is a unicast address, but the destination address is a group address, which defines one or more destinations. The group address identifies the members of the group.

A multicast packet starts from the source S1 and goes to all destinations that belong to group G1.

In multicasting, when a router receives a packet, it may forward it through several of its interfaces.

In multicasting, the router may forward the received packet through several of its interfaces.

Applications of Multicasting

1) **Access to Distributed Databases:** Most of the large databases today are distributed. That is, the information is stored in more than one location, usually at the time of production.

   The user who needs to access the database does not know the location of the information.

   A user's request is multicast to all the database locations, and the location that has the information responds.

2) **Information Dissemination:** Businesses often need to send information to their customers. If the nature of the information is the same for each customer, it can be multicast.

In this way a business can send one message that can reach many customers. **For example,** a software update can be sent to all purchasers of a particular software package.

3) **Dissemination of News:** In a similar manner news can be easily disseminated through multicasting. One single message can be sent to those interested in a particular topic.

For example, the statistics of the championship high school basketball tournament can be sent to the sports editors of many newspapers.

4) **Teleconferencing:** Teleconferencing involves multicasting. The individuals attending a teleconference all need to receive the same information at the same time. Temporary or permanent groups can be formed for this purpose.

5) **Distance Learning:** One growing area in the use of multicasting is distance learning. Lessons taught by one single professor can be received by a specific group of students.

This is especially convenient for those students who find it difficult to attend classes on campus.

Ques 10) Explain IGMP in detail.

Ans: Internet Group Message Protocol (IGMP)

Internet Group Management Protocol (IGMP), which is used by hosts and routers that support **multicasting**. It lets all the systems on a physical network know which hosts currently belong to which multicast groups.

This information is required by the multicast routers, so they know which multicast datagrams to forward onto which interfaces.

Like ICMP, IGMP is considered part of the IP layer. Also like ICMP, IGMP messages are transmitted in IP datagrams. Unlike other protocols, IGMP has a fixed-size message, with no optional data.

Figure 5.7 shows the encapsulation of an IGMP message within an IP datagram.

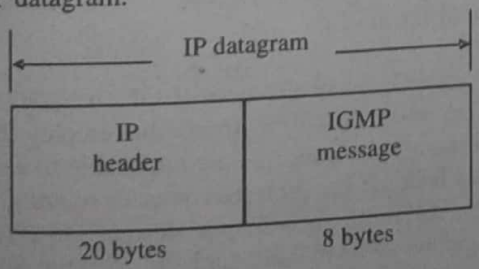


Figure 5.7 Encapsulation of an IGMP Message within an IP Datagram

IGMP Message

Figure 5.8: shows the format of the 8-byte IGMP message:

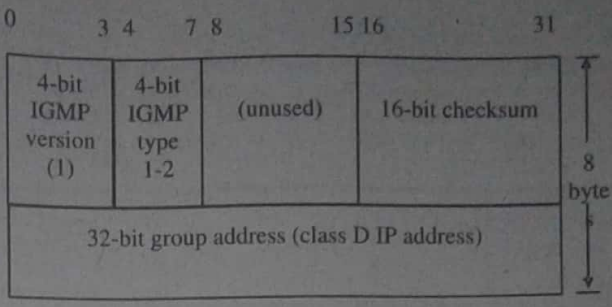


Figure 5.8: Format of Fields in IGMP Message

The IGMP version is 1. An IGMP type of 1 is a query sent by a multicast router, and 2 is a response sent by a host. The checksum is calculated in the same manner as the ICMP checksum.

The group address is a class D IP address. In a query the group address is set to 0, and in a report it contains the group address being reported.

IGMP Reports and Queries

IGMP messages are used by multicast routers to keep track of group membership on each of the router's physically attached networks. The following rules apply:

1) A host sends an IGMP report when the first process joins a group. If multiple processes on a given host join the same group, only one report is sent, the first time a process joins that group. This report is sent-out the same interface on which the process joined the group.

2) A host does not send a report when processes leave a group, even when the last process leaves a group.

   The host knows that there are no members in a given group, so when it receives the next query (next step), it would not report the group.

3) A multicast router sends an IGMP query at regular intervals to see if any hosts still have processes belonging to any groups. The router must send one query out each interface. The group address in the query is 0 since the router expects one response from a host for every group that contains one or more members on that host.

4) A host responds to an IGMP query by sending one IGMP report for each group that still contains atleast one process.

