An ICMP Reference

Site Sponsor: Netsparker — find vulnerabilities in your web applications before someone else does it for you.

☞ Every Sunday I put out a curated list of the week's most interesting stories in infosec, technology, and humans. You can subscribe to it here.

The Internet Control Message Protocol (RFC 792) was designed to provide network connectivity information to administrators and applications. The protocol is broken up into two classifications: *types*, and *codes*. The types are the overall categories, and the codes are the individual messages within the categories.

Some types don't have any codes beneath them, and receive by default a "no-code" number of zero (0). An example is Type 8 (a `ping` packet), which is often thought of as Type 8, Code 0. Also notice the color-coded pairings within the types; they indicate a relationship the pair, e.g. an echo request solicits an echo reply, and a timestamp request solicits a timestamp reply.

```
hermes root # tcpdump -nnvXSs 1514 -c1 icmp
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 1514 byt
23:11:10.370321 IP (tos 0x20, ttl  48, id 34859, offset 0, flags [none], lengt
69.254.213.43 > 72.21.34.42: icmp 64: echo request seq 0
        0x0000:  4520 0054 882b 0000 3001 7cf5 45fe d52b  E..T.+..0.|.E..+
        0x0010:  4815 222a 0800 3530 272a 0000 25ff d744  H."..50'..%..D
        0x0020:  ae5e 0500 0809 0a0b 0c0d 0e0f 1011 1213  .^..............
        0x0030:  1415 1617 1819 1a1b 1c1d 1e1f 2021 2223  .............!"#
        0x0040:  2425 2627 2829 2a2b 2c2d 2e2f 3031 3233  $%&'()*+,-./0123
        0x0050:  3435 3637                                4567
```

In the `ping` packet above I've highlighted the type and code in green. 0800 indicates Type 08 and Code 00.

The Most Common Types

**For a complete list see IANA

- Type 0 : Echo Reply
- Type 3 : Destination Unreachable
    - 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
    - 13 : Communication Administratively Prohibited
    - 14 : Host Precedence Violation
    - 15 : Precedence cutoff in effect

- Type 5 : Redirect
    - 0 : Redirect Datagram for the Network (or subnet)
    - 1 : Redirect Datagram for the Host
    - 2 : Redirect Datagram for the Type of Service and Network
    - 3 : Redirect Datagram for the Type of Service and Host

- Type 8 : Echo Request
- Type 11 : Time Exceeded
    - 0 : Time to Live exceeded in Transit
    - 1 : Fragment Reassembly Time Exceeded

- Type 13 : Timestamp Request
- Type 14 : Timestamp Reply
- Type 17 : Address Mask Request
- Type 18 : Address Mask Reply
- Type 30 : Traceroute

SOME KEY POINTS ABOUT ICMP

1. ***ICMP Doesn't Have Ports*** You can't actually `ping` a port. Or, more accurately, "pinging a port" is a misnomer. When someone speaks of "pinging a port" they are actually referring to using a layer 4 protocol (such as TCP or UDP) to see if a port is open. So if someone "pings" port 80 on a box, that usually means send it a TCP SYNto that system in order to see if it's responding. The misnomer exists because "pinging something" is now synonymous in the IT world with checking to see if it's alive in a general sense. So if you're checking to see if a port is listening, it's natural to refer to that act as "pinging" the port. Just remember that the original, real `ping`uses ICMP, which doesn't use ports at all.

1. ***ICMP Works At Layer Three (3)*** While ICMP sits "on top of", i.e. *is embedded in*, IP, ICMP is *not* a layer 4 protocol. It's still considered to be at layer 3 rather than one layer higher.

1. ***Traceroute Uses ICMP Type 11, Code 0 (TTL Exceeded) To Do Its Work*** Windows (`tracert`) and Unix/Linux (`traceroute`) use different protocols by default to do traceroutes. Windows uses ICMP, while Unix/Linux uses

UDP. The key point here, however, is that *the embedded protocol doesn't matter*. Tracerouting works because of the TTL value in the **IP** portion of the packet — not the ICMP, TCP, or UDP parts. This is why it doesn't matter what "upper level" protocol is used.

```
hermes root # tcpdump -nnvXSs 1514 -c1 icmp and dst hermes
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 1514 byt
16:07:53.016435 IP (tos 0xc0, ttl 255, id 27812, offset 0, flags [none], lengt
72.21.34.41 > 72.21.35.45: icmp 36: time exceeded in-transit
        0x0000:  45c0 0038 6ca4 0000 ff01 79e3 4815 2229  E..8l.....y.H.")
        0x0010:  4815 222a <blue0b00 f4ff 0000 0000 4500 001c  H."........E...
        0x0020:  6c53 0000 0001 ccdd 4815 222a 480e cf63  lS......H."H..c
        0x0030:  0800 10a2 e75d 0000                      .....]..
```

This TTL Exceeded packet shows the Type 11 (0b), Code 0 (00) in the first two bytes of the ICMP header.

Fun with ICMP

If you're ever interviewing someone for a networking-oriented position, consider the following trick question:

> ### What port does ping work over?

If they are interviewing for a position that requires they know their protocols and they give it any real thought, consider another candidate.: