Multicast to the Browser

Status Update @2021-07, IETF 111 mboned

Jake Holland

draft-ietf-mboned-dorms

draft-ietf-mboned-cbacc

draft-ietf-mboned-ambi

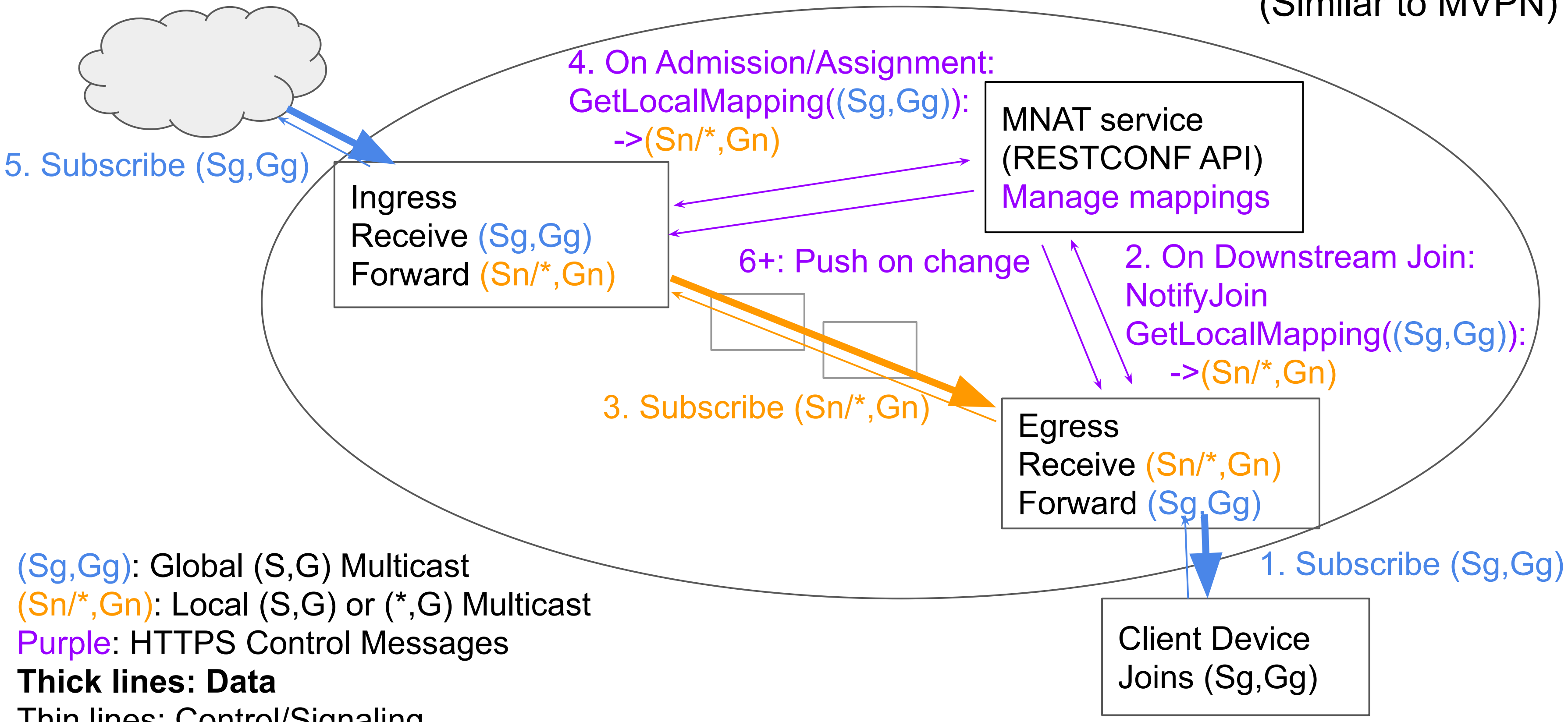
(draft-ietf-mboned-mnat)

