Service Function Chaining (SFC)

IETF 104
Prague

WG Chairs:
Jim Guichard (jguichard1966@gmail.com)
Joel Halpern (jmh@joelhalpern.com)
Note Well

- This summary is only meant to point you in the right direction, and doesn’t have all the nuances. The IETF’s IPR policy is set forth in BCP 79; please read it carefully.

- **The brief summary:**
  - By participating with the IETF, you agree to follow IETF processes.
  - If you are aware that a contribution of yours (something you write, say, or discuss in any IETF context) is covered by patents or patent applications, you must disclose that fact.
  - You understand that meetings might be recorded, broadcast, photographed, and publicly archived.

For further information, talk to a chair, ask an Area Director, or review the following:
- BCP 9 (on the Internet Standards process)
- BCP 25 (on the Working Group processes)
- BCP 78 (on the IETF Trust)
- BCP 79 (on Intellectual Property Rights in the IETF)
Agenda (Brief)

• Agenda Bashing
• SFC ECN
• SFC OAM
• SFC YANG
• AOB
• Closing
Agenda (Detailed)

• Introduction (WG-chairs) - [10 minutes]
  – Agenda bashing, note-well, (WG-chairs) - [10 minutes]

• Network Service Header (NSH) Explicit Congestion Notification (ECN) Support (Donald Eastlake) - [15 minutes]

• Active OAM for Service Function Chains in Networks (Greg Mirsky) - [15 minutes]

• NSH Encapsulation for In-situ OAM Data (Frank Brockners) - [15 minutes]
Agenda (Detailed) Cont.

• Proof of Transit (Frank Brockners) - [15 minutes]

• SFC Consistency OAM (Ao Ting) - [15 minutes]

• SFC YANG (Ao Ting) - [15 minutes]

• Closing (WG-chairs) - [5 minutes]
WG Status

- [https://datatracker.ietf.org/doc/draft-guichard-spring-nsh-sr/](https://datatracker.ietf.org/doc/draft-guichard-spring-nsh-sr/) presented in SPRING WG and likely to be adopted
- WG has a commitment to work on security improvements but so far only POT work in this space – how do we proceed?
- Specifies a TLV to disseminate a subscriber identifier to upstream SFs
- Inherits the same security considerations from RFC7576 and RFC8300
  - Like any NSH TLV, the information is not leaked outside an administrative domain
- During the review of RFC 8459, security ADs were concerned with the lack of integrity protection mechanism for TLVs
  - The same concern is likely to be raised for this specification
- Should the authors investigate a solution specific to this I-D? e.g.,
  - Generate an EDCSA signature for a subscriber identifier
  - The subscriber identifier + Signature are conveyed in NSH
  - SFC nodes validate the signature using the public keys
- Or ???
- Your feedback is needed!