Using these queries and reports, a multicast router keeps a table of which of its interfaces have one or more hosts in a multicast group.

When the router receives a multicast datagram to forward, it forwards the datagram (using the corresponding multicast link-layer address) only out the interfaces that still have hosts with processes belonging to that group.

Figure 5.9 shows these two IGMP messages, reports sent by hosts, and queries sent by routers. The router is asking each host to identify each group on that interface:

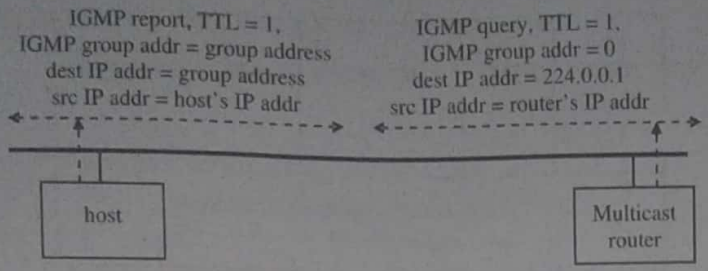


Figure 5.9: IGMP Reports and Queries

In **figure 5.9** TTL field of the reports and queries is set to 1. This refers to the normal TTL field in the IP header. A multicast datagram with an initial TTL of 0 is restricted to the same host. By default, multicast datagrams are sent with a TTL of 1. This restricts the datagram to the same subnet. Higher TTLs can be forwarded by multicast routers.

An ICMP error is never generated in response to a datagram destined to a multicast address. Multicast routers do not generate ICMP "time exceeded" errors when the TTL reaches 0.

Normally user processes are not concerned with the outgoing TTL. One exception, however, is the **Traceroute** program, which is based on setting the TTL field. Since multicasting applications must be able to set the outgoing TTL field, this implies that the programming interface must provide this capability to user processes.

By increasing the TTL an application can perform an expanding ring search for a particular server. The first multicast datagram is sent with a TTL of 1. If no response is received, a TTL of 2 is tried, then 3, and so on. In this way the application locates the closest server, in terms of hops.

The special range of addresses 224.0.0.0 through 224.0.0.255 is intended for applications that never need to multicast further than one hop. A multicast router should never forward a datagram with one of these addresses as the destination, regardless of the TTL.

In **figure 5.9** we also indicated that the router's IGMP query is sent to the destination IP address of 224.0.0.1. This is called the **all-hosts group address**.

It refers to all the multicast-capable hosts and routers on a physical network. Each host automatically joins this multicast group on all multicast-capable interfaces, when the interface is initialized. Membership in this group is never reported.

Ques 11) What is interior and exterior routing protocol?

Ans: Interior Routing Protocol
Interior routing protocol designed for networks that are controlled by an organization. Design criteria for interior routing protocols to find the best path on the network.

The computers within each autonomous system know about the other computers in that system and usually exchange routing information because the number of computers is kept manageable.

If an autonomous systems grows too large, it can be split into smaller parts. The routing protocols used inside an autonomous system are called interior routing protocols.

The routing protocols such as RIP and OSPF, are considered interior routing protocols.

Exterior Routing Protocol
Protocols used between autonomous systems are called exterior routing protocols. Although interior routing protocols are usually designed to provide detailed routing information about all or most computers inside the autonomous systems, exterior protocols are designed to be more careful in the information they provide.

Usually, exterior protocols provide information about only the preferred or the best routes rather than all possible routes.

Border Gateway Protocol (BGP) is the most common exterior routing protocol in use today.

Ques 12) What is BGP? What are the main characteristics of BGP? Also discuss its type.

Ans: Border Gateway Protocol (BGP)
BGP is a complex, advanced distance Exterior Gateway Protocol (EGP), BGP exchange routing information between **Autonomous Systems** (ASs).

BGP is especially used for exchanging routing information between all of the major Internet Service Providers (ISPs), as well between larger client sites and their respective ISPs. And, in some large enterprise networks, BGP is used to interconnect different geographical or administrative regions.

Some of the primary attributes of BGP is the use of pieces of information about a known route, where it came from, and how to reach it, A BGP router will also generate an error message if it receives a route that is missing these are mandatory attributes.

The Border Gateway Protocol (BGP) was developed for use in conjunction with internets that employ the TCP/IP suite, although the concepts are applicable to any internet. BGP has become the preferred exterior router protocol for the internet. Functions BGP was designed to allow routers, called gateways in the standard, in different Autonomous Systems (ASs) to cooperate in the exchange of routing information. The protocol operates in terms of messages, which are sent over TCP connections.

