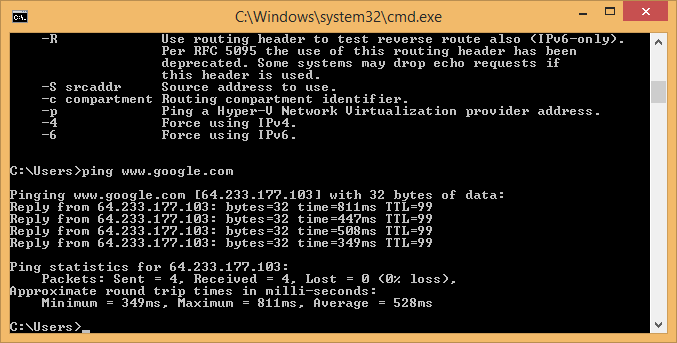
**Q**. **Name the TCP/IP utility troubleshooting tool that often used for network management that make Use of ICMP .**

**A.** The utility used to trouble shot is Ping. Example with screenshot shown below



**Ping**

**The Ping utility is essentially a system administrator's tool that is used to see if a computer is operating and also to see if network connections are intact. Ping uses the Internet Control Message Protocol (ICMP) Echo function which is detailed in RFC 792. A small packet is sent through the network to a particular IP address. This packet contains 32 bytes. The computer that sent the packet then waits (or 'listens') for a return packet. If the connections are good and the target computer is up, a good return packet will be received. PING can also tell the user the number of hops that lie between two computers and the amount of time it takes for a packet to make the complete trip. Additionaly, an administrator can use Ping to test out name resolution. If the packet bounces back when sent to the IP address but not when sent to the name, then the system is having a problem matching the name to the IP address.**

**How Ping works**

**It sends an ICMP (Internet ControlMessage Protocol) Echo Request to a specified interface on the network and, in response, it expects to receivean ICMP Echo Reply. By doing this, the program can test connectivity, gauge response time, and report a variety of errors.**

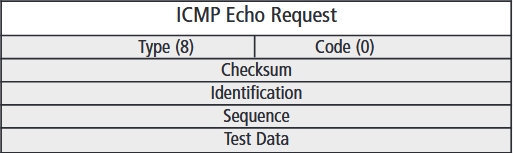
**What Actually Goes On**

When the ping program begins execution, it opens a raw socket sensitive only to ICMP. This means two things:

• **On output** : the sending of ICMP Echo Requests, the program is required to format the ICMP message.The system will provide the IP header and the Ethernet (usually) header.

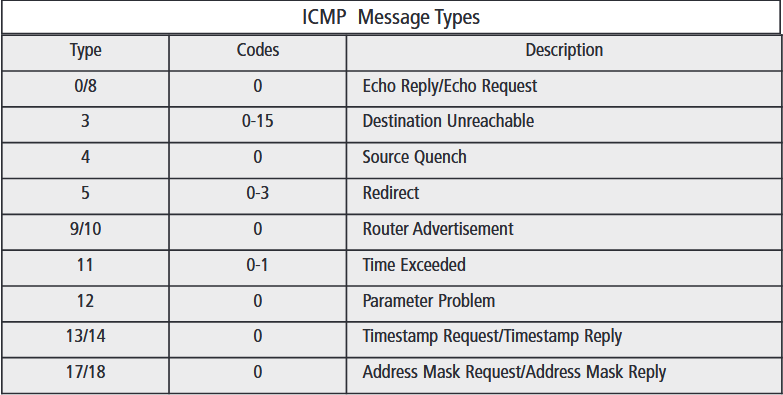
• **On input** : the program must examine all ICMP messages coming in and cull out the items of interest.The expected input is ICMP Echo Replies.

**On the outbound side, the Echo Requests are formatted in the manner shown in Figure below. The message type isalways the coded value eight (8). The code field always contains zero. The checksum is used for error detection.The ICMP message header and data are included in its computation. The ping program performs this calcula-tion and fills in the blank. The identification field follows and is supposed to contain the process ID (PID) thatuniquely identifies that execution of the ping program to the operating system.On Windows systems, this fieldcontains the constant value 256. Next is the sequence number field, which starts at 0 and is bumped by oneon each Echo Request sent. After these required fields, optional test data will follow. In the ping implementa-tion that I examined (Slackware Linux),this included a timestamp used in the round-trip time calculation uponreceipt of the Echo Reply.**



**As for inbound ICMP messages, ping’s task is a bit more complex. Because ping is using a raw ICMP socket,the program is presented with a copy of all incoming ICMP messages,except for a few special cases likeincoming Echo Requests generated by other people pinging us (the latter are handled by the system).Thismeans that ping sees not only the expected Echo Replies when they arrive but also things like DestinationUnreachable, Source Quench, and Time Exceeded messages**

**ICMP message types.**



There are different Flags that can be used with ping those are listed below :