ICMP

The Internet Control Message Protocol (ICMP) was first defined in RFC 792, September, 1981. ICMP message types were later expanded in RFC 1700. ICMP operates at the TCP/IP Network layer and is used to exchange information between devices.

ICMP packets serve many uses in today's computer network. When a router cannot deliver a packet to a destination network or host, an informational message is returned to the source. Also, the **`ping`** and **`tracert`** commands send ICMP messages to destinations, and destinations respond with ICMP messages.

Understand the Format of ICMP Packets.

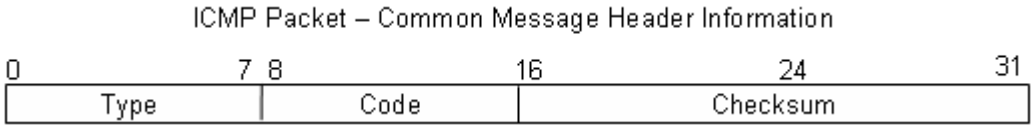


Figure 1. ICMP Message Header

Refer to Figure 1, the ICMP header fields common to all ICMP message types. Each ICMP message starts with an 8-bit Type field, an 8-bit Code field, and a computed 16-bit Checksum. The ICMP message type describes the remaining ICMP fields. The table in Figure 2 shows ICMP message types from RFC 792:

Value	Meaning
0	Echo Reply
3	Destination Unreachable
4	Source Quench
5	Redirect
8	Echo
11	Time Exceeded
12	Parameter Problem
13	Timestamp
14	Timestamp Reply
15	Information Request
16	Information Reply

Figure 2. ICMP Message Types

Codes provide additional information to the Type field. For example, if the Type field is 3, destination unreachable, additional information about the problem is returned in the Code field. The table in Figure 3 shows message codes for an ICMP Type 3 message, destination unreachable, from RFC 1700:

Code Value	Meaning
0	Net Unreachable
1	Host Unreachable
2	Protocol Unreachable

3	Port Unreachable
4	Fragmentation Needed and Don't Fragment was Set
5	Source Route Failed
6	Destination Network Unknown
7	Destination Host Unknown
8	Source Host Isolated
9	Communication with Destination Network is Administratively Prohibited
10	Communication with Destination Host is Administratively Prohibited
11	Destination Network Unreachable for Type of Service
12	Destination Host Unreachable for Type of Service

Figure 3. ICMP Type 3 Message Codes

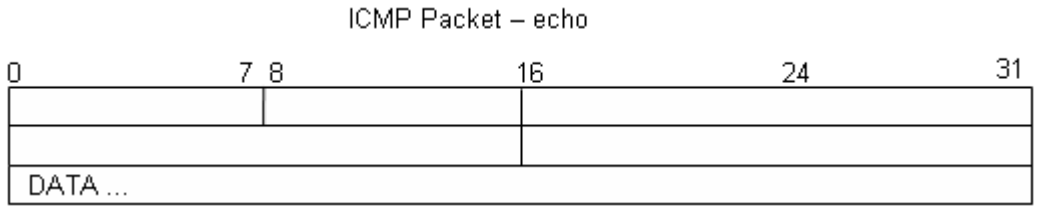
Packet format:

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								Code								ICMP header checksum															
Identifier																Sequence number															
Data :::																															

Using ICMP message capture shown in Figure 4, fill in the fields for the ICMP packet echo request. Values beginning with `0x` are hexadecimal numbers:

```
Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0x365c [correct]
  Identifier: 0x0200
  Sequence number: 0x1500
  Data (32 bytes)
```

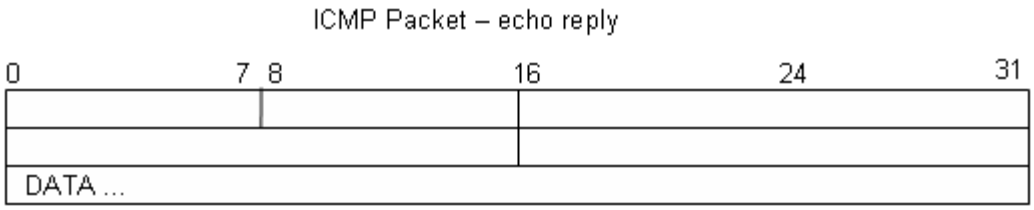
Figure 4. ICMP Packet Echo Request



Using the ICMP message capture shown in Figure 5, fill in the fields for the ICMP packet echo reply:

```
Internet Control Message Protocol
  Type: 0 (Echo (ping) reply)
  Code: 0
  Checksum: 0x3e5c [correct]
  Identifier: 0x0200
  Sequence number: 0x1500
  Data (32 bytes)
```

Figure 5. ICMP Packet Echo Reply



At the TCP/IP Network layer, communication between devices is not guaranteed. However, ICMP does provide minimal checks for a reply to match the request.