BGP is primarily used to support the complexity of the public Internet; **Cisco** has added several clever and useful features to its BGP implementation (**BGP 4**).

Characteristics of BGP

1) It is an advanced distance-vector protocol.
2) BGP sends full routing updates at the start of the session, trigger updates are sent afterward.
3) BGP maintains connection by sending periodic keepalives.
4) It creates and maintains connections between peers, using TCP port 179.
5) BGP sends a triggered update when a keepalive, an update, or a notification is not received.
6) It has its own routing table, although it is capable of both sharing and inquiring of the interior IP routing table.
7) BGP uses a very complex metric, and is the source of its strength. The metric, referred to as attributes, allows great flexibility in path selection.

Types of BGP

There are two types of BGP:

1) **iBGP:** Internal BGP (iBGP) operates inside an autonomous System (AS).
2) **eBGP:** External BGP (eBGP) is also known as an interdomain routing protocol, operates outside an AS and connects one AS to another. These terms are just used to describe the same protocol just the area of operation is what differs.

Ques 13) Discuss about the BGP message format.

Or

Explain the following:

1) **Open Messages and Update Messages**
2) **Keepalive Messages and Notification Messages**

Ans: BGP Messages

Figure 5.10 illustrates the formats of all of the BGP messages. Each message begins with a 19-octet **header containing** three fields (shaded area):

1) **Marker:** Reserved for authentication. The sender may insert a value in this field that would be used as part of an authentication mechanism to enable the recipient to verify the identity of the sender.
2) **Length:** Length of message in octets.
3) **Type:** Type of message – Open, Update, Notification, Keepalive.

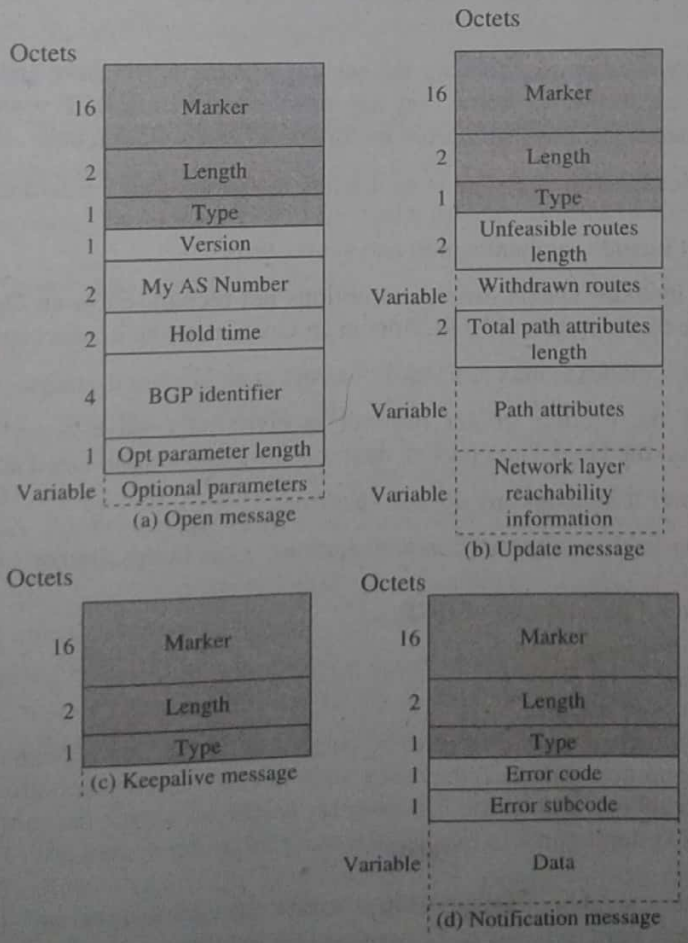


Figure 5.10: BGP Message Formats

The four types of messages are as below:

