

# Return Path in SFC OAM

<https://tools.ietf.org/html/draft-ao-sfc-oam-return-path-specified-01>

Ting Ao, Greg Mirsky

# Background

- Use Reply Service Function Path TLV in conjunction with Reply Mode field set to "Reply via Specified Path" in Echo request to control the return path of Echo reply control message

# Update from -00

- SFC Echo request/reply has been introduced (draft-wang-sfc-multi-layer-oam). The draft is now viewed as extension of SFC Echo request/reply protocol.
- Added Security Considerations section

# Security Considerations

Security considerations discussed in [I-D.ietf-sfc-nsh] apply to this document.

In addition, the SFC Return Path extension, defined in this document, may be used for potential "proxying" attacks. For example, an echo request initiator may specify a return path that has a destination different from that of the initiator. But normally, such attacks will not happen in an SFC domain where the initiators and receivers belong to the same domain, as specified in [RFC7665]. Even if the attack happens, in order to prevent using the SFC Return Path extension for proxying any possible attacks, the return path SFP SHOULD have destination to the sender of the echo request, identified in SFC Source TLV [I-D.wang-sfc-multi-layer-oam]. The receiver may drop the echo request when it cannot determine whether the return path SFP has the destination to the initiator. That means, when sending echo request, the sender SHOULD choose a proper source address according to the specified return path SFP to help the receiver to make the decision.

# Next steps

- Comments, questions always welcome and greatly appreciated
- WG adoption?