ICMP - AN INTRODUCTION

Internet Control Message Protocol [ICMP] is companion to IP, designed to compensate these deficiencies

- ICMP is a network layer protocol
- Its messages are encapsulated inside IP datagrams before going to lower layer
- Ping and Traceroute uses ICMP messages,

ICMP Messages

1) Error Reporting Messages
2) Query Messages

1) Error Reporting
   - Destination unreachable
   - Source quench
   - Time exceeded
   - Parameters problems
   - Redirection

ICMP messages [Error reporting]

1. Destination unreachable

When the subnet or a router can not locate the destination

Or

When a packet with DF bit, can not be delivered because a 'small-packet' network stands in the way

2. Time exceeded

When a packet is dropped because its counter has reached zero. This event is a symptom that packets are looping enormous congestion or the time values are being set too low.

3. Parameter problem

Indicates that an illegal value has been detected in the header field
Indicates a bug in the sending host's IP software Or Possibly in the software of a router transited.

4. Source quench

To throttle hosts that send too many packets, When a host receives this message, it slows down sending packets

5. Redirect

Is used when a router notices that a packet seems to be routed wrong
It is used by the router to tell the sending host about the probable error.

2) Query Messages
   - Echo request and reply
   - Time-stamp request and reply
   - Address mask request and reply

1. ECHO & ECHO Reply

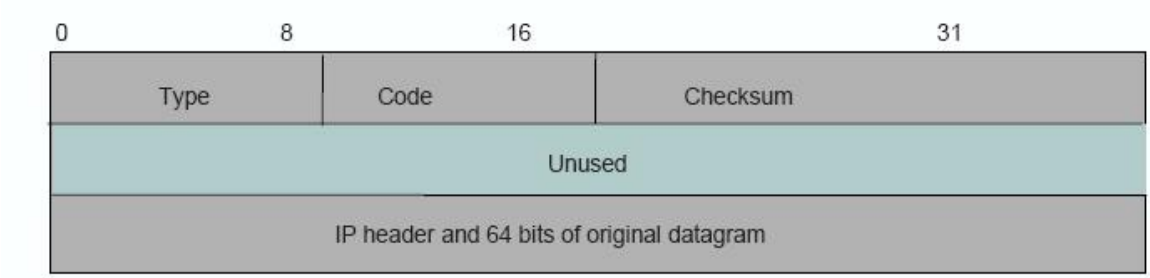
To see if a given destination is reachable and alive, upon receipt of ECHO message, the destination is expected to send an ECHO REPLY message back.

2. Time stamp & Time stamp reply

Similar to ECHO queries, except that the arrival time of the message and departure time of the reply are recorded in the reply.
This facility is used to measure network performance.

Message type	Description
Destination unreachable	Packet could not be delivered
Time exceeded	Time to live field hit 0
Parameter problem	Invalid header field
Source quench	Choke packet
Redirect	Teach a router about geography
Echo request	Ask a machine if it is alive
Echo reply	Yes, I am alive
Timestamp request	Same as Echo request, but with timestamp
Timestamp reply	Same as Echo reply, but with timestamp

ICMP Basic Error Message Format



Type of message: some examples
0 Network Unreachable; 3 Port Unreachable
1 Host Unreachable 4 Fragmentation needed
2 Protocol Unreachable 5 Source route failed
11 Time-exceeded,
code=0 if TTL exceeded
• Code: purpose of message
• IP header & 64 bits of original datagram
– To match ICMP message with original data in IP packet

Echo Request & Echo Reply Message Format

Echo request: type=8; Echo reply: type=0
– Destination replies with echo reply by copying data in request onto reply message
• Sequence number to match reply to request
• ID to distinguish between different sessions using echo services
• Used in PING

ICMP functions

1) Announce network errors: Such as host or Entire portion of the network being unreachable, due to some type of failure. A TCP or UDP packet directed at a port number with no receiver attached is also reported via ICMP.
2) Announce network congestion: When a router begins buffering too many packets, due to an inability to transmit them as fast as they are being received, it will generate ICMP Source Quench messages. Directed at the sender, these messages should cause the rate of packet transmission to be slowed.
3) Assist Troubleshooting: ICMP supports an Echo function, which just sends a packet on a round--trip between two hosts. Ping, a common network management tool, is based on this feature. Ping will transmit a series of packets, measuring average round—trip times and computing loss percentages.
4) Announce Timeouts: If an IP packet's TTL field drops to zero, the router discarding the packet will often generate an ICMP packet announcing this fact.

Source : http://elearningatria.files.wordpress.com/2013/10/unit2.pdf