1) **Open Messages:** After a TCP connection is established between two BGP systems, they exchange BGP open messages to create a BGP connection between them. Once the connection is established, the two systems can exchange BGP messages and data traffic. Open messages consist of the BGP header plus the following fields:
   i) **Version:** The current BGP version number is 4.
   ii) **My AS Number:** BGP open message's AS number field contains 16-bits that contains the AS number of the BGP routing instance that transmitted the open message.
   iii) **Hold Time:** Proposed hold-time value.
   iv) **BGP Identifier:** IP address of the BGP system. This indicates the ID of the sender of the BGP open message and is equal to the IP address that is assigned to the device.
   v) **Optional Parameters Length:** The BGP open message's optional parameters length is an 8-bit field that indicates the number of bytes in the optional parameters section of the BGP open message.
   vi) **Optional Parameters:** The BGP open message's optional parameters contain all optional parameters for BGP sessions.
2) **Update Messages:** BGP systems send update messages to exchange network reachability information. BGP systems use this information to construct a graph that describes the relationships among all known ASs. Update messages consist of the BGP header plus the following optional fields:
   i) **Unfeasible Routes Length:** Length of the withdrawn routes field.
   ii) **Withdrawn Routes:** IP address prefixes for the routes being withdrawn from service because they are no longer deemed reachable.
   iii) **Total Path Attribute Length:** Length of the path attributes field; it lists the path attributes for a feasible route to a destination.
   iv) **Path Attributes:** Properties of the routes, including the path origin, the multiple exit discriminator (MED), the originating system's preference for the route, and information about aggregation, communities, confederations, and route reflection.
   v) **Network Layer Reachability Information (NLRI):** IP address prefixes of feasible routes being advertised in the update message.
3) **Keepalive Messages:** This is the packet used to keep the session running when there are no updates. Keepalives are sent between BGP speakers to let each other know they are still there. When a BGP router fails to hear a Keepalive message, it removes all routes heard from that peer from its forwarding information base (FIB).
4) **Notification Messages:** The Notification Message is sent when an error condition is detected. The following errors may be reported:
   i) **Message Header Error:** It includes authentication and syntax errors.
   ii) **Open Message Error:** It includes syntax errors and options not recognised in an Open message. This message can also be used to indicate that a proposed Hold Time in an Open message is unacceptable.
   iii) **Update Message Error:** It includes syntax and validity errors in an Update message.
   iv) **Hold Timer Expired:** If the sending router has not received successive Keepalive and/or Update and/or Notification messages within the Hold Time period, then this error is communicated and the connection is closed.
   v) **Finite State Machine Error:** It includes any procedural error.
   vi) **Cease:** It is used by a router to close a connection with another router in the absence of any other error.

Ques 14) Discuss about the functional procedures of BGP.

Ans: Functional Procedures of BGP

Three functional procedures are involved in BGP:

1) **Neighbour Acquisition:** Two routers are considered to be neighbours if they are attached to the same network. If the two routers are in different autonomous systems, they may wish to exchange routing information. For this purpose, it is necessary first to perform neighbour acquisition. In essence, neighbour acquisition occurs when two neighbouring routers in different autonomous systems agree to exchange routing information regularly.
2) **Neighbour Reachability:** Once a neighbour relationship is established, the neighbour reachability procedure is used to maintain the relationship. Each partner needs to be assured that the other partner still exists and is still engaged in the neighbour relationship. For this purpose, the two routers periodically issue Keepalive messages to each other.

3) **Network Reachability:** The final procedure specified by BGP is network reachability. Each router maintains a database of the networks that it can reach and the preferred route for reaching each network.

When a change is made to this database, the router issues an Update message that is broadcast to all other routers implementing BGP. Because the Update message is broadcast, all BGP routers can build up and maintain their routing information.

Ques 15) What is IPv6 addressing? Give the structure of IPv6 Packet?

Ans: IPv6 (Internet Protocol Version 6) Addressing

IPv6 is backward compatible with and is designed to fix the shortcomings of IPv4, such as data security and maximum number of user addresses. This is the next generation IP protocol. IPv6 increases the address space from 32 to 128 bits, providing for an unlimited (for all intents and purposes) number of networks and systems.

This increased size provides for a broader range of addressing hierarchies and a much larger number of addressable nodes.

IPv6 is a network layer standard used by electronic devices to exchange data across a packet-switched internetwork. It follows IPv4 as the second version of the Internet Protocol to be formally adopted for general use.