Outline

- Context Reminders (brief overviews)
- Development & Outreach status
- Doc status & next steps

Context: MNAT: (draft-ietf-mboned-mnat)

(Similar to MVPN)



4. On Admission/Assignment:
GetLocalMapping((Sg,Gg)):
->(Sn/*,Gn)

MNAT service
(RESTCONF API)
Manage mappings

5. Subscribe (Sg,Gg)

Ingress
Receive (Sg,Gg)
Forward (Sn/*,Gn)

6+: Push on change

2. On Downstream Join:
NotifyJoin
GetLocalMapping((Sg,Gg)):
->(Sn/*,Gn)

3. Subscribe (Sn/*,Gn)

Egress
Receive (Sn/*,Gn)
Forward (Sg,Gg)

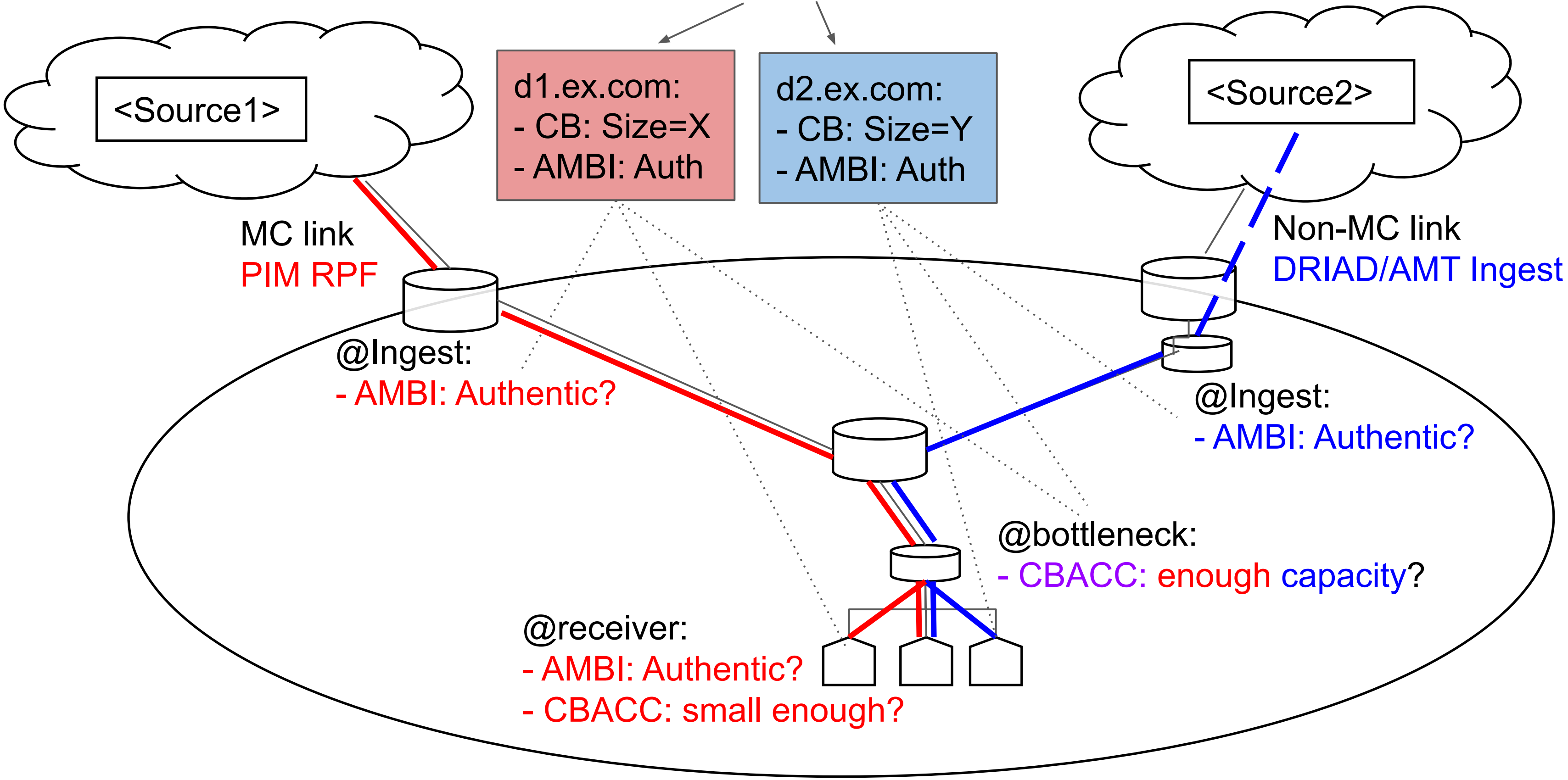
1. Subscribe (Sg,Gg)

