Multicast Community Group
TPAC 2022, Vancouver

Jake Holland (Akamai), chair
https://www.w3.org/community/multicast/

Health rules reminder

- Take a covid test each day before attending any in-person event
- Do not come to the meeting if your test is positive
- Masks:
  - must be worn at all times in all common spaces and meeting rooms
  - must cover the nose and mouth
  - can be removed only as necessary to consume food and beverages (Food forbidden in meeting rooms and only allowed in the dedicated space)
  - must be absolutely worn while speaking
- Find all the rules at: https://www.w3.org/2022/09/TPAC/health

W3C Expectations

- This group operates under W3C Code of Ethics and Professional Conduct
  - We're all passionate about improving the Web, but let's all keep the conversations cordial and professional.

- The group operates under the Community and Business Group Process
  - W3C seeks organizational licensing commitments under the W3C Community Contributor License Agreement (CLA). When people request to participate without representing their organization's legal interests, W3C will in general approve those requests for this group with the following understanding: W3C will seek and expect an organizational commitment under the CLA starting with the individual's first request to make a contribution to a group Deliverable.

TPAC meeting tips

- To enter the speaker queue, either
  - ‘Raise your hand’ using the control in the Zoom interface
  - Or ask for queue using your Zoom mic.
  - Or ask for queue using the deck mics on site.
  - Or q+ on https://irc.w3.org/?channels=%23multicast
- Please mute if you are not actively speaking.
- Please use headphones when speaking to minimize echo.
- The first time you speak, please state your full name and affiliation.

Agenda

- Intro (5m)
  - Welcome, Agenda-bash
- Multicast Community Group (25m)
  - Mission, Goals, Motivation: 15m
  - Recent work: 10m
- Discussion (30m)
  - Questions, Comments, Feedback

Multicast CG

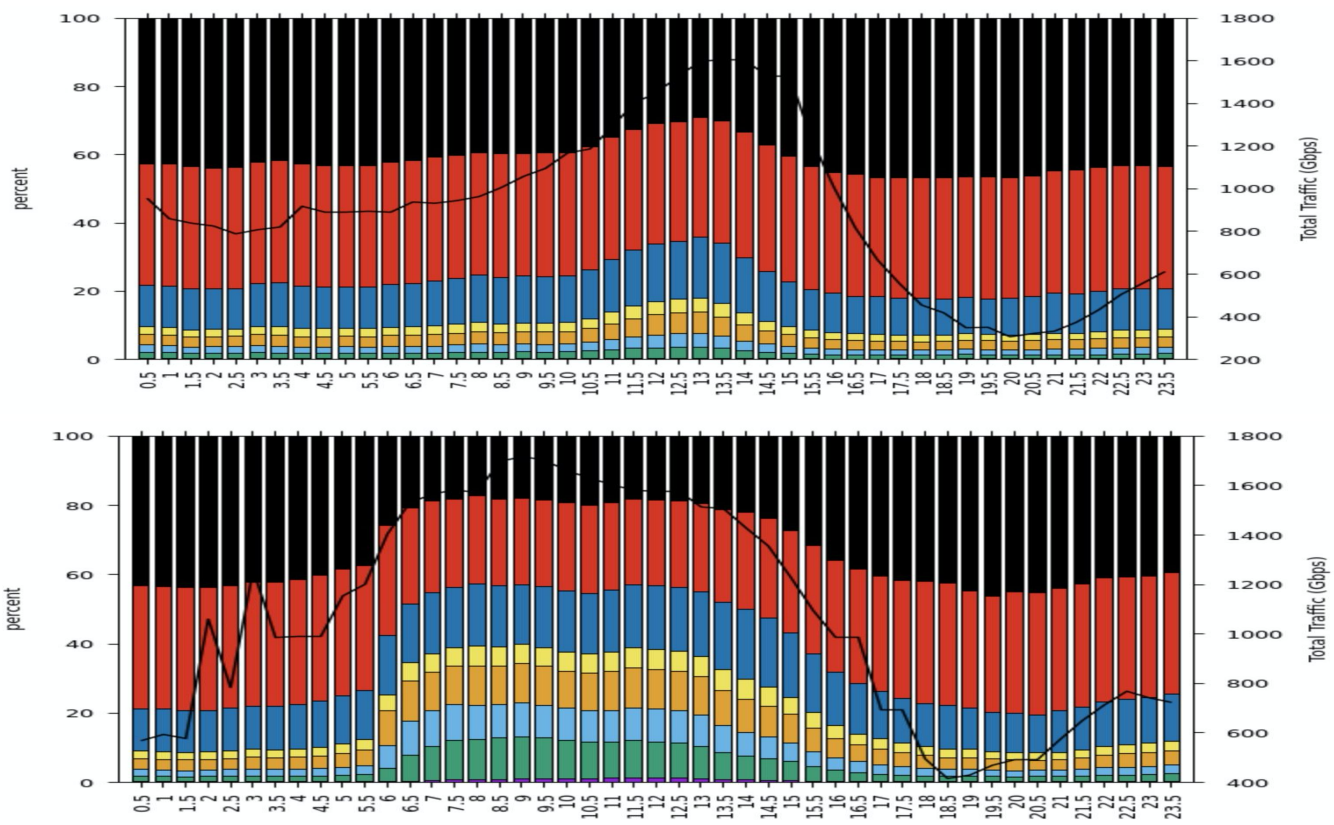
Mission:

Enable multicast IP transport for web traffic to efficiently solve scalability problems in networking and web operations.

https://w3c.github.io/multicast-cg/multicast-cg-charter.html

Goal: get browsers to receive multicast, maintaining web security requirements.

Motivation: Impact of Peaks



Normal traffic day
vs.
Peak traffic day

Goodput of 100KB+ objects
(Histograms each half-hour)

Motivation: Peak Traffic Days

- Peaks come from **popular content**
- **Popular content** = same bits to many people
  - Live sports
  - Popular VOD (Squid Game, Game of Thrones, etc.)
  - Popular Downloads (IOS, Patch Tuesday, Fortnite, Call of Duty)
- **Higher** actual traffic **demand** (not just shifting between services)
- Networks strained ~10-30x/year

Motivation: Peak Traffic Days

- Peaks come from **popular content**
- **Popular content** = same bits to many people
  - Live sports
  - Popular VOD (Squid Game, Game of Thrones, etc.)
  - Popular Downloads (IOS, Patch Tuesday, Fortnite, Call of Duty)

= mostly web traffic & smart tvs

- More actual traffic demand (not just shifting between services)
- Networks strained ~10-30x/year

Motivation: Global Network Efficiency

- Climate Impact
  - Internet=3.7%* of global carbon footprint (2019 estimate)
    - 1% of total global footprint is internet video (300m tonnes)
      - ~15-25% addressable with multicast
      - (does not include broadcast in transition to IP)
    - 24m tonnes from video games (chiefly downloads)
    - Wide multicast ~4x better than stopping crypto proof-of-work
- Cost of delivery & services
  - Network capital costs driven by peak load
  - Power needs/provider costs scale with traffic volume
  - Lower costs + competition => lower price for users

* “Why your internet habits are not as clean as you think”, 2020-03-05, BBC

(Extra Background Resources w/ Motivation)

- APNIC Blog Post
- IETF 111 Web Multicast Bar Bof (slides)
- IETF 112 secdispatch (slides)

Recent Proposal: Multicast Extensions for QUIC

- Protocol Specification
  draft-jholland-quic-multicast
- Security Model
  draft-krose-multicast-security
- Demo implementation in very early days:
  aioquic fork

QUIC Multicast: Basic Operation

- Source-Specific IP Multicast for some server --> client data
- Anchored on the unicast connection
  - Frames from multicast channels could equally have been sent unicast
  - No special restrictions on unicast connection
- Server-driven (with client consent)
  - Server MAY ask client to join channels (via extension frames in the draft)
  - Client MAY join as requested
- Client provides limits (for congestion control as in RFC 8085)
  - Aggregate Max Rate
  - Max Channel Count
- Client ACKs over unicast
  - per-channel packet number space
  - similar to multipath (w/multiple packet number spaces)

QUIC Multicast: Protocol Extensions

- Transport Parameters
  - declare multicast support + client initial limits
- New Extension Frames
  - Server -> Client
    - Channel lifetime & static properties: **MC_ANNOUNCE**, **MC_RETIRE**
    - Key rotation for encryption: **MC_KEY**
    - Requests of client's channel state: **MC_JOIN**, **MC_LEAVE**
    - Integrity guarantees: **MC_INTEGRITY**
  - Client -> Server
    - Report channel join status: **MC_STATE**
    - Report packets received: **MC_ACK**
    - Congestion control limits: **MC_LIMITS**

H3 Capabilities

- Response linked to request, so origin policy applies
- Server Push
  - unicast push-promises referring to streams sent on multicast channels
- Webtransport Server-initiated streams
  - unicast requesting stream id

Has unicast overhead, could be mitigated in future extensions
(e.g. a stream id in response header instead of client’s req stream id)

QUIC Multicast: Security Characteristics

- Symmetric Keys shared across many clients for multicast traffic
  - Content presumed discoverable for broadcast events
  - Decoupled from a destination IP
- IGMP/MLD (network join) = new information in local network
  - Key question: **under what conditions is this safe?**
    - Mitigation: disable in enhanced privacy mode
  - **Threat model gap?**
    - Literature on confidentiality focuses on private/personal info
- Integrity protection anchored in secure unicast connection