CS 372 Lecture #31

Internet Control Message Protocol (ICMP)

- error messages
- informational messages

Note: Many of the lecture slides are based on presentations that accompany *Computer Networking: A Top Down Approach,* 6th edition, by Jim Kurose & Keith Ross, Addison-Wesley, 2013.

Error detection

- IP provides *best-effort delivery*
- IP can detect a variety of errors, e.g. :
  - Checksum
  - TTL expires
  - No route to destination network
- IP discards datagrams with certain types of problems
- Some types of errors can be reported
- *Internet Control Message Protocol* (ICMP) provides error-reporting mechanisms (RFC 792)
- Router sends control message back to source
  - Contains coded information about the problem

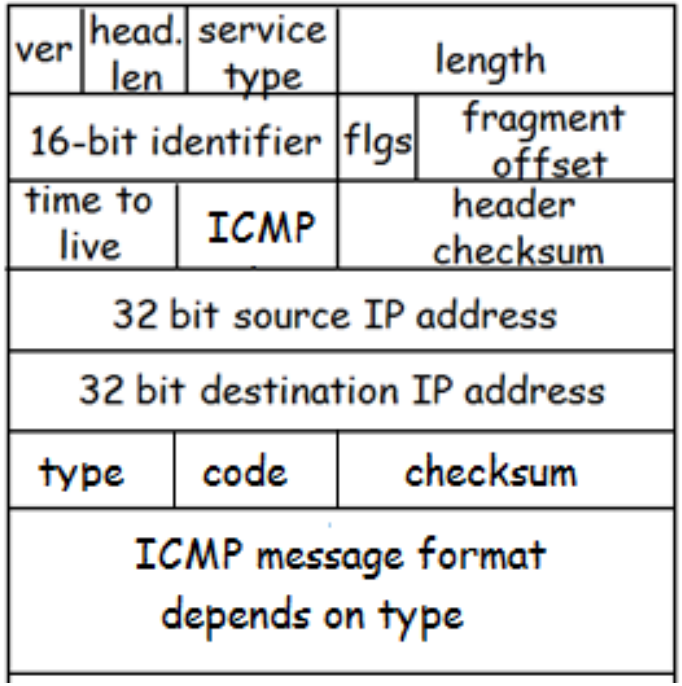
ICMP message format (RFC 792)

- Encapsulated in IP datagram
- Message format depends on type
  - Type 8-bit [0 .. 40] (41 .. 255 reserved)
  - Code 8-bit (sub-type)
  - Checksum
    - Same as UDP
  - Other information (32-bit units)
    - Router addresses, etc.
  - Original IP Header + first 8 bytes of data
    - Original IP header is at least 20 bytes.
    - Datagram data is used by host to match message to appropriate process.

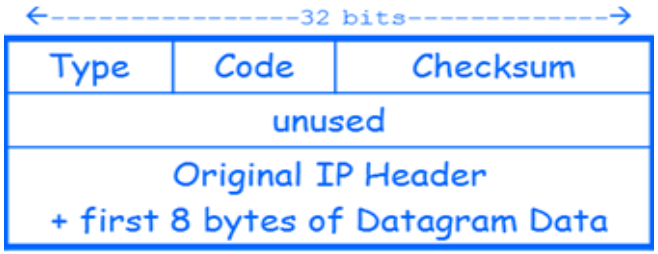
Types and codes:

see http://en.wikipedia.org/wiki/Internet_Control_Message_Protocol

IP datagram



Example ICMP type 3 message



ICMP messages

- *ICMP* defines 2 classes of messages
  - error messages
  - informational messages

Examples:

Type	Code	Description
0	0	echo reply
3	0	destination network unreachable
3	1	destination host unreachable
3	2	destination protocol unreachable
3	3	destination port unreachable
3	6	destination network unknown
3	7	destination host unknown
4	0	source quench
8	0	echo request
9	0	route advertisement
10	0	router solicitation
11	0	TTL expired
12	0	bad IP header

Example error messages:

- Destination unreachable
  - router sends when a datagram cannot be delivered to its final destination
- Source quench
  - router sends when it has no more queuing space available.
- Time exceeded
  - message is sent in two cases
    1. router sends when TTL = 0
    2. destination host sends when reassembly timer expires before all fragments arrive
- Fragmentation required
  - router sends when datagram too large for outbound network (if "do-not-fragment" flag is set)

ICMP messages

- *ICMP* defines 2 classes of messages
  - error messages
  - informational messages

Examples:

Type	Code	Description
0	0	echo reply
3	0	destination network unreachable
3	1	destination host unreachable
3	2	destination protocol unreachable
3	3	destination port unreachable
3	6	destination network unknown
3	7	destination host unknown
4	0	source quench
8	0	echo request
9	0	route advertisement
10	0	router solicitation
11	0	TTL expired
12	0	bad IP header

Example informational messages:

- Echo request/reply
  - Sent to ICMP software on any host/router
  - In response to a request, the ICMP software is required to send an ICMP echo reply message.
- Address mask request/reply
  - Broadcast when a host boots
  - Router replies with the mask used in that subnet
- Router path MTU discovery
  - Distributed path discovery

ICMP Applications

- Implemented at the network layer
  - only user interface goes to the application layer
- *ping*, *echo*, *traceroute*, *etc.*
- Discovery, router collaboration
  - optimal path, MTU, etc.
  - intra-system routing, e.g.:
    - Router Information Protocol (RIP)
    - Open Shortest Path First Protocol (OSPF)
  - inter-system routing, e.g.:
    - Border Gateway Protocol (BGP)

Reachability and *ping*

- An internet host, *A*, is *reachable* from another host, *B*, if datagrams can be delivered from *A* to *B*
- *ping* program tests reachability - sends datagram from *B* to *A* and *A echoes* it back to *B*
  - Uses ICMP "echo request" (8,0) and "echo reply" (0,0) messages
  - IP includes "application" code to reply to incoming ICMP "echo request" messages

traceroute

- List of all routers on the computed path from *A* to *B* is called the *route* from *A* to *B*
- *traceroute* uses UDP with TTL field set and sends to a very unlikely port
- Finds route via *expanding ring search* *
  - when ICMP message arrives, source keeps copy of message
  - UDP segment eventually arrives at destination host
    - destination returns ICMP "port unreachable" message (3, 3)

* Expanding ring search

First datagram
- TTL = 1
- gets to first router, TTL = 0
- is discarded and ICMP "time exceeded" message is returned
  - message includes router address/name

Next datagram
- TTL = 2
- gets through first router to second router, TTL = 0
- is discarded and ICMP "time exceeded" message is returned
  - message includes router address/name

…

Continue until message from destination received

Path MTU discovery

- Fragmentation should be avoided if possible
- Source can determine *path MTU* - smallest MTU on path from source to destination
  - Probes path using source MTU datagrams with *do-not-fragment* flag set
  - Router with smaller MTU responds with ICMP "fragmentation required" (3,4) message
  - Source sends smaller datagrams until destination reached

Router discovery

- Any router along the route can fail, isolating host from internet (black hole)
- Router can broadcast request for "router solicitation" (10,0) to auto-configure default route
- Router can broadcast "router advertisement" (9,0) of existence when first connected
- Routers can share discoveries for updating routing tables

Summary Lecture #31

- ICMP message examples
  - error
  - informational
- ICMP applications
  - *ping*, *traceroute*
  - router collaboration
    - optimal path, path MTU, router discovery