Chap 6 − ICMP

Internet Control Message Protocol

ICMP data are encapsulated in IP datagrams

IP header − 20 bytes
ICMP Message (4 bytes + variable length part)

ICMP header format

  type specifier
  function code
  16 bit checksum

Type specifier values

48 #define ICMP_ECHOREPLY 0 /* Echo Reply */
49 #define ICMP_DEST_UNREACH 3 /* Destination Unreachable */
50 #define ICMP_SOURCE_QUENCH 4 /* Source Quench */
51 #define ICMP_REDIRECT 5 /* Redirect (change route) */
52 #define ICMP_ECHO 8 /* Echo Request */
53 #define ICMP_TIME_EXCEEDED 11 /* Time Exceeded */
54 #define ICMP_PARAMETERPROB 12 /* Parameter Problem */
55 #define ICMP_TIMESTAMP 13 /* Timestamp Request */
56 #define ICMP_TIMESTAMPREPLY 14 /* Timestamp Reply */
57 #define ICMP_INFO_REQUEST 15 /* Information Request */
58 #define ICMP_INFO_REPLY 16 /* Information Reply */
59 #define ICMP_ADDRESS 17 /* Address Mask Request */
60 #define ICMP_ADDRESSREPLY 18 /* Address Mask Reply */
Two basic classes

Query
- Ping request/reply
- Timestamp request/reply
- Address-mask request/reply

Error
- Destination unreachable
- Redirect
- Time (hop count) exceeded
- Bad parameters
  - Contains IP header + 1st 8 bytes of offending datagram

ICMP Query examples

Packet format

  - ICMP Header
  - Identifier / Sequence number
  - Query specific data

ICMP Echo

  - Intended to test for reachability
  - Now neither a necessary nor sufficient condition to ensure reachability

ICMP Address Mask

  - Intended for diskless workstations
  - Query specific data is the address mask
  - Note bugs explained in examples in book
    - svr4 sends wrong mask
    - bsdi broadcasts the reply. (see fig 6.5)

ICMP Timestamp

  - Originate timestamp – Requester
  - Receive timestamp – Reply
  - Transmit timestamp – Reply

  - Time is in milliseconds since midnight UTC
  - Use has been somewhat obsoleted by NTP
ICMP Error messages

Ethernet header
IP header (Dest = originator)
8 byte ICMP header
Original IP header + at least 8 bytes of message.

ICMP error messages are never generated in response to:

Receipt of an ICMP error.
A datagram carrying a broadcast address
A datagram sent as a link layer broadcast
Other than the first fragment
A datagram whose source address doesn’t define a single host.
(Some of these rules were learned the hard way!)

Error codes for type=3 Unreachable

#define ICMP_NET_UNREACH 0 /* Network Unreachable */
define ICMP_HOST_UNREACH 1 /* Host Unreachable */
define ICMP_PROT_UNREACH 2 /* Protocol Unreachable */
define ICMP_PORT_UNREACH 3 /* Port Unreachable */
define ICMP_FRAG_NEEDED 4 /* Fragmentation Needed/DF set */
define ICMP_SR_FAILED 5 /* Source Route failed */
define ICMP_NET_UNKNOWN 6
#define ICMP_HOST_UNKNOWN 7
#define ICMP_HOST_ISOLATED 8
#define ICMP_NET_ANO 9
#define ICMP_HOST_ANO 10
#define ICMP_NET_UNR_TOS 11
#define ICMP_HOST_UNR_TOS 12
#define ICMP_PKT_FILTERED 13 /* Packet filtered */
define ICMP_PREC_VIOLATION 14 /* Precedence violation */
define ICMP_PREC_CUTOFF 15 /* Precedence cut off */

Error codes for type=11 Time Exceeded

#define ICMP_EXC_TTL 0 /* TTL count exceeded */
define ICMP_EXC_FRAGTIME 1 /* Fragment Reass time exceeded */