Network Protocols

Transport Layer and UDP
(TCP in another slide-deck)
Why a transport layer?

• IP gives us end-to-end connectivity doesn't it?
• Why, or why not, more than one transport layer?
• What does a transport layer typically do?
  • Process identification
  • Reliability
  • Flow control
• Are there times when those are unnecessary?
• What are the security / performance issues?
If no L4, what to do with rx data?

HTTP data

<table>
<thead>
<tr>
<th>IPs: 192.0.2.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPd: 192.0.2.2</td>
</tr>
<tr>
<td>Proto: n/a</td>
</tr>
</tbody>
</table>

Thanks!!
But...
How to get this to my to HTTPd?
Try to parse and interpret!?!?
Help me out dude!!
**User Datagram Protocol (UDP)**

| bit   | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
|-------|---|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
|       |   |   |   |   |   |   |   |   |   |   | Source Port |   |   |   |   |   | Destination Port |
|       |   |   |   |   |   |   |   |   |   |   | Length |   |   |   |   |   | Checksum |
|       |   |   |   |   |   |   |   |   |   |   | Data |   |   |   |   |   |   |
|       |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |...|
Application multiplexing

- OS independent identifier for a network app
- Each app assigned a locally unique 16-bit id
  - src or dst “port number”, see /etc/services
- Server (listener) apps
  - Tend to use standard, “well-known” ports
- Client (opener) tends to ephemeral (dynamic) port
  - Usually >1023, but depends on OS and app
- See http://www.iana.org/assignments/port-numbers
UDP is very simple

- Basically just an application multiplexer
- The length field is practically redundant
  - IP total length – 8 = UDP payload
- Source port may be zero if no reply expected
- Even the checksum is optional!
  - Though its inexpensive, recommended to use it
- No inherent flow control, reliability, connection
- Why is this good, how could this be bad?
What uses UDP?

- SNMP, TFTP, DHCP, syslog, Netflow
- Streaming media (VoIP, radio, video)
  - Some use TCP (thank you security dilettantes)
- DNS, NTP
  - UDP death likely (hi dilettantes) if not for these
Common IP transport protocols

- UDP – very common, but usually low rate of pkts
- TCP – most common, typically most of your pkts
- Some usage, but not widely deployed:
  - UDP-Lite
  - SCTP
  - DCCP
- Note, not all IP protocols considered a “transport”
  - e.g. we don't think of ICMP/IGMP as a transport