Hybrid Two-step telemetry collection method

draft-mirsky-ippm-hybrid-two-step

Greg Mirsky
Wang Lingqiang
Guo Zhui
Haoyu Song
Pascal Thubert

IETF-113, March 2022

Protocol Recap

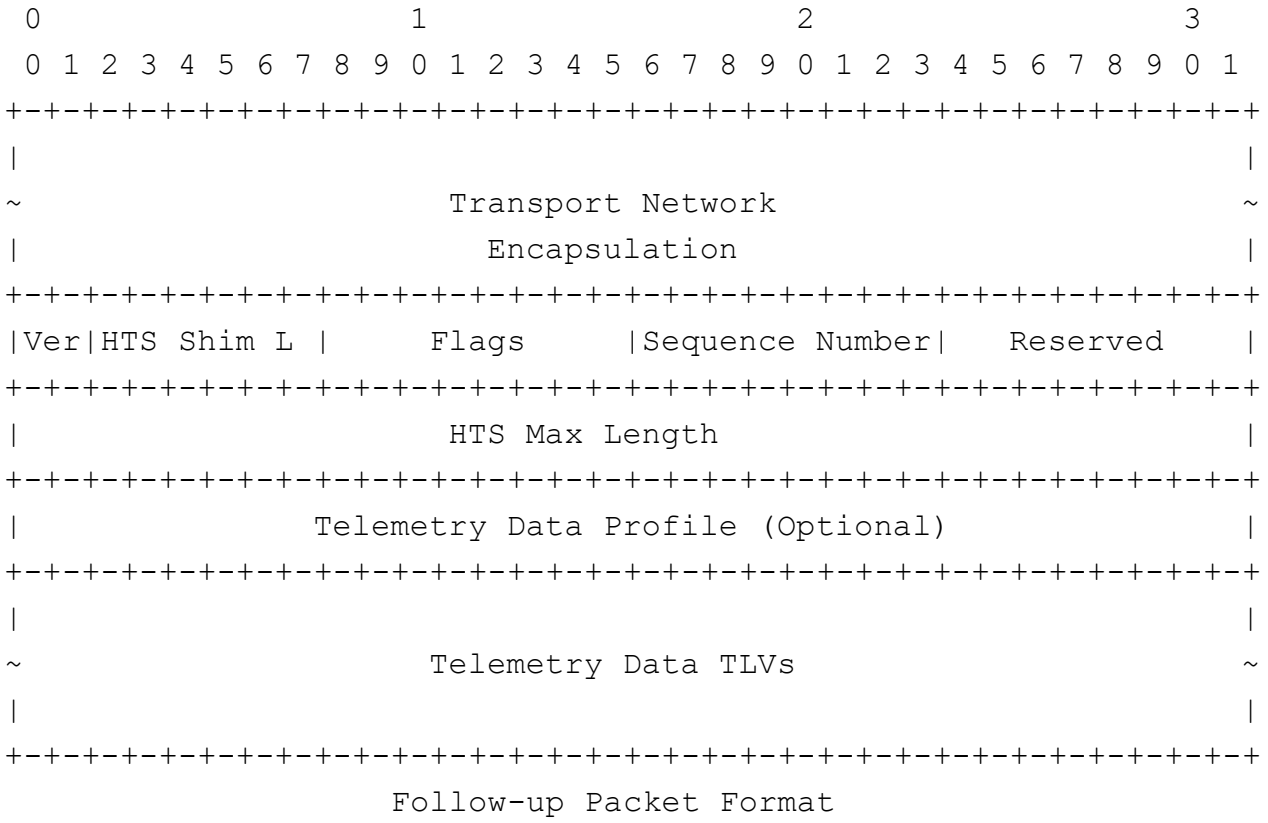
- HTS is a method to collect and transport on-path telemetry information
- HTS can be used for p2p and p2mp cases
- HTS allows for more accurate measurements by separating acts of generating information and its collection and transport
- HTS removes any limits on the amount of telemetry information collected and transported
- HTS supports downstream and upstream modes
- HTS allows for integrity protection of the collected telemetry information

