ICMP: Internet Control Message Protocol

(1) ICMP Introduction

- Motivation
  - IP may fail to deliver datagrams because
    - the destination is not available
    - the time-to-live counter expires
    - routers become congested
  - We need to let the sender know what has happened
  - ICMP is a required part of IP

- Purpose
  - ICMP allows routers (and hosts) to send error or control messages to other routers or hosts
  - ICMP provides communication between the Internet Protocol software on one machine and the Internet Protocol software on another

- Restrictions
  - ICMP messages are not generated for errors that result from datagrams carrying ICMP error messages. Why?
  - ICMP is only sent to the original source. Why?

- ICMP Encapsulation
  - ICMP is encapsulated in an IP packet, but is considered part of the IP or Internet layer.
(2) ICMP Messages

- The Common ICMP header
  - Each ICMP message has its own format, they all begin with the same three fields
  - TYPE (8-bit): identifies the message
  - CODE (8-bit): provides further information about the message type
  - CHECKSUM (16-bit):
  - In addition, ICMP messages that report errors always include the header and the first 64 data bits of the datagram causing the problem.

<table>
<thead>
<tr>
<th>Type Field</th>
<th>ICMP Message Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Echo Reply</td>
</tr>
<tr>
<td>3</td>
<td>Destination Unreachable</td>
</tr>
<tr>
<td>4</td>
<td>Source Quench</td>
</tr>
<tr>
<td>5</td>
<td>Redirect (change a route)</td>
</tr>
<tr>
<td>8</td>
<td>Echo Request</td>
</tr>
<tr>
<td>9</td>
<td>Router Advertisement</td>
</tr>
<tr>
<td>10</td>
<td>Router Solicitation</td>
</tr>
<tr>
<td>11</td>
<td>Time Exceeded for a Datagram</td>
</tr>
<tr>
<td>12</td>
<td>Parameter Problem on a Datagram</td>
</tr>
<tr>
<td>13</td>
<td>Timestamp Request</td>
</tr>
<tr>
<td>14</td>
<td>Timestamp Reply</td>
</tr>
<tr>
<td>15</td>
<td>Information Request (obsolete)</td>
</tr>
<tr>
<td>16</td>
<td>Information Reply (obsolete)</td>
</tr>
<tr>
<td>17</td>
<td>Address Mask Request</td>
</tr>
<tr>
<td>18</td>
<td>Address Mask Reply</td>
</tr>
</tbody>
</table>

- Echo request and reply message
  - Used to test reachability
  - An echo request can also contain optional data (the content does not matter)
  - An echo reply always returns exactly the same data as was received in the request
  - Sent by ping program

- Host Unreachable
  - When a router cannot forward or deliver an IP datagram, it sends a destination unreachable message back to the original source
  - The CODE field specifies details
    - 0: network unreachable
    - 1: host unreachable
    - 2: protocol unreachable
    - 3: port unreachable
    - 4: fragmentation needed and DF (don’t fragment) set
    - 5: source route failed
    - Etc.

- Source Quench
  - To deal with congestion and datagram flow control
  - When routers are overrun with traffic, it is called congestion.
A machine uses ICMP source quench messages to report congestion to the original source. There is no ICMP message to reverse the effect of a source quench. Usually the host gradually increases the rate when no further source quench requests are received.

**Route Redirect**
- Routers exchange routing information periodically to accommodate network changes and keep their routes up-to-date. However, hosts do not do this.
- A general rule: *Routers are assumed to know correct routes; hosts begin with minimal routing information and learn new routes from routers.*
- When a router detects a host using a nonoptimal route, it sends the host an ICMP *redirect* message, requesting that the host change its route.
- Limited to interactions between a router and a host on a directly connected network
- Example:

---

### (3) Attacks Using ICMP Messages

**Mapping Network Topology**
- Mapping a target network is a very strategic part of most intelligently planned attacks. This initial step in reconnaissance attempts to discover the live hosts in a target network. An attacker then can direct a more focused scan or exploit toward live hosts only.
- Sending individual ICMP echo: this is what the *ping* command does.
- Sending ICMP echo requests to the broadcast addresses of a network.
- Sending ICMP echo requests to network and broadcast address of subdivided networks
- Sending an ICMP address mask request to a host on the network to determine the subnet mask to better understand how to map efficiently.

**Smurf Attack**
- Ping a broadcast address, with the (spoofed) IP of a victim as source address
- All hosts on the network respond to the victim
- The victim is overwhelmed
- Keys: Amplification and IP spoofing
- Protocol vulnerability; implementation can be “patched” by violating the protocol specification, to ignore pings to broadcast addresses
- ICMP echo just used for convenience
- All ICMP messages can be abused this way
- "Fraggle" is the equivalent with UDP

**Ping of Death**
- ICMP echo with fragmented packets
- Maximum legal size of an ICMP echo packet: $65535 - 20 - 8 = 65507$
- Fragmentation allows bypassing the maximum size: $(\text{offset + size}) > 65535$
- Reassembled packet would be larger than 65535 bytes
- OS crashes
- Same attack with different IP protocols
ICMP Redirect Attack

- Ask a host to send their packet to the target “router”.
- Useful for man-in-the-middle attacks
- Winfreez(e)
  - Windows
  - ICMP Redirect: YOU are the quickest link to host Z
  - Host changes its routing table for Z to itself
  - Host sends packets to itself in an infinite loop