Internet Control Message Protocol

ICMP

The Context

- IP-Related Protocol: ICMP
Internet Control Message Protocol (ICMP)

- The Internet Control Message Protocol (ICMP) is used by routers and hosts to send network control information to each other.

- From a layering point of view, ICMP is a separate protocol that sits above IP and uses IP to transport messages.

- In practice, ICMP is an integral part of IP and all IP modules must support the ICMP protocol.

![Layering Diagram]

Internet Control Message Protocol

- ICMP messages are encapsulated in IP datagrams.

<table>
<thead>
<tr>
<th>ICMP Header</th>
<th>ICMP Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Header</td>
<td>IP Data</td>
</tr>
<tr>
<td>Frame Header</td>
<td>Frame Data</td>
</tr>
</tbody>
</table>

- ICMP frames are identified by IP Protocol field value 1.
- Used by IP to send error and control messages.
- Uses IP to send its messages.
ICMP Message Format

- ICMP message: content contains the first 8 bytes of IP datagram causing error, plus other things

Types of ICMP Messages

- Information messages

  - Sender sends a query to another machine (either host or router) and expects an answer. For example, a host might want to know if a router is alive

- Error indication messages

  - The IP software on a host or router has encountered a problem processing an IP datagram. For example, it may be unable to route the datagram to its destination.
ICMP Types of Messages

<table>
<thead>
<tr>
<th>Category</th>
<th>Type</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Error-reporting</td>
<td>3</td>
<td>Destination unreachable</td>
</tr>
<tr>
<td>messages</td>
<td>4</td>
<td>Source quench</td>
</tr>
<tr>
<td></td>
<td>11</td>
<td>Time exceeded</td>
</tr>
<tr>
<td></td>
<td>12</td>
<td>Parameter problem</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>Redirection</td>
</tr>
<tr>
<td>Query messages</td>
<td>8 or 0</td>
<td>Echo request or reply</td>
</tr>
<tr>
<td></td>
<td>13 or 14</td>
<td>Timestamp request or reply</td>
</tr>
<tr>
<td></td>
<td>17 or 18</td>
<td>Address mask request or reply</td>
</tr>
<tr>
<td></td>
<td>10 or 9</td>
<td>Router solicitation or advertisement</td>
</tr>
</tbody>
</table>

ICMP Error Reporting

- Error reporting
  - Destination unreachable
  - Source quench
  - Time exceeded
  - Parameter problems
  - Redirection
ICMP Error Messages

**ICMP always reports error messages to the original source.**

**Important Points**
- No ICMP error message will be generated in response to a datagram carrying an ICMP error message.
- No ICMP error message will be generated for a fragmented datagram that is not the first fragment.
- No ICMP error message will be generated for a datagram having a multicast address.
- No ICMP error message will be generated for a datagram having a special address such as 127.0.0.0 or 0.0.0.0.

ICMP Data for Error Messages

![Diagram showing ICMP data structure for error messages.](image-url)
ICMP Error Messages (1)

- **Destination Unreachable (type 3)**
  - When a gateway (router) cannot route a datagram (e.g., it doesn't have an appropriate route in its local table, or it needs to fragment and the DF bit is set), it discards the message and returns an ICMP "destination unreachable" message to the sending host.

- **Source Quench (type 4)**
  - When a gateway becomes congested and runs out of buffer space, it may discard a datagram and return a source quench message. Source quench messages are used to request that the sender reduce the rate at which it is sending datagrams.

ICMP Error Messages (2)

- **Time Exceeded (type 11)**
  - As a datagram is processed, routers decrement its time-to-live (TTL) field. If the TTL value reaches 0, the gateway discards the datagram and sends a time exceeded message (code 0) to the sender.
  - Code 1 is used by a destination host to show that not all fragments have arrived within a set time.
Recall: Traceroute

- Traceroute records the route that packets take
- A clever use of ICMP and the TTL field
- When a router receives a packet, it decrements TTL
- If TTL=0, send ICMP “Time exceeded” back to sender
- To determine a route
  - Send a packet with TTL = 1 (hop)
  - The first router discards the packet and sends ICMP “Time Exceeded”; when ICMP “Time Exceeded” is received, record the sender’s (router’s) address
  - Increment TTL
  - Repeat until the destination host is received or an error occurs

Traceroute (contd.)
ICMP Error Messages (3)

- **Parameter Problem (type 12)**
  - When a host or gateway encounters a problem parsing an IP datagram, it returns a parameter problem message to the datagram's sender

- **Redirection (type 5)**
  - Sent from a router to a local host on the same network
  - Informs the source of a better route to the destination
  - A host usually starts with a small routing table that is gradually augmented and updated. Redirection helps it.