Structure of IPv6

An IPv6 packet (**figure 5.11**) has the following general form:

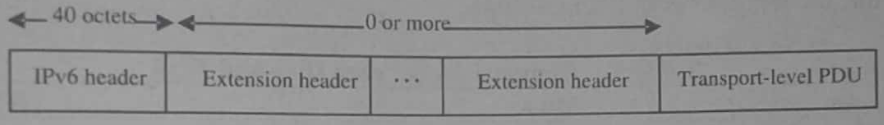


Figure 5.11: IPv6 Structure

The only header that is required is referred to simply as the IPv6 header. This is of fixed size with a length of 40 octets, compared to 20 octets for the mandatory portion of the IPv4 header. The following extension headers have been defined:

1) **Hop-by-Hop Options Header:** Defines special options that require hop-by-hop processing.
2) **Routing Header:** Provides extended routing, similar to IPv4 source routing.
3) **Fragment Header:** Contains fragmentation and reassembly information.
4) **Authentication Header:** Provides packet integrity and authentication.
5) **Encapsulating Security Pay-load Header:** Provides privacy.
6) **Destination Options Header:** Contains optional information to be examined by the destination node.

Ques 16) What are the different issues related to IPv6?

Ans: Issues Related to IPv6

The issues related to IPv6 network security are as follows:

1) **Lack of IPv6 Security Training/Education:** The biggest risk today is the lack of IPv6 security knowledge. Enterprises must invest time and money in IPv6 security training upfront, before deploying. Network security is more effective as part of the planning stage rather than after deployment.
2) **Security Device Bypass via Unfiltered IPv6 and Tunnelled Traffic:** Only a lack of knowledge is considered a bigger risk than the security products themselves. Conceptually it's simple, security products need to do two things – recognize suspicious IPv6 packets and apply controls when they do. However in practice this is hardly possible in IPv4 let alone an environment that may have rogue or unknown tunnel traffic.
3) **Lack of IPv6 Support at ISPs and Vendors:** Thorough testing is critical until IPv6 security functionality and stability are on par with that of IPv4. A test network and a test plan for all protocols involved must be devised to test all equipment – especially new security tech from vendors. Every network is unique and requires a unique test plan.

   Further complicating the issue is not having a native IPv6 connection from provider. A tunnel connected to interface further increases security complexity and provides an opening for man-in-the-middle and denial-of-service attacks.
4) **Congruence of Security Policies in IPv4 & IPv6:** Weak IPv6 security policies are a direct result of the current deficit in IPv6 security knowledge. Not only do the depth of the IPv6 security policies need to be equal to that of their IPv4 counterparts but their breadth must be wider to encompass new vulnerabilities that didn't need to be considered in an IPv4 homogeneous environment.

Ques 17) What are the advantages of IPv6 over IPv4?

Ans: Advantage of IPv6 over IPv4

1) **Larger Address Space:** Address filed in IPv6 is 128 bits long while the address filed of IPv4 is only 32 bits in length. IPv6 offers very large, i.e., 296 address space as compared to IPv4.
2) **Better Header Format:** The header of IPv6 has been designed in a way to speed-up the routing process. In header of IPv6 options are separated from the base header. Options are inserted into base header only when required by the upper-layer data.
3) **Provision for Extension:** IPv6 has been designed in a way that a protocol can be extended easily to meet the requirements of emerging technologies or new applications.
4) **Resource Allocation Support in IPv6:** IPv6 provides a mechanism called Flow Label for resource allocation. Flow label enables source to send request for the special handling of a packet. This mechanism is really helpful in real-time audio and video transmission.
5) **Security Features:** To ensure confidentiality and packet's integrity encryption and authentication options are included in IPv6.

Ques 18) What is difference between IPv6 and IPv4?

Ans: Difference between IPv6 & IPv4

Table below shows the difference between IPv6 and IPv4:

Table 5.1: Comparison between IPv6 and IPv4

Description	IPv4	IPv6
Address	32 bits long (4 bytes). The text form of the IPv4 address is nnn.nnn.nnn.nnn, where 0<=nnn<=255, and each n is a decimal digit.	128 bits long (16 bytes). The text form of the IPv6 address is xxxx:xxxx:xxxx:xxxx: xxxx:xxxx:xxxx:xxxx, where each x is a hexadecimal digit representing 4 bits.
Address Allocation	Originally, addresses were allocated by network class.	Allocation is in the earliest stages.
Address Lifetime	Generally, not an applicable concept.	IPv6 addresses have two lifetimes: preferred and valid, with the preferred lifetime always <= valid.
Address Mask	Used to designate network from host portion.	Not used
Address Types	Unicast, multicast, and broadcast.	Unicast, multicast, and anycast.
Domain Name System (DNS)	Applications accept host names and then use DNS to get an IP address, using socket API	Same for IPv6.
File Transfer Protocol (FTP)	File Transfer Protocol allows you to send and receive files across networks.	Some implementations of FTP does not support IPv6.
Fragments	When a packet is too big for the next link over which it is to travel, it can be fragmented by the sender (host or router).	For IPv6, fragmentation can only occur at the source node, and reassembly is only done at the destination node. The fragmentation extension header is used.
Interface	The conceptual or logical entity used by TCP/IP to send and receive packets and always closely associated with an IPv4 address, if not named with an IPv4 address. Sometimes referred to as a logical interface.	Same concept as IPv4.
IP Header	Variable length of 20-60 bytes, depending on IP options present.	Fixed length of 40 bytes. There are no IP header options. Generally, the IPv6 header is simpler than the IPv4 header.
IP Header Options	Various options that might accompany an IP header (before any transport header).	The IPv6 header has no options. Instead, IPv6 adds additional (optional) extension headers. The extension headers are AH and ESP (unchanged from IPv4), hop-by-hop, routing, fragment, and destination. Currently, IPv6 supports some extension headers.

