Transports over UDP (TOU)

IETF96

Tom Herbert <therbert@fb.com>
Motivations

- Hide (encrypt) L4 headers from the network
  - Better security for end users
  - Undo protocol ossification
- Reduce dependency on client OSes
  - OS deployment problems on Android, iOS
  - Security here also
- Disassociated location
  - Cnxs viable across NAT remapping the network
  - Cnxs survive device address change in mobile
Header format

- IP
- UDP
- GUE
- DTLS
- TCP, DCCP, SCTP, ...
Elements

● 7-tuple to match connections
  ○ Similar to RFC6773 (DCCP/UDP)
  ○ Works well with connection UDP sockets

● Session identifier
  ○ 64-bit ID that is unique amongst all TOU connections
  ○ Session identifier negotiation

● Effects on L4 protocol
  ○ Connection lookup changed
  ○ Pseudo header checksum (don’t include addresses)
Relationships

- **SPUD/PLUS**
  - TOU is encapsulation of transport protocols
  - Signaling to network could be in GUE

- **QUIC**
  - Goal of TOU is to leverage existing L4 protocols
  - Layering using existing security, encapsulation

- **nvo3**
  - TOU is L4/UDP encapsulation
  - GUE encapsulates for IP protocol number
Status

- draft-herbert-transports-over-udp-01
- Initial patches posted to Linux net-dev (basic TCP/UDP encapsulation)
- Client development underway (userspace TCP stack)
- IETF interest?