ICMP Redirect Example (1)

Host A has one default router, which is R2
ICMP Redirect Example (2)

When A wants to send a message to the Campus Net, it sends it to the default router (R2)

R2 forwards the message to R1

ICMP Redirect Example (3)

R2 also sends an ICMP redirect message to A, telling it to use R1 for connections to csgate.vill.edu
ICMP Redirect

<table>
<thead>
<tr>
<th>Type: 5</th>
<th>Code: 0 to 3</th>
<th>Checksum</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address of the target router</td>
<td>Part of the received IP datagram including IP header plus the first 8 bytes of datagram data</td>
<td></td>
</tr>
</tbody>
</table>

Redirection Message Format

ICMP Redirect Example (4)

A sends subsequent packets directly to R1

Note: some hosts deliberately ignore ICMP Redirect messages as a precaution against network attacks.
ICMP Query Messages

- Used to diagnose network problems
- In this type of ICMP message, a node sends a message that is answered in a specific format by the destination node.

**Echo Request / Reply (types 8 / 0)**

- If machine A sends an ICMP echo request message to machine B, machine B is required to respond with an ICMP echo reply
- In UNIX, the program **ping** allows a user to check whether a machine is reachable and functioning
Ping

- Uses ICMP Echo request/reply to
  - test destination reachability
  - compute round trip time
  - count the # of hops to destination

- Source sends ICMP echo request message to the destination address
  - echo request packet contains timestamp also

- Destination replies with an ICMP echo reply message containing the data in the original request message

- Source can calculate RTT of packets

- If no echo reply comes back, destination unreachable

---

Ping (contd.)

Sample output:
Reply from 164.107.144.3: 48 bytes in 47 msec. TTL: 253
ICMP Echo Request / Reply Message

<table>
<thead>
<tr>
<th>Type: 8 or 0</th>
<th>Code: 0</th>
<th>Checksum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identifier</td>
<td>Sequence number</td>
<td></td>
</tr>
</tbody>
</table>

Optional data
Sent by the request message; repeated by the reply message

- The identifier and sequence number may be used by the echo sender to aid in matching the replies with the echo requests.

ICMP Timestamp Request / Reply Message

<table>
<thead>
<tr>
<th>Type: 13 or 14</th>
<th>Code: 0</th>
<th>Checksum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identifier</td>
<td>Sequence number</td>
<td></td>
</tr>
</tbody>
</table>

- Original timestamp
- Receive timestamp
- Transmit timestamp

- Timestamp-request and timestamp-reply messages can be used to calculate the round-trip time between a source and a destination machine.
ICMP Mask Request / Reply Message

<table>
<thead>
<tr>
<th>Type: 17 or 18</th>
<th>Code: 0</th>
<th>Checksum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identifier</td>
<td>Sequence number</td>
<td>Identifier</td>
</tr>
<tr>
<td>Address mask</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Timestamp-request and timestamp-reply messages can be used to calculate the round-trip time between a source and a destination machine.

ICMP Router Solicitation / Advertisement

<table>
<thead>
<tr>
<th>Type: 9</th>
<th>Code: 0</th>
<th>Checksum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of addresses</td>
<td>Address entry size</td>
<td>Lifetime</td>
</tr>
<tr>
<td>Router address 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Address preference 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Router address 2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Address preference 2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
New ICMP Version:

ICMPv6

Context for ICMPv6

ICMPv6 follows the same strategy and purposes of version 4. It is only slightly more complex than ICMPv4.
Internet Control Message Protocol ICMPv6

- ICMPv6 is more complex than ICMPv4:
  - some protocols that were independent in version 4 are now part of ICMPv6
  - new messages have been added to ICMPv6 to make it more useful
- Introduces some simplifications by eliminating obsolete types of messages no longer in use

ICMPv6 Header

- Type (8 bits)
  - High order bit = 0 (0 – 127) indicates error message
  - High-order bit = 1 (128 – 255) indicates information message.
- Code (8 bits)
  - depends on the message type
- Checksum (16 bits)
  - Used to detect errors in ICMP and part of IPv6
ICMPv6 Messages

- Transported within an IPv6 packet in which extension headers can also be present.
- Identified by a value of 58 in the Next Header field of the IPv6 header or of the preceding Header.