LAN Connection	Used by an IP interface to get to the physical network. Many types exist; **for example,** token ring, and Ethernet. Sometimes referred to as the physical interface, link, or line.	IPv6 can be used with any Ethernet adapters and is also supported over virtual Ethernet between logical partitions.
Packet Filtering	Basic firewall functions integrated into TCP/IP, configured using iSeries Navigator.	You cannot use packet filtering with IPv6.
Route	Logically, a mapping of a set of IP addresses (might contain only one) to a physical interface and a single next-hop IP address. IP packets whose destination address is defined as part of the set are forwarded to the next hop using the line. IPv4 routes are associated with an IPv4 interface, hence, an IPv4 address.	Conceptually, similar to IPv4. One important difference: IPv6 routes are associated (bound) to a physical interface rather than an interface. One reason that a route is associated with a physical interface is because source address selection functions differently for IPv6 than for IPv4.

Ques 19) Write short note on ICMPv6.

Or

What are the main functions of ICMPv6?

Ans: ICMPv6

Internet Control Message Protocol (both ICMPv4 and ICMPv6) is a protocol which acts as a communication messenger protocol between the communicating devices in IP network. ICMP messages provide feedback, error reporting and network diagnostic functions in IP networks which are necessary for the smooth operation of IPv6.

The Internet Control Message Protocol Version 6 (ICMPv6) is a new version of the ICMP that forms an integral part of the Internet Protocol version 6 (IPv6) architecture. ICMPv6 messages are transported within an IPv6 packet that may include IPv6 extension headers.

ICMPv6 is an integral part of IPv6 and ICMPv6 protocol in IPv6 and has much more importance and functions than ICMPv4 protocol in IPv4.

Functions of ICMPv6

Main functions of ICMPv6 are as follows:

1) Error Reporting
2) Network Diagnostics
3) Neighbor Discovery
4) Multicast Membership Reporting
5) Router Solicitation and Router Advertisements

ICMPv6 removed the ICMPv4 functions that are obsolete and took over the functions of two major IPv4 protocols IGMP (Internet Group Membership Protocol) and ARP (Address Resolution Protocol). IGMP and ARP are no more with IPv6.

Ques 20) What is the packet format of ICMPv6? Also discuss the message types of ICMPv6.

Ans: Packets Format

ICMPv6 packets have the format shown in the **figure below**:

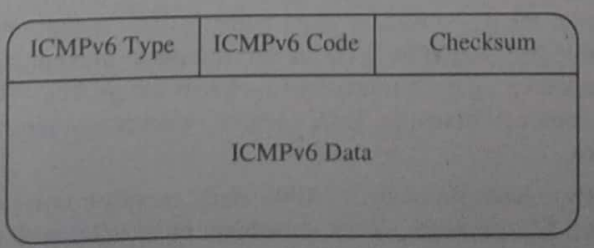


Figure 5.12: ICMPv6 Packet

The 8-bit Type field indicates the type of the message. If the high-order bit has value zero (values in the range from 0 to 127), it indicates an error message; if the high-order bit has value 1 (values in the range from 128 to 255), it indicates an information message. The 8-bit Code field content depends on the message type.

Checksum field helps in the detection of errors in the ICMP message and in part of the IPv6 message.