Client Device
Joins (Sg,Gg)

(Sg,Gg): Global (S,G) Multicast
(Sn/*,Gn): Local (S,G) or (*,G) Multicast
Purple: HTTPS Control Messages
Thick lines: Data
Thin lines: Control/Signaling

Context: DORMS+AMBI/CBACC

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

<Source1>

<Source2>

MC link
PIM RPF

Non-MC link
DRIAD/AMT Ingest

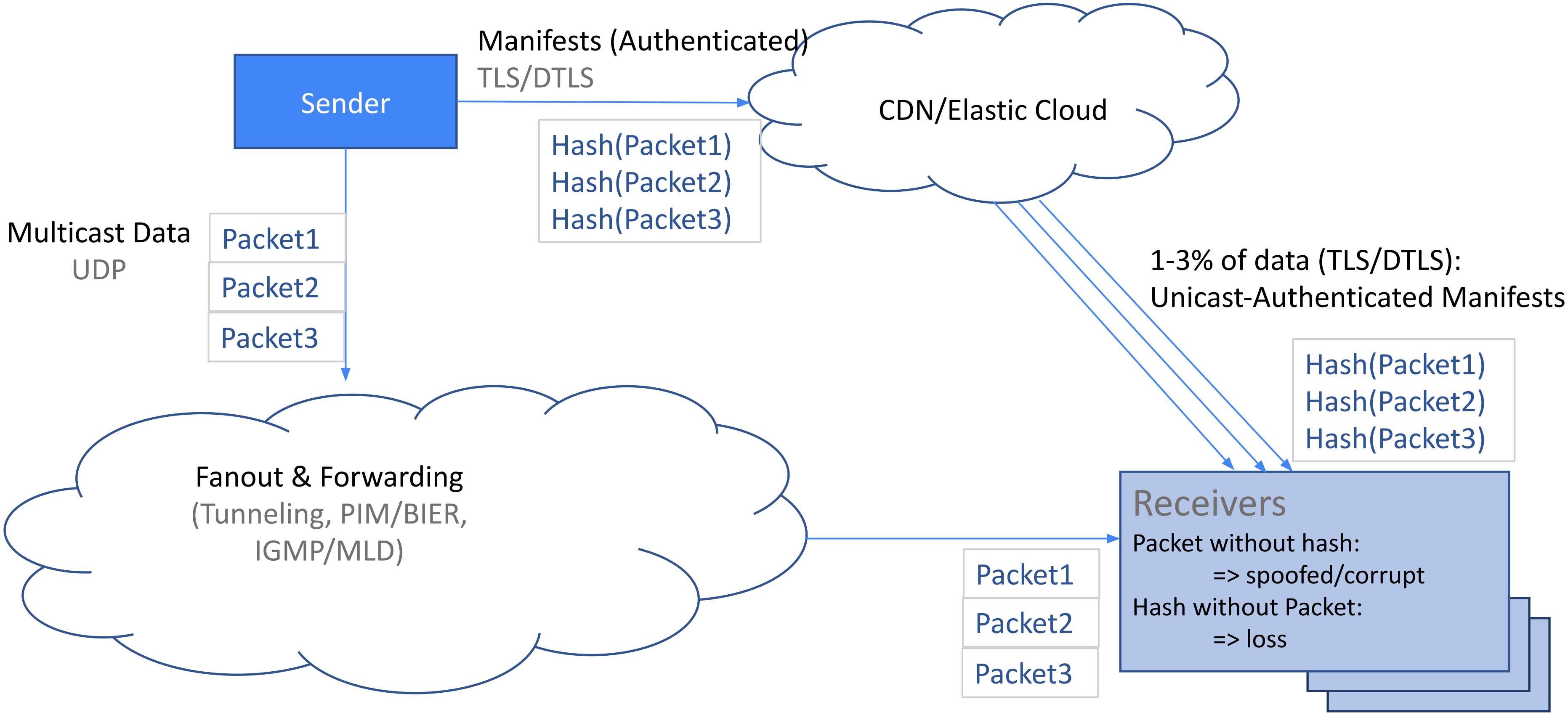
@Ingest:
- AMBI: Authentic?