Hybrid Two-step

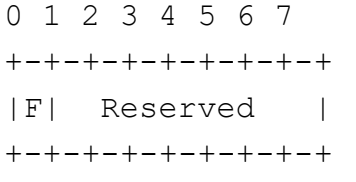
Hybrid Two-step:

- Use a specially constructed message, follow-up message, to collect telemetry information along the way of the data flow packet that triggers information's origination.
- A trigger packet is network layer-specific, and the corresponding follow-up packet uses the same transport network encapsulation.
- The follow-up message originated by the ingress node–The follow-up message is intended to cross the same set of nodes and links as its trigger-packet.
- The follow-up packet may share the same QoS treatment by the transport network, or its QoS may differ. The former is referred to as "in-band", and the latter is out-of-band HTS.
- The follow-up message is terminated by the egress node, thus not leaving the domain.
- Only one outstanding follow-up message may be "in-flight", i.e., one set of telemetry can be held for the next follow-up message.

The Follow-up packet format

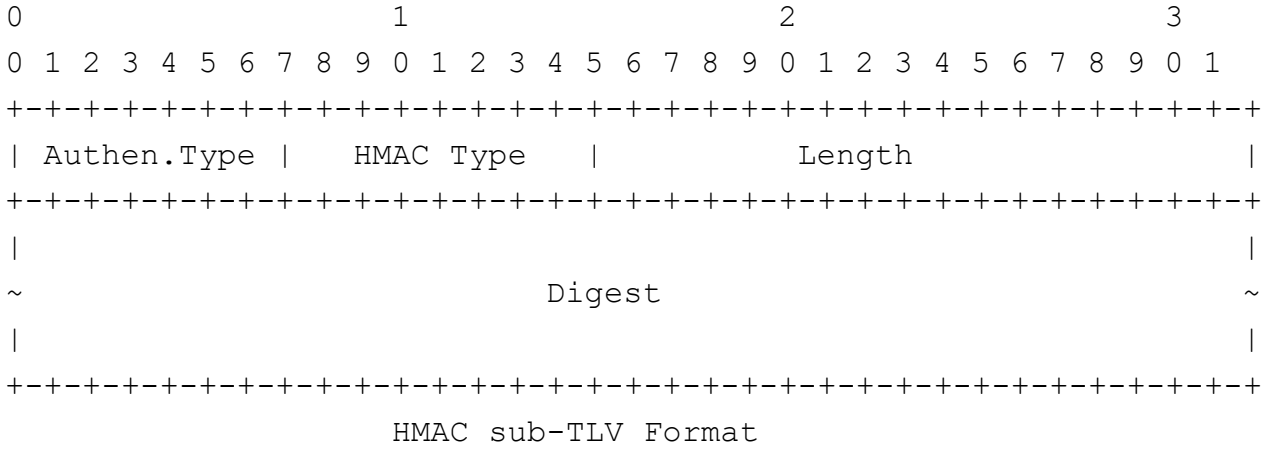


Follow-up Packet Format



Flags Field Format

Authentication in HTS



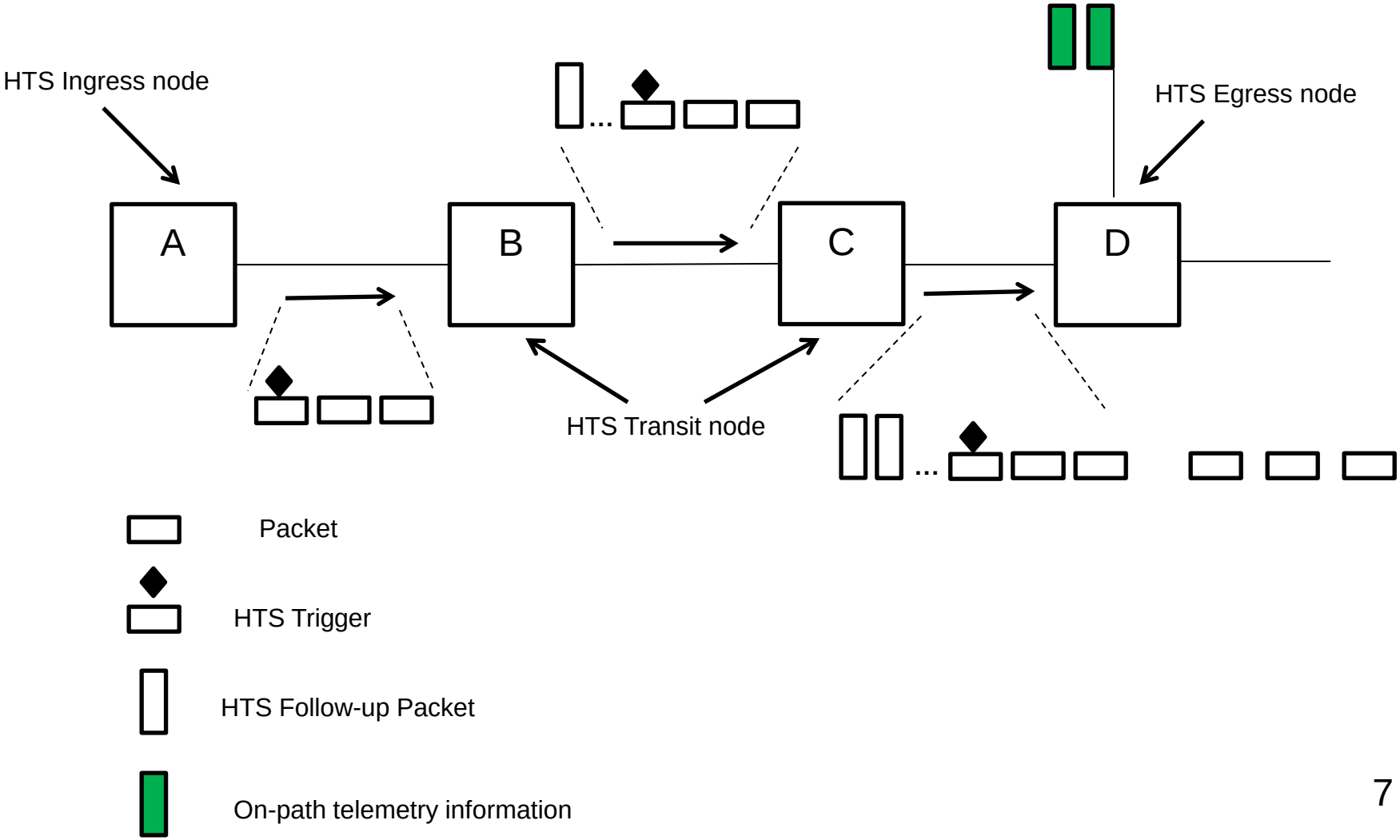
HMAC sub-TLV Format

- Use of HMAC-SHA-256 truncated to 128 bits [RFC4868]
- HMAC is calculated over text as the concatenation of the Sequence Number field of th e Follow-up packet and the preceding data collected in the Telemetry Data TLV
- The digest MUST be truncated to 128 bits and written into the Digest field
- In the HTS authenticated mode, the Authentication sub-TLV MUST be present in each T elemetry Data TLV, i.e., each node independently authenticates data it appends to the HTS Follow-up packet
- HMAC MUST be verified before using any data in the included Telemetry Data TLV
- If HMAC verification fails, the system MUST stop processing corresponding Telemetry Data TLV and notify an operator