ICMPv6 Message Types

ICMPv6 is a multipurpose protocol as it is used for a plethora of activities such as reporting errors encountered in processing data packets, reporting multicast memberships, performing Neighbor Discovery, and performing diagnostics. An ICMP message is identified by a value of 58 in the Next Header field of the IPv6 header or of the preceding Header. A list of currently defined message types is shown in the **table below**:

Table 5.2: ICMPv6 Message Types

Type	Meaning
1	Destination Unreachable
2	Packet Too Big
3	Time Exceeded
4	Parameter Problem
128	Echo Request
129	Echo Reply
130	Group Membership Query
131	Group Membership Report
132	Group Membership Reduction
133	Router Solicitation
134	Router Advertisement
135	Neighbor Solicitation
136	Neighbor Advertisement
137	Redirect
138	Router Renumbering

Ques 21) Describe the ICMPv6 message.

Or

Explain the error and Information message of ICMPv6.

Ans: ICMPv6 Messages

ICMPv6 is a multipurpose protocol and is used for a variety of activities including error reporting in packet processing, diagnostic activities, Neighbor Discovery process and IPv6 multicast membership reporting. To perform these activities, ICMPv6 messages are subdivided into two classes:

1) **Error Messages:** ICMPv6 error messages are used to report errors in the forwarding or delivery of IPv6 packets. The ICMPv6 "Type field" values for the error message are between 0 and 127.

   The Internet Control Message Protocol Version 6 (ICMPv6) error messages belong to four different categories:

   i) **Destination Unreachable:** Destination Unreachable ICMPv6 error message is generated by the source host or a router when an IPv6 datagram packet cannot be delivered for any reason other than congestion.

   ii) **Packet Too Big:** Packet Too Big ICMPv6 error messages are generated by the router when a packet cannot be forwarded to the next hop link because the size of the IPv6 datagram is larger than the MTU (Maximum Transmission Unit) of the link. Packet Too Big ICMPv6 error message includes the MTU of the next link also. MTU is the size of the largest protocol data unit that is supported over the link.

   iii) **Time Exceeded:** Similar to the Time-to-Live field value in IPv4 datagram header, IPv6 header includes a Hop Limit field. The Hop Limit field value in IPv6 header is used to prevent routing loops. Hop Limit field in IPv6 datagram header is decremented by each router that forwards the packet. When the Hop Limit field value in IPv6 header reaches zero, the router discards the IPv6 datagram packet and returns a "Time Exceeded" ICMPv6 error message to the source host.

   iv) **Parameter Problems:** Parameter Problem ICMPv6 error message is typically related with the problems and mistakes related with IPv6 header itself. When a problem or mistake with an IPv6 header make a router cannot process the packet, the router stops processing the IPv6 datagram packet, discards the packet and returns a "Parameter Problem" ICMPv6 error message to the source host.

2) **Information Messages:** ICMPv6 informational messages are used for network diagnostic functions and additional critical network functions like Neighbor Discovery, Router Solicitation & Router Advertisements, Multicast Memberships. Echo Request and Echo Reply are also ICMPv6 informational messages. ICMPv6 informational messages have values for the Type field (8 bit binary number) between 128 and 255.

Internet Control Message Protocol Version 6 (ICMPv6) information messages are subdivided into three groups:

i) **Diagnostic Messages:** ICMPv6 Echo request and Echo reply are the Diagnostic messages. Every IPv6 host must return an ICMPv6 Echo reply when it receives an ICMPv6 Echo request. Echo request and Echo reply messages are used by the ping command to check the network connectivity between two IPv6 hosts.

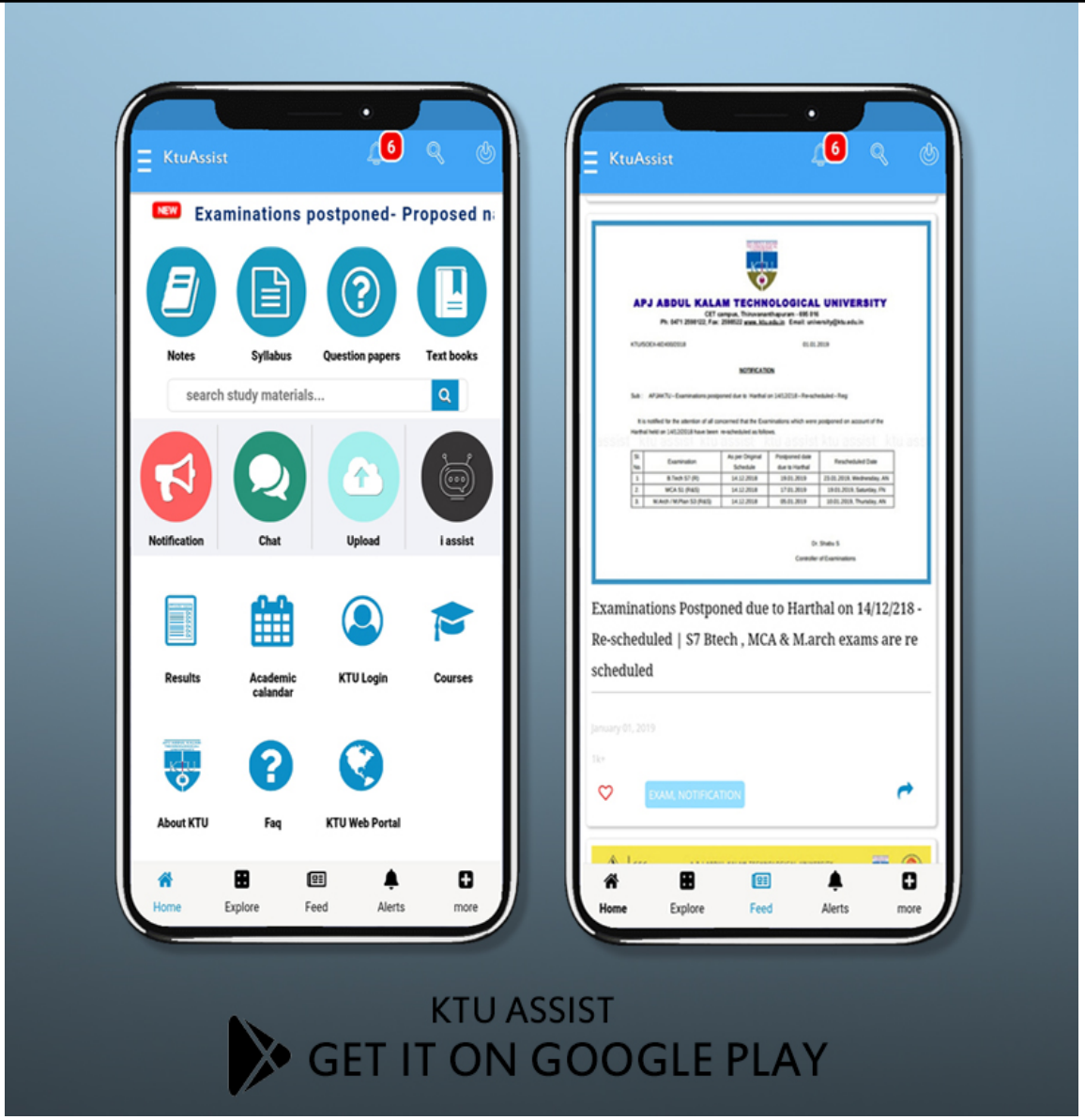
ii) **MLD (Multicast Listener Discovery) Messages:** ICMPv6 MLD Messages are used by an IPv6 enabled router to discover hosts who are interested in multicast packets, and the multicast addresses they are interested. MLD messages are used by MLD Protocol. MLD (Multicast Listener Discovery) Protocol is the IPv6 equivalent of IGMP (Internet Group Management) Protocol in IPv4.

iii) **ND (Neighbor Discovery) Messages:** ICMPv6 ND Messages are used for the Neighbor Discovery Protocol (NDP). ND Messages includes Router Solicitation & Router Advertisement, Neighbor Solicitation and Neighbor Advertisement.

Ques 22) What are the advantages of ICMPv6?

Ans: Advantages of ICMPv6

1) If a wrong IP address is used for configuring a client to the DNS server, an ICMP message is sent by the destination device to indicate the error.
2) If a program does not allow fragmentation of its communications but it is required to communicate with a destination device, the router undertaking the fragmentation of the packet sends an ICMP message to the source device to indicate the error.
3) If a client sends all communications to a particular router despite another router offering a best route, the particular router responds with the IP address of the router that provides a better route in the form of an ICMP message.
4) All IP headers contain a Time to Live (TTL) value. This value is decremented as the IP packet is forwarded through each router. If a packet arrives at a router with a Time To Live (TTL) value of 1, the router cannot decrement the value any further and forward it. Instead, the router discards the packet and sends an ICMP message to indicate the expiry of the packet's TTL value.
5) The Internet Control Message Protocol Version 6 (ICMPv6) also provides testing and diagnostics services for many utilities. In order to test the communication process, an ICMP echo is used by the Internet Protocol Packet Internet Gopher (PING) utility.



END

facebook.com/ktuassist

instagram.com/ktu_assist