@Ingest:
- AMBI: Authentic?

@bottleneck:
- CBACC: enough capacity?

@receiver:
- AMBI: Authentic?
- CBACC: small enough?

Context: AMBI (Asymmetric Manifest-Based Integrity)



Sender

Manifests (Authenticated)
TLS/DTLS

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

CDN/Elastic Cloud

Multicast Data
UDP

Packet1
Packet2
Packet3

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

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

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

Packet1
Packet2
Packet3

Receivers

Packet without hash:
=> spoofed/corrupt

Hash without Packet:
=> loss

Trial Status

- Finished first round of trials: ingest with multicast-ingest-platform
    - Attempted 5 ISP labs
        - mix of fiber, cable, DSL, with Wi-Fi client, all ISP gear. 1 thru production network.
    - Succeeded 3
        - But with manual OS MNAT-egress config on 2
            - Real production will need client or CPE integration
    - Deferred 1 (required MNAT for Nokia OLT workaround, declined manual setup test)
    - Failed 1 (Calix gear roadblock unsolved)
- Talks continuing with more ISPs interested in follow-up
- Talks continuing with content customers interested in follow-up

Conclusion: cautious optimism.
- tentatively: will build iff major buy-in. pending ongoing talks

Browser Implementation: Early 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

Browser Implementation Status

- Rejected as experiment in Chromium upstream
- Carrying a fork until further notice.
    - Tracking dev and stable releases
    - Linux (ubuntu) binaries available: https://github.com/GrumpyOldTroll/chromium_fork
- Addressing feedback
    - Starting Web consensus journey
        - draft-krose-multicast-security
        - Formed W3C Multicast Community Group to incubate
        - Side meeting yesterday: invited webtransport
    - Encryption next steps
        - Either QUIC-like with draft-pardue-quic-http-mcast or an AMBI extension

W3C Engagement

- Community Group formed in June, meeting monthly starting August
  https://www.w3.org/community/multicast/
  https://github.com/w3c/multicast-cg
- Chartered to incubate Web APIs supporting multicast
  - Phase 1: attempting web transport

Doc Status

- DORMS & CBACC early Yang Doctor Review completed
  - Fixes in latest draft
- **DORMS ready for last call?**
- Substantial AMBI updates:
  - Added Threat Model section
  - Added TLV space to manifest
    - Extension target for passing encryption keys & parameters
- Some TBDs fixed in CBACC, still some remaining work
  - Priority still not solved
- MNAT
  - Not updated yet.
  - Will incorporate some YANG principles feedback from DORMS/CBACC
  - Helpful diagram from Kyle Rose in next version
- Implementations not yet updated to latest