Exploration: The Internet Control Message Protocol (ICMP)

Introduction

Routers can communicate with each other, and with sender hosts using ICMP messages. They can send both error and informational messages using ICMP. But what is ICMP and why do we need it?

IP provides a best-effort delivery service. IP can detect a variety of errors including:

- Checksum
- TTL expires
- No route to destination network

If an error occurs IP will discard the datagram. Some of these errors can be reported. The Internet Control Message Protocol (ICMP) provides for error-reporting mechanisms (RFC 792). To report errors, the router sends an ICMP control message back to the source. This message contains coded information about the problem. But what is ICMP?

An ICMP message is encapsulated in a standard IP datagram. The message format (datagram payload) depends on the ICMP type. The type is 8-bits [0 .. 40] (41 .. 255 reserved). There is also an additional 8-bit code for the message sub-type.

IP datagram

<table>
<tr><td>ver</td><td>head len</td><td colspan="2">service type</td><td colspan="4">length</td></tr>
<tr><td colspan="4">16-bit Identifier</td><td>flags</td><td colspan="3">fragment offset</td></tr>
<tr><td colspan="2">time to live</td><td colspan="2">ICMP</td><td colspan="4">header checksum</td></tr>
<tr><td colspan="8">32-bit source IP address</td></tr>
<tr><td colspan="8">32-bit destination IP address</td></tr>
<tr><td colspan="2">type</td><td colspan="2">code</td><td colspan="4">checksum</td></tr>
<tr><td colspan="8">ICMP message format depends on type</td></tr>
</table>

An ICMP message is encapsulated in a standard IP datagram.

ICMP Error Messages

There are 2 classes of ICMP messages: Error and Informational. Both have the same header. Let’s look first at some of the error messages:

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

ICMP Information Messages

Let’s now look first at some of the ICMP informational messages:

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

ICMP Applications

The type and sub-type of an ICMP message are used by the host to match messages to the appropriate process. This process will be running one of a number of ICMP applications. All of these applications are implemented in the network layer, however, the GUI (if any) will run in the application layer of the host. Examples include ping, echo, traceroute, and more.

One of the more important classes of ICMP applications involve router-to-router communication. When a new router is added to the core, this router must signal it’s availability so that it can participate in routing. To do this, the router can broadcast a request for “router solicitation” (type: 10, code: 0) to auto-configure a default route. The router can also broadcast a “router advertisement” (type: 9, code: 0) to let other routers know of its existence when first connected. Other similar router-to-router messages enable router collaboration on the optimal path, smallest MTU discovery, sharing of routing table information, and more. This is what makes the router core a highly efficient plug-and-play system.

Fragmentation causes a lot of overhead to be added to communications so it should be avoided if at all possible. A source can determine path MTU (smallest MTU on the full path from source to dest) by using ICMP error messages. The source will probe the path using datagrams with the do-not-fragment flag set. If the datagram reaches a router in the path and the next hop has a smaller MTU than the datagram, then that router will discard the datagram and send an ICMP error message back to the source with the “fragmentation required” code.

In this way the source can probe the full path with smaller and smaller datagrams until the destination is reached and the smallest MTU is known.

This concludes our discussion of ICMP messages. Be sure to watch the video lecture below for more details, including a discussion of the traceroute and ping applications. Then test your knowledge with the included Self-Check exercises.

Video Lecture

ICMP

CS 372 Lecture

Internet Control Mes tocol (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.

(PDF (https://oregonstate.instructure.com/courses/1798856/files/83165130/download?wrap=1) (https://oregonstate.instructure.com/courses/1798856/files/83165130/download?wrap=1) |PPT (https://oregonstate.instructure.com/courses/1798856/files/83165073/download?wrap=1) (https://oregonstate.instructure.com/courses/1798856/files/83165073/download?wrap=1))

Self-Check Exercises

ICMP allows information to be carried between what types of devices (e.g. router to…)?

- □ Router to Source Host
- □ Router to Router
- □ Source Host to Destination Host
- □ Destination Host to Source Host

✔ Check

How is an ICMP message carried?

Resources

- **Internet Control Message Protocol Types and Codes**
  (https://en.wikipedia.org/wiki/Internet_Control_Message_Protocol)
  "Internet Control Message Protocol." In Wikipedia, February 4, 2020.