ICMP

Internet Networking
recitation #4
Making The Network Layer Work.

1. The Internet Protocol (IP)
   • The creation of IP packets.
   • Hop-by-hop delivery from end to end.

2. Routing Tables
   • Algorithms to populate router forwarding tables.

3. Internet Control Message Protocol
   • Communicates network layer information between end hosts and routers.
   • Reports error conditions.
   • Helps us diagnose problems.
Internet Control Message Protocol

• IP and ICMP are companion protocols.
  • ICMP sits on top of IP (IP protocol=1).
    Does it makes sense??

• ICMP provides error report.
• It also provides testing functionality.
• No recursiveness – An ICMP report cannot be triggered by an ICMP message.
How ICMP Messages are sent?

Host A — Host B
ICMP Message Structure

Original Message Arrives

Routing Error

Create ICMP Message From Original Message

Application

Transport

ICMP

Network (IP)

Link (Ethernet)
ICMP Basic Header

- Type - Type of message (Destination Unreachable).
- Code - ICMP subtype (Destination network/host/port Unreachable).
- Checksum - Similar to IP checksum (Works on the header and data).

- Every specific ICMP message will add fields of its own.
Some ICMP Message Types

• Destination Network Unreachable (Type 3, Code 0).
• Destination Host Unreachable (Type 3, Code 1).
• Destination Port Unreachable (Type 3, Code 3).
• Echo Request (Type 8).
• Echo Reply (Type 0).
• TTL Expired (Type 11, Code 0).
Echo and Echo Reply

- Returns an echo of the data and the sequence number that was sent
How “ping” uses ICMP?
How “ping” uses ICMP?

• When a router or host receives an ICMP message of type “echo” it should respond by an “echo-reply”.

• The reply is derived from the request by:
  • Swapping IP header’s source and destination address.
  • Replacing type ECHO (8), by ECHO-REPLY (0).
  • Computing new IP and ICMP checksums.
  • The data payload remains unchanged.
Time Exceeded Message

<table>
<thead>
<tr>
<th>Time Exceeded Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1</td>
</tr>
<tr>
<td>+---------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>+---------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>+----------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>+----------------------------------------------------------------</td>
</tr>
</tbody>
</table>

- Time exceeded (Type 11):
  - Code 0: Time-to-live equals 0 during transit
  - Code 1: Time-to-live equals 0 during reassembly
    - Fragment reassembly time exceeded
How “traceroute” uses ICMP?
How “traceroute” uses ICMP?

• Traceroute works by sending regular IP packets (UDP) towards the destination, and progressively increasing the TTL field, starting from 1.

• The first relay on the path will decrement TTL field to 0, destroy the packet, and send back “TIME-EXCEEDED” (11) ICMP message. The source address of this message identifies the first relay.

• The next message is sent with TTL of 2, and so on…
Destination Unreachable

**Destination Unreachable Message**

<table>
<thead>
<tr>
<th>Type</th>
<th>Code</th>
<th>Checksum</th>
<th>Unused</th>
<th>Internet Header + 64 bits of Original Data Datagram</th>
</tr>
</thead>
</table>

- **0** = net unreachable;
- **1** = host unreachable;
- **2** = protocol unreachable;
- **3** = port unreachable;
- **4** = fragmentation needed and DF set;
- **5** = source route failed.
PMTU Discovery

- path MTU discovery is an iterative procedure.
- Send max-sized packet with “do not fragment” flag set.
- If MTU is encountered, An ICMP message will be returned.
  - “Destination unreachable(Type 3), Fragmentation needed(Code 4)"
- This message is returned with its originator’s next-hop MTU.

- Send MTU-sized packet with “do not fragment” flag set.
- When successful, no reply at IP level.
  - “No news is good news”
PMTU in practice

• In practice, in most OS’s, every TCP packet is send with the DF flag set (Default behavior, can be set otherwise).
• If a network with smaller MTU encountered, an ICMP type 4 code 3 will be sent.
• Other protocols (UDP for example) do not implement PMTU and leave it the developers responsibility.
• Unfortunately, bad practice of blocking ICMP traffic is quite common today.
Questions?