IOAM with HTS

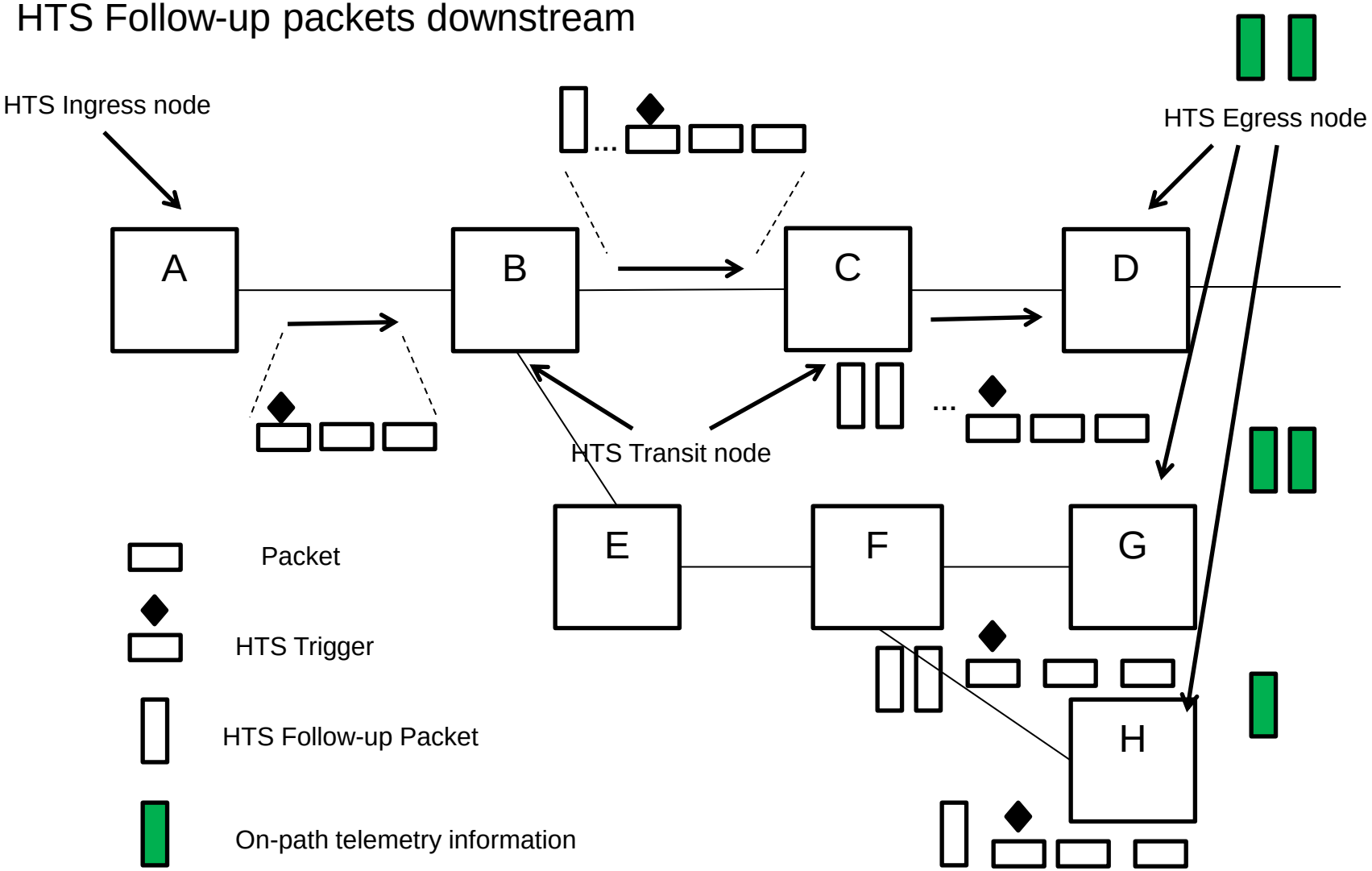
- Using HTS in an IOAM domain is one of the interesting cases.
- A trigger packet includes IOAM Namespace-ID and IOAM-Trace-Type.
- The ingress HTS node copies IOAM Namespace-ID and IOAM-Trace-Type into the follow-up packet's Telemetry Data Profile field.
- IOAM-Trace-Type information defined in [I-D.ietf-ippm-ioam-data] can be used in the Telemetry Data Profile field.

