Lecture 9: Internetworking

CSE 123: Computer Networks
Alex C. Snoeren

HW 2 due WEDNESDAY
So what *does* IP do?

- **Addressing**
- **Fragmentation**
  - E.g. FDDI’s maximum packet is 4500 bytes while Ethernet is 1500 bytes, how to manage this?
- **Some** error detection
- **Routers** only forward packets to next hop
  - They do not:
    - Detect packet loss, packet duplication
    - Reassemble or retransmit packets

- We’ll start by deconstructing the header…
# IP Packet Header

<table>
<thead>
<tr>
<th>Field</th>
<th>Byte Range</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ver</td>
<td>0</td>
<td>Version</td>
</tr>
<tr>
<td>HL</td>
<td>1-2</td>
<td>Header Length</td>
</tr>
<tr>
<td>TOS</td>
<td>3</td>
<td>Type of Service</td>
</tr>
<tr>
<td>length</td>
<td>4-16</td>
<td>Length of the Packet</td>
</tr>
<tr>
<td>identification</td>
<td>17-31</td>
<td>Identification</td>
</tr>
<tr>
<td>offset</td>
<td>17-31</td>
<td>Offset from Beginning of Header</td>
</tr>
<tr>
<td>TTL</td>
<td>4</td>
<td>Time to Live</td>
</tr>
<tr>
<td>protocol</td>
<td>5</td>
<td>Protocol Type</td>
</tr>
<tr>
<td>header checksum</td>
<td>6-31</td>
<td>Header Checksum</td>
</tr>
<tr>
<td>source address</td>
<td>32-63</td>
<td>Source IP Address</td>
</tr>
<tr>
<td>destination address</td>
<td>64-95</td>
<td>Destination IP Address</td>
</tr>
<tr>
<td>options (if any)</td>
<td>96-2087</td>
<td>Options (if any)</td>
</tr>
<tr>
<td>data (if any)</td>
<td>96-2087</td>
<td>Data (if any)</td>
</tr>
</tbody>
</table>

The IP Packet Header is 20 bytes long.
Version field

- Which version of IP is this?
  - Plan for change
  - Very important!

- Current versions
  - 4: most of Internet today
  - 6: new protocol with larger addresses
  - What happened to 5?
    Standards body politics.
Header length

- How big is IP header?
  - Counted in 32-bit words
  - Variable length
    » Options
  - Engineering consequences of variable length…

- Most IP packet headers are 20 bytes long
How long is whole packet in bytes?
- Includes header
- Limits total packet to 64K
- Redundant?
IP Checksum

- Header contains simple checksum
  - Validates content of header *only*

- Recalculated at each hop
  - Routers need to update TTL
  - Hence straightforward to modify

- Ensures *correct* destination receives packet
Protocol

● Which transport protocol is the data using?
  ◆ i.e. how should a host interpret the data

● TCP = 6
● UDP = 17
Type-of-Service

- How should this packet be treated?
  - Care/don’t care for delay, throughput, reliability, cost
  - How to interpret, how to apply on underlying net?
  - Largely unused until 2000 (hijacked for new purposes, ECN & Diffserv)
TTL (Time-to-Live)

- How many more routers can this packet pass through?
  - Designed to limit packet from looping forever
- Each router decrements TTL field
- If TTL is 0 then router discards packet
Fragmentation

- Different networks may have different maximum frame sizes
  - Maximum Transmission Unit (MTUs)
  - Ethernet 1.5K, FDDI 4.5K
- Router breaks up single IP packet into two or more smaller IP packets
  - Each fragment is labeled so it can be correctly reassembled
  - End host reassembles them into original packet
IP ID and Bitflags

- Source inserts unique value in identification field
  - Also known as the IPID
  - If packet is fragmented, the router copies this value into any fragments
- Offset field indicates position of current fragment (in bytes/8)
  - Zero for non-fragmented packet
- Bitflags provide additional information
  - More Fragments bit helps identify last fragment
  - Don’t Fragment bit prohibits (further) fragmentation
  - Note recursive fragmentation easily supported—just requires care with More Fragments bit
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>
<tr>
<td>1500</td>
<td>x</td>
<td>1</td>
<td>1480</td>
</tr>
<tr>
<td>1500</td>
<td>x</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1040</td>
<td>x</td>
<td>0</td>
<td>2960</td>
</tr>
</tbody>
</table>
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
    » ICMP protocol: special IP packet format for sending error msgs
  - Reassembly at destination as before
For Next Time

- NO CLASS FRIDAY
- Read 3.2.5 in P&D
- Homework 2 due WEDNESDAY