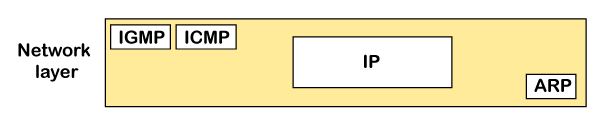
ICMP PROTOCOL

|  |  |
| --- | --- |
| Prepared by: | K Prashanth |
| Reviewed by: | Abhinab |

* **It stands for Internet Control Message Protocol.**
* **It is designed to overcome the problems in IP protocol, problems in IP protocol are:**

1. No error reporting.
2. Lacks the mechanism for query.

* It is also considered as a protocol of the Network layer.

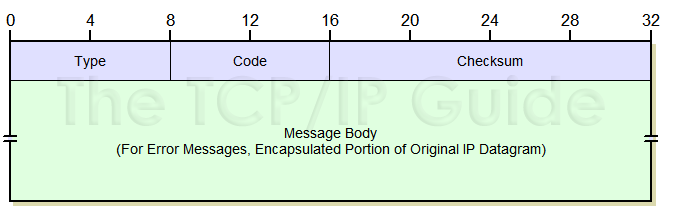


* It is a protocol used for error reporting and debugging in the network layer.
* ICMP is mainly used in network such as router or stations.
* A good example for ICMP is “PING”.
* PING stands for Packet internet or inter network groper.
* ICMP is divided into two types:

1. Error reporting messages.
2. Query messages.

* ICMP messages are not directly passed to the data link layer, instead the messages 1st encapsulated inside the IP datagrams before going to the lower layer.

**ICMP HEADER FORMAT**



* **Type:**

It is defined the type of message like error reporting or query.

* **Code:**

It is defined the sub type of the ICMP message, Reason for message.

* **Check sum:**

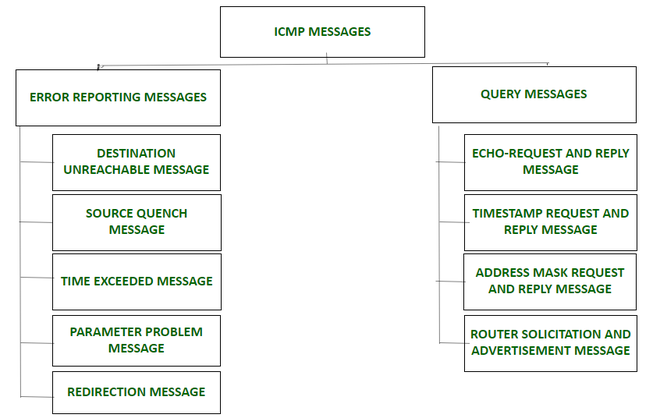
It is used for the error checking.

* **Message body:**

Contains specific fields used to implement each message type.

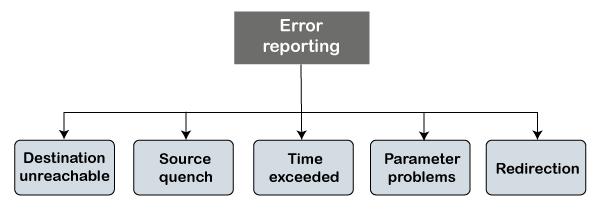
**TYPES OF ICMP MESSAGES**

* **Error reporting messages**
  + It is used to report problems that router or host may encounter while processing IP packets.
  + These messages are always reporting error message to the original source.
  + ICMP doesn’t correct errors.
* **Query messages**
* Fetch important messages & Specifies information from a router or host**.**

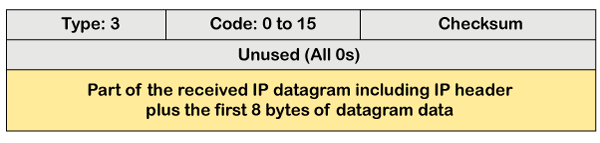


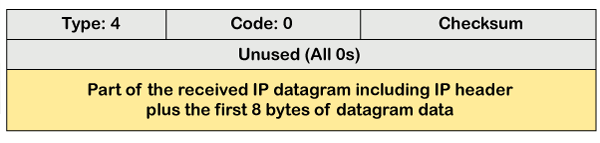
**Types of error reporting messages:**

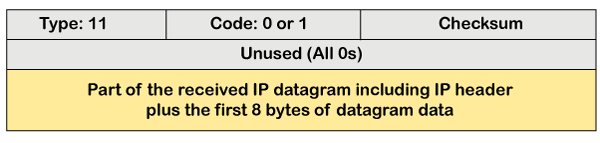
* The error reporting messages are broadly classified into the following categories:



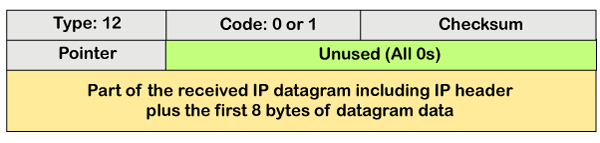
* **Destination unreachable:**
  + The destination unreachable error occurs when the packet does not reach the destination. Suppose the sender sends the message, but the message does not reach the destination, then the intermediate router reports to the sender that the destination is unreachable.



