Web Multicast

Side Meeting, IETF 111
Jake Holland
Outline

● Intro/Agenda-bash
  ○ Recording? (Seeking active consent from participants)
  ○ Note Well
● Why (~15m)
● How (slides included--brief skim, in favor of discussion time)
● Discussion
IETF Note Well

This is a reminder of IETF policies in effect on various topics such as patents or code of conduct. It is only meant to point you in the right direction. Exceptions may apply. The IETF's patent policy and the definition of an IETF "contribution" and "participation" are set forth in BCP 79; please read it carefully.

- By participating in the IETF, you agree to follow IETF processes and policies.
- If you are aware that any IETF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion.
- As a participant in or attendee to any IETF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public.
- Personal information that you provide to IETF will be handled in accordance with the IETF Privacy Statement.
- As a participant or attendee, you agree to work respectfully with other participants; please contact the ombudsteam (https://www.ietf.org/contact/ombudsteam/) if you have questions or concerns about this.

Definitive information is in the documents listed below and other IETF BCPs. For advice, please talk to WG chairs or ADs:

- [BCP 9](https://www.ietf.org/rfc/rfc2026.txt) (Internet Standards Process)
- [BCP 25](https://www.ietf.org/rfc/rfc4216.txt) (Working Group processes)
- [BCP 25](https://www.ietf.org/rfc/rfc4216.txt) (Anti-Harassment Procedures)
- [BCP 25](https://www.ietf.org/rfc/rfc4216.txt) (Patents, Participation)
- [BCP 54](https://www.ietf.org/rfc/rfc3976.txt) (Code of Conduct)
- [BCP 78](https://www.ietf.org/rfc/rfc4255.txt) (Copyright)
- [BCP 79](https://www.ietf.org/rfc/rfc4255.txt) (Patents, Participation)
- [https://www.ietf.org/privacy-policy/](https://www.ietf.org/privacy-policy/) (Privacy Policy)
Why: User Experience (Effects of Congestion)

Observed goodput to large ISP by Time of Day (normal-traffic day, 100KB+ objects)
Observed goodput to same ISP* by Time of Day (high-traffic day, 100KB+ objects)

* NB: effect present in most ISPs, but not always this clear a signal.

By eye: ~½ the goodput for a 9-hour peak
Key Problem Solved: Access Network Congestion

![Cable Network Diagram](https://commons.wikimedia.org/w/index.php?curid=61793561)

- Problematic Congestion
- Deepest Useful Caches

Cable Network Diagram By Saub09 at English Wikibooks, CC BY-SA 2.5,
https://commons.wikimedia.org/w/index.php?curid=61793561
Broadcast link capabilities can be leveraged by multicast? (up to?)

- Fiber (GPON, etc): yes (~3k/ONT)
- Cable: yes (~2k/service group)
- DSL: depends (~1.5k/chassis)
  - PPP-based deployments can’t use broadcast
  - Helps uplink bandwidth, but similar power usage
- Ethernet: usually (~2k in enterprise/university/apartment networks)
  - Needs L2 snooping & replication capability--usually there, not always
- 3G & 4G: sort-of (with eMBMS: ~3k/tower, special signaling)
- 5G: yes (with Xcast: ~3k/tower?, normal signaling?)
- ATSC: maybe one day (~10-100k/antenna, will need special signaling)

(* Wifi in homes may need updates--solutions exist, deployment spotty)
Other Effects

● Climate Impact
  ○ Internet=$3.7\%$* of carbon footprint globally (as much as air travel!)