ICMPv6 Error-Reporting Messages

- Destination-Unreachable
- PacketToo-Big
- Time-Exceeded
- Parameter-Problem
ICMPv6 Error Reporting Messages

<table>
<thead>
<tr>
<th>Type</th>
<th>Message Name</th>
<th>Summary Description of Message Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Destination Unreachable</td>
<td>Indicates that a datagram could not be delivered to its destination. <em>Code</em> value provides more information on the nature of the error.</td>
</tr>
<tr>
<td>2</td>
<td>Packet Too Big</td>
<td>Sent when a datagram cannot be forwarded because it is too big for the MTU of the next hop in the route. This message is needed in IPv6 and not IPv4 because in IPv4, routers can fragment oversized messages, while in IPv6 they cannot.</td>
</tr>
<tr>
<td>3</td>
<td>Time Exceeded</td>
<td>Sent when a datagram has been discarded prior to delivery due to the <em>Hop Limit</em> field reduced to zero.</td>
</tr>
<tr>
<td>4</td>
<td>Parameter Problem</td>
<td>Indicates a miscellaneous problem (specified by the <em>Code</em> value) in delivering a datagram.</td>
</tr>
</tbody>
</table>

Error Reporting in ICMP (v4 vs. v6)

<table>
<thead>
<tr>
<th>Type of Message</th>
<th>Version 4</th>
<th>Version 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination unreachable</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Source quench</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Packet too big</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Time exceeded</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Parameter problem</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Redirection</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
ICMPv6 Informational Messages

- Echo-Request
- Echo-Reply
- Router-Solicitation
- Router-Advertisement
- Neighbor-Solicitation
- Neighbor-Advertisement
- Redirect

ICMPv6 Echo Request / Reply

- **Echo-Request**: Sent to test connectivity to another device
- **Echo-Reply**: Sent in response to Echo request

![ICMPv6 Echo Request/Reply Diagram]
Neighbor Discovery Messages

- Used by nodes (hosts or routers) on the same link
  - Router-Solicitation Message
  - Router-Advertisement Message
  - Neighbor-Solicitation Message
  - Neighbor-Advertisement Message

ICMPv6 Neighbor Discovery Messages

<table>
<thead>
<tr>
<th>Type</th>
<th>Message Name</th>
<th>Summary Description of Message Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>133</td>
<td>Router Solicitation</td>
<td>Prompts a router to send a Router Advertisement</td>
</tr>
<tr>
<td>134</td>
<td>Router Advertisement</td>
<td>Sent by routers to tell hosts on the local network that the router exists and describe its capabilities</td>
</tr>
<tr>
<td>135</td>
<td>Neighbor Solicitation</td>
<td>Sent by a device to request the MAC address of another local device and provide its own</td>
</tr>
<tr>
<td>136</td>
<td>Neighbor Advertisement</td>
<td>Provides information about a host to the local network</td>
</tr>
</tbody>
</table>
### Information Messages in ICMP (v4 vs. v6)

<table>
<thead>
<tr>
<th>Type of Message</th>
<th>Version 4</th>
<th>Version 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Echo request and reply</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Timestamp request and reply</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Address mask request and reply</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Router solicitation and advertisement</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Neighbor solicitation and advertisement</td>
<td>ARP</td>
<td>Yes</td>
</tr>
<tr>
<td>Group membership</td>
<td>IGMP</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Path MTU Discovery for ICMPv6 (PMTUD)
PMTUDv6 Overview

- To enable hosts to discover the min. MTU on a path to a particular destination.
- Fragmentation in IPv6 is not performed by intermediary routers.
- The source node may fragment packets by itself only when the path MTU is smaller than the packets to deliver.
- PMTUD for IPv6 uses ICMPv6 error message — Type 2 Packet Too Big

IPv4 vs. IPV6 MTU

- **Increased Default MTU**
  - In IPv4 minimum required MTU = 576 bytes.
  - In IPv6 minimum required MTU = 1280 bytes.
  - Improves efficiency by increasing the ratio of maximum payload to header length, and reduces the frequency of fragmentation.

- **Elimination of En Route Fragmentation**
  - In IPv4, datagrams may be fragmented by either the source device, or by routers during delivery.
  - In IPv6, only the source node can fragment; **routers do not**.
  - The source must therefore fragment to the size of the smallest MTU on the route before transmission.
How Do Hosts Know What Size to Use?

Two choices:

1. Use Default MTU
   - Use the default MTU of 1280, which all physical networks must be able to handle.
   - Good choice especially for short communications or for sending small amounts of data.

2. Use Path MTU Discovery feature
   - A node sends messages over a route to determine what the overall minimum MTU for the path is

Path MTU Discovery