Computer Networks and Data Systems

Internet Control Message Protocol (ICMP)
ICMP overview

- Primarily used for error and status messages
- Some security dweebs seem to fear ICMP
  - Let’s be rational regarding ICMP
- ICMP is kind of like many protocols in one
  - All ICMP messages have 3 common fields
    - TYPE, CODE, CHECKSUM
  - Otherwise ICMP messages can vary widely
By way of example...

• Extract of my standard iptables ruleset:

```
# icmp ingress / egress
-p icmp --icmp-type echo-reply -j ACCEPT
-p icmp --icmp-type destination-unreachable -j ACCEPT
-p icmp --icmp-type echo-request -j ACCEPT
-p icmp --icmp-type time-exceeded -j ACCEPT
-p icmp --icmp-type parameter-problem -j ACCEPT
-p icmp -j DROP
```
ICMP echo / echo reply

- This is the heart of the infamous “ping”
- ID and sequence numbers match ping to reply
- The variable length data is “echoed” back
ICMP destination unreachable

- Returned to a sender by a router, host or firewall
  - Host, net, protocol, port unreachables
  - Administratively prohibited
  - Fragmentation needed and DF was set
    - Filtering has caused problems – thx dweebs
    - And some more, but not typically very common
- Includes original IP header + 64 bits
  - This can be handy for debugging
ICMP time exceeded

• Almost always a TTL has expired
  • Fragmentation reassembly expired, rare
• Perhaps you're doing a traceroute?
• Perhaps there is a routing loop?
• You again get IP header + 64 bits
ICMP parameter problem

- Some sort of datagram header processing error
- I can't think of a time I've seen this in practice
- Could probably do w/o it, but should be harmless
  - I'm a little more liberal in what I accept
Other ICMP messages of note

• Source quench
  • ineffective as congestion control knob
• Redirect
  • You want to know if you're getting them
  • But you don't want them!
• Timestamp, netmask, etc. requests
  • These just seem to be information leaks to me
ICMPv6

• Similar semantics to ICMP with IPv4
  • But new IP protocol number and some changes
• Packet Too Big
  • Fragmentation now done at the ends (PMTU)
• Router Solicitation / Advertisement
  • Aid to automatic address configuration
• Neighbor Solicitation / Advertisement
  • Akin to ARP in IPv4