● 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
Why: Avoidable Traffic (game/os downloads - new releases)

Under 100 streams: >40% reduction in peak load to ISP (high-traffic day)
Avoidable Traffic (game/os downloads - normal)

Under 100 streams: >8*% reduction overall traffic to ISP (normal day)

* lower bound. We think there's much more
Why: Avoidable Traffic (web video)

1 stream, >15% reduction in peak load to ISP (popular sport event day)
How: Browser API Proposal (original)

Multicast Receive **API** (WICG)
**AMBI** (IETF)
**DORMS** (IETF)
**CBACC** (IETF)

Javascript

```javascript
var mr = new MulticastReceiver(
  source='198.51.100.10',
  group='232.1.1.1', port=5001,
  dorms='dorms.example.com');
reader=mr.readable.getReader();
async function readData() { let
  { done, value } = await reader.read();
  mr.join()
}
```

IETF 106 mboned (slides)
How: AMBI (Asymmetric Manifest-Based Integrity)

Sender

Multicast Data
UDP

Packet1
Packet2
Packet3

Fanout & Forwarding
(Tunneling, PIM/BIER, IGMP/MLD)

Hash(Packet1)
Hash(Packet2)
Hash(Packet3)

Manifests (Authenticated)
TLS/DTLS

CDN/Elastic Cloud

1-3% of data (TLS/DTLS):
Unicast-Authenticated Manifests

Receivers
Packet without hash:
=> spoofed/corrupt
Hash without Packet:
=> loss
1. **Explicit** DORMS hostname from secure context (implicit ok iff DNSSEC--mostly for network)
2. CORS request to DORMS server (if not same origin)
3. DORMS has **AMBI** data with:
   a. integrity url
   b. Hash algorithm/params
4. Integrity stream over TLS/DTLS

---

**Javascript**

```javascript
var mr = new MulticastReceiver(
  source='198.51.100.10',
  group='232.1.1.1', port=5001,
  dorms='dorms.example.com');
reader=mr.readable.getReader();
async function readData() { let
  { done, value } = await reader.read();
  mr.join();
}
```

---

**IETF 106 mboned (slides)**
How: DORMS+AMBI/CBACC

MC link
PIM RPF

@Ingest:
- AMBI: Authentic?

DNS SRV:
_dorms._tcp.<1ecruoS>.in6.arpa=d1.ex.com
_dorms._tcp.<2ecruoS>.in6.arpa=d2.ex.com

d1.ex.com:
- CB: Size=X
- AMBI: Auth

d2.ex.com:
- CB: Size=Y
- AMBI: Auth

@Ingest:
- AMBI: Authentic?

@bottleneck:
- AMBI: Authentic?
- CBACC: enough capacity?

@receiver:
- AMBI: Authentic?
- CBACC: small enough?
Early ISP Feedback

- Tentatively Positive
  - Successful Lab Trials with 5 ISPs
    - Cable, Fiber, DSL
  - Some others looking now

- Needs Receivers
  - Web API critical for live video (esp: Smart TVs, mobile)
  - Web nice-to-have for Game/OS/software downloaders

- Needs Content
  - Customer talks ongoing, also tentatively positive
  - Prototypes with real customer data used for trial evals
Early Web Feedback

- **Security:**
  - MUST require encryption for a new web API
    - Not visible to those without keys (in spite of one-to-many keys)
    - Makes on-path observation an active attack instead of passive

- **Privacy:**
  - Next-hop join exposure to LAN is fundamentally different from TLS/unicast
    - Addressable by other means? (e.g. random mac?)
    - Precedent? Note openscreen exposes similar info
  - Upstream benefits to privacy--indistinguishably shared destination IP

- **Suitability:**
  - Mixed-content experiments not welcome
  - Needs wider consensus & review (after adding encryption) before possibility to deem this non-mixed, due to fundamental differences with unicast/TLS

See Chromium net-dev thread
Next Steps

● Try using QUIC framing & Alt-svc instead of web-app join: 
  draft-pardue-quic-http-mcast as starting point
  ○ Adds packet encryption (shared keys)
  ○ Adds object-level payload collating
  ○ Implementation starting point: nghq (add AMBI/strong packet auth)

● Get consensus on requirements: draft-krose-multicast-security

● Get a good IETF venue
  ○ Madrid BoF? QUIC? WebTransport?