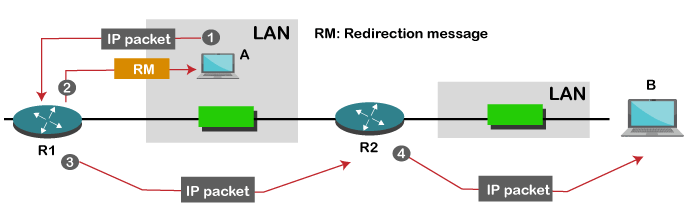
* The above diagram shows the message format of the destination unreachable message. In the message format
* Type: It defines the type of message. The number 3 specifies that the destination is unreachable.
* **Code (0 to 15):** It is a 4-bit number which identifies whether the message comes from some intermediate router or the destination itself.
* Sometimes the destination does not want to process the request, so it sends the destination unreachable message to the source. A router does not detect all the problems that prevent the delivery of a packet.
* **Source quench:**
* There is no flow control or congestion control mechanism in the network layer or the IP protocol. The sender is concerned with only sending the packets, and the sender does not think whether the receiver is ready to receive those packets or is there any congestion occurs in the network layer so that the sender can send a lesser number of packets, so there is no flow control or congestion control mechanism. In this case, ICMP provides feedback, i.e., source quench. Suppose the sender resends the packet at a higher rate, and the router is not able to handle the high data rate. To overcome such a situation, the router sends a source quench message to tell the sender to send the packet at a lower rate.
* 
* The above diagram shows the message format of the source quench message. It is a type 4 message, and code is zero.
* So, the sender must either stop or slow down the sending of datagrams until the congestion is reduced. The router sends one source-quench message for each datagram that is discarded due to the congestion in the network layer.
* **Time exceeded:**
* Sometimes the situation arises when there are many routers that exist between the sender and the receiver. When the sender sends the packet, then it moves in a routing loop. The time exceeded is based on the time-to-live value. When the packet traverses through the router, then each router decreases the value of TTL by one. Whenever a router decreases a datagram with a time-to-live value to zero, then the router discards a datagram and sends the time exceeded message to the original source.
* In the case of fragmentation, the code will be different as compared to TTL. Let's observe the message format of time exceeded.



* The above message format shows that the type of time-exceeded is 11, and the code can be either 0 or 1. The code 0 represents TTL, while code 1 represents fragmentation. In a time-exceeded message, the code 0 is used by the routers to show that the time-to-live value is reached to zero.
* The code 1 is used by the destination to show that all the fragments do not reach within a set time.
* **Parameter problems:**
  + The router and the destination host can send a parameter problem message. This message conveys that some parameters are not properly set.



* The above diagram shows the message format of the parameter problem. The type of message is 12, and the code can be 0.
* **Redirection**



* When the packet is sent, then the routing table is gradually augmented and updated. The tool used to achieve this is the redirection message. For example, A wants to send the packet to B, and there are two routers exist between A and B. First, A sends the data to the router 1. The router 1 sends the IP packet to router 2 and redirection message to A so that A can update its routing table.

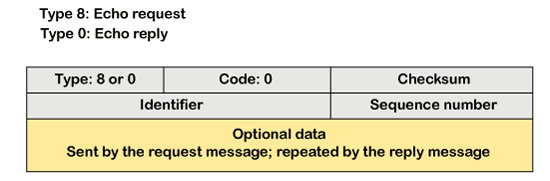
**ICMP Query Messages**

* The ICMP Query message is used for error handling or debugging the internet. This message is commonly used to ping a message.
* **Echo-request and echo-reply message:**
* A router or a host can send an echo-request message. It is used to ping a message to another host that "Are you alive". If the other host is alive, then it sends the echo-reply message. An echo-reply message is sent by the router or the host that receives an echo-request message.

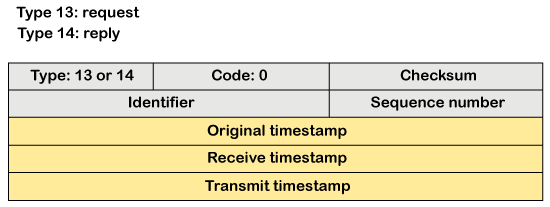
**Key points of Query messages**

1. The echo-request message and echo-reply message can be used by the network managers to check the operation of the IP protocol. Suppose two hosts, i.e., A and B, exist, and A wants to communicate with host B. The A host can communicate to host B if the link is not broken between A and B, and B is still alive.
2. The echo-request message and echo-reply message check the host's reachability, and it can be done by invoking the ping command.

The message format of echo-request and echo-reply message.



* The above diagram shows the message format of the echo-request and echo-reply message. The type of echo-request is 8, and the request of echo-reply is 0. The code of this message is 0.
* **Timestamp-request and timestamp-reply message:**
* The timestamp-request and timestamp-reply messages are also a type of query messages. Suppose the computer A wants to know the time on computer B, so it sends the timestamp-request message to computer B. The computer B responds with a timestamp-reply message.
* Message format of timestamp-request and timestamp-reply.



* The type of timestamp-request is 13, and the type of timestamp-reply is 14, The code of this type of message is 0.
* Key points related to timestamp-request and timestamp-reply message
* It can be used to calculate the round-trip time between the source and the destination, even if the clocks are not synchronized.
* It can also be used to synchronize the clocks in two different machines if the exact transit time is known.
* If the sender knows the exact transit time, then it can synchronize the clock. The sender asks the time on the receiver's clock, and then it adds the time and propagation delay. Suppose the time is 1:00 clock and propagation delay is 100ms , then time would be 1:00 clock plus 100ms.