Lecture 10: Addressing

HW 2 due NEXT FRIDAY
Lecture 10 Overview

- Fragmentation example
- ICMP, the *other* network-layer protocol
- IP Addresses
  - Class-based addressing
- Subnetting
  - Classless addressing
Fragmentation Example

One large datagram becomes several smaller datagrams

(Offset actually encoded as bytes/8)

<table>
<thead>
<tr>
<th>length</th>
<th>ID</th>
<th>MF</th>
<th>offset</th>
</tr>
</thead>
<tbody>
<tr>
<td>4000</td>
<td>x</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>length</th>
<th>ID</th>
<th>MF</th>
<th>offset</th>
</tr>
</thead>
<tbody>
<tr>
<td>1500</td>
<td>x</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1500</td>
<td>x</td>
<td>1</td>
<td>1480</td>
</tr>
<tr>
<td>1040</td>
<td>x</td>
<td>0</td>
<td>2960</td>
</tr>
</tbody>
</table>

CSE 123 – Lecture 10: Addressing
Recursive fragmentation

Suppose this packet needs to be sent on a network with a 500-byte MTU.

<table>
<thead>
<tr>
<th>length</th>
<th>ID</th>
<th>MF</th>
<th>offset</th>
</tr>
</thead>
<tbody>
<tr>
<td>1500</td>
<td>x</td>
<td>1</td>
<td>1480</td>
</tr>
</tbody>
</table>

How many fragments will result?

A. 1  
B. 2  
C. 3  
D. 4

What will be the offset of the second fragment?

A. 480 bytes  
B. 1480 bytes  
C. 1960 bytes  
D. 1980 bytes
Costs of Fragmentation

- Interplay between fragmentation and retransmission
  - A single lost fragment may trigger retransmission
  - Any retransmission will be of entire packet (why?)

- Packet must be completely reassembled before it can be consumed on the receiving host
  - Takes up buffer space in the mean time
  - When can it be garbage collected?

- Why not reassemble at each router?
Path MTU Discovery

- Path MTU is the smallest MTU along path
  - Packets less than this size don’t get fragmented

- Fragmentation is a burden for routers
  - We already avoid reassembling at routers
  - Avoid fragmentation too by having hosts learn path MTUs

- Hosts send packets, routers return error if too large
  - Hosts can set “don’t fragment” flag
  - Hosts discover limits, can size packets at source
Aside: ICMP

- What happens when things go wrong?
  - Need a way to test/debug a large, widely distributed system

- ICMP = Internet Control Message Protocol (RFC792)
  - Companion to IP – required functionality

- Used for error and information reporting:
  - Errors that occur during IP forwarding
  - Queries about the status of the network
ICMP Error Message Generation

- ICMP messages include portion of IP packet that triggered the error (if applicable) in their payload
Common ICMP Messages

- Fragmentation needed
  - Need to fragment, but don’t fragment bit set

- TTL Expired
  - Used by the “traceroute” program
    - traceroute traces packet routes through Internet

- Destination unreachable
  - “Destination” can be host, network, port, or protocol

- Redirect
  - To shortcut circuitous routing

- Echo request/reply
  - Used by the “ping” program
    - ping just tests for host liveness
ICMP Restrictions

- The generation of error messages is limited to avoid cascades
  - Error causes error that causes error…

- Don’t generate ICMP error in response to:
  - An ICMP error
  - Broadcast/multicast messages (link or IP level)
  - IP header that is corrupt or has bogus source address
  - Fragments, except the first

- ICMP messages are often rate-limited too
  - Don’t waste valuable bandwidth sending tons of ICMP messages
Addressing Considerations

- Fixed length or variable length addresses?

- Issues:
  - Flexibility
  - Processing costs
  - Header size

- Engineering choice: IP uses fixed length addresses
IP Addresses

- 32-bits in an IPv4 address
  - Dotted decimal format a.b.c.d
  - Each represent 8 bits of address

- Hierarchical: Network part and host part
  - E.g. IP address 128.54.70.238
  - 128.54 refers to the UCSD campus network
  - 70.238 refers to the host ieng6.ucsd.edu

- Which part is network vs. host?
Class-based Addressing

- Most significant bits determines “class” of address

  Class A: \[ \begin{array}{c|c|c} 0 & \text{Network} & \text{Host} \end{array} \]
  - 127 nets, 16M hosts

  Class B: \[ \begin{array}{c|c|c} 1 & \text{Network} & 16 \end{array} \]
  - 16K nets, 64K hosts

  Class C: \[ \begin{array}{c|c|c} 1 & 1 & \text{Network} \end{array} \]
  - 2M nets, 254 hosts

- Special addresses
  - Class D (1110) for multicast, Class E (1111) experimental
  - 127.0.0.1: local host (a.k.a. the loopback address)
  - Host bits all set to 0: network address
  - Host bits all set to 1: broadcast address

To what class network does 132.239.180.101 belong?

A. A  
B. B  
C. C  
D. D
IP Forwarding Tables

- Router needs to know where to forward a packet

- Forwarding table contains:
  - List of network names and next hop routers
  - Local networks have entries specifying which interface
    » Link-local hosts can be delivered with Layer-2 forwarding

- E.g. www.ucsd.edu address is 132.239.180.101
  - Class B address – class + network is 132.239
  - Lookup 132.239 in forwarding table
  - Prefix – part of address that really matters for routing
Subnetting

- Individual networks may be composed of several LANs
  - Only want traffic destined to local hosts on physical network
  - Routers need a way to know which hosts on which LAN

- Networks can be arbitrarily decomposed into subnets
  - Each subnet is simply a prefix of the host address portion
  - Subnet prefix can be of any length, specified with netmask

CSE 123 – Lecture 10: Addressing
For Next Time

- Read 4.1
- Turn in Homework 2 before class Friday