Theory of HTS operation

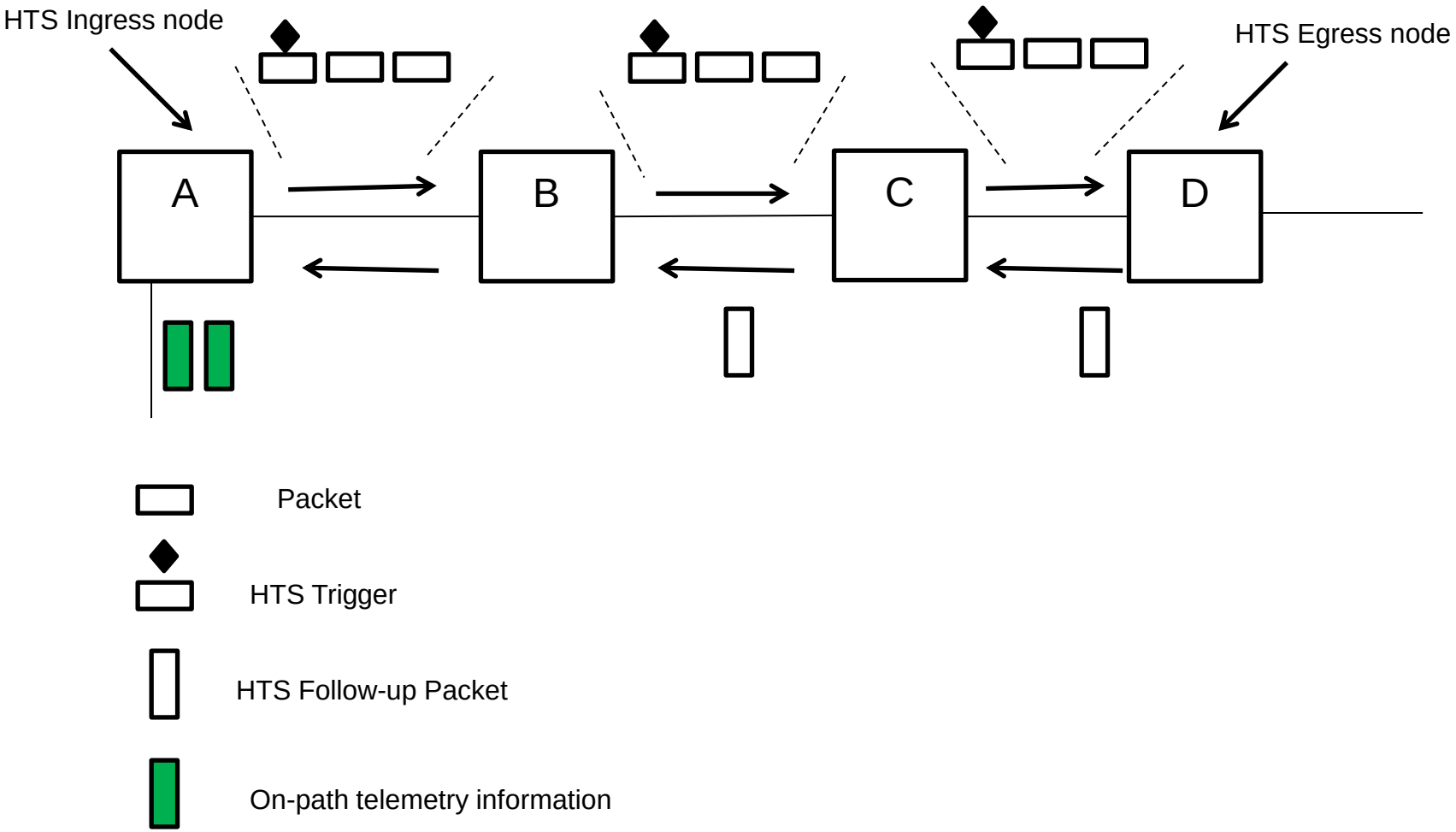


HTS in multicast distribution tree

Branch Node forwards HTS over the first branch and then originates HTS Follow-up packets downstream



Upstreaming HTS



Next steps

- Your comments, suggestions, questions always welcome and greatly appreciated
- WG adoption

Thank you