The Opaque Internet

Jon Crowcroft, 17.8.2023

https://www.cst.cam.ac.uk/people/jac22
TCP/IP Headers as we used to see them

---

**Figure 3: Fields that change during a TCP connection**

<table>
<thead>
<tr>
<th>Byte</th>
<th>Protocol Version</th>
<th>Header Length</th>
<th>Type of Service</th>
<th>Total Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>Source Port</td>
<td>Destination Port</td>
<td>Source Address</td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>Sequence Number</td>
<td></td>
<td>Destination Address</td>
<td></td>
</tr>
<tr>
<td>28</td>
<td>Acknowledgment Number</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>32</td>
<td>Data Offset</td>
<td></td>
<td>Data Byte 1</td>
<td></td>
</tr>
<tr>
<td>36</td>
<td>Checksum</td>
<td></td>
<td>Data Byte 2</td>
<td></td>
</tr>
<tr>
<td>40</td>
<td></td>
<td></td>
<td>Data Byte 3</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>...</td>
<td></td>
</tr>
</tbody>
</table>

The IP header checksum is **not** an end-to-end checksum in the sense of [14]: The time-to-live update forces the IP checksum to be recomputed at each hop. The author has had unpleasant personal experience with the consequences of violating the **end-to-end argument** in [14] and this protocol is careful to pass the end-to-end TCP checksum through unmodified. See sec. 4.
Old school

• Nats (port NATs), firewalls, Carrier Grad Nats
• ToR
• Proxies/caches
• Middle Boxes ("accelerators") (early ack, muck with window etc)
• CDNs, Load Balancers

• And of course HTTPs (TLS)….means we only see IP and ports maybe
“new” kids

- Akamai, Cloudflare
- E.g. see
  
  https://radar.cloudflare.com/

- Books are out of date
  - E.g. lots of QUIC, Masque, one-hop relay etc etc
  - TCP is only about half of it these days
  - IPv6 addr alloc is weird
  - Before you even get there you have DOT
    - https://www.cloudflare.com/learning/dns/dns-over-tls/
QUIC (on UDP...) exchanges..
Challenges #1

• BGP – routeviews
• Can’t do from single vantage point…
• Lots of tools to detect hijacks etc, but depend on
  • Deploying collectors is a Big Effort
  • Luckily, lots of people have done this
  • Look for their resources/repositories of data too!
Asymmetric routes are v. common

- So outbound isn’t same as
- Inbound😊
Challenges #2

- Performance measurement is hard
  - packet trains, etc – need to be cleverer
  - ping mesh won’t detect topology
  - Embeddings, layer 2 segments etc
Challenges #3

- Censorship isn’t binary (any more)
  - Partly as DPI doesn’t work when most stuff is crypted (TLS/QUIC)
  - Lots of in-flight packet modification near edge
  - Where people go via cache/proxy/loadbalancer
  - Or where service has a plain (IM/zoom/teams/skype/jitsi mixers) hub
Challenges #4

- Adversaries to measurement
- Inject false responses
- Deep six your measurement traffic
- How do they know?
  - Flow signatures….subtle (ML based sometimes)
  - Sometimes just look at very simple things is best
  - Packet header fields (if plain)
Challenges #5

• Care of ethics (negative impact on performance & privacy)
• Some viewpoints are not safe to use… and may endanger others –
  • see this essential reading:
    Ethical Concerns for Censorship Measurement
• Your measurement may reduce the performance someone needs (and paid for) – these folks take extreme care not to do that
  https://availability.samknows.com/broadband/
Re-decentralised

• Federated stuff is hard to measure
• Tor, Mastodon, Matrix etc
• Intentionally so (for good reasons)
  • Avoid censorship
  • Avoid state surveillance (e.g. whistleblower or NGO)
  • Avoid untrustworthy systems at all
Conclusions

• See https://conferences.sigcomm.org/imc/2022/paper-access/
  (or any other year 😊)
https://www.codebgp.com/about/
  (recent Greek startup bought by cisco 😊)
https://www.routeviews.org/routeviews/