Network Working Group
Internet-Draft

Prasad Kulangara
Persistent Systems

Intended status: Standards Track
Expires: July 2026

20 January 2026

Universal Tunnel-less SSE Signaling and SD-WAN Direct Switchover (DST) Extension for Spoke-to-Spoke Traffic

draft-kulangara-zero-sse-dst-00

Persistent Systems
Email: prasad_k1@persistent.com

Abstract

This document specifies a universal, tunnel-less mechanism for Secure Service Edge (SSE) steering based on a new SSE Identification Header (SSE-ID). The architecture enables endpoints, OS network stacks, and enterprise SD-WAN edge devices to signal the intent for traffic to be routed to an SSE provider without using GRE or IPsec tunnels.

This document also defines an SD-WAN extension called the Direct Switchover Token (DST). DST provides a vendor-agnostic mechanism enabling SD-WAN spokes to establish direct, encrypted, spoke-to-spoke paths for traffic that does not require SSE inspection. DST is issued by a central controller after initial packets reach a hub or the controller and after evaluating policy and SSE requirements.

Additionally, this document introduces (a) a Participating ISP routing model using an SSE-Only Public Pool (SOPP) and an SSE POP ID (SPID) to locate and route to SSE edges on SSE-enabled circuits, and (b) a Merger & Acquisition (M&A) access mode that allows two enterprises to access resources via the SSE cloud using Enterprise IDs; in this mode, traffic is spliced inside the SSE fabric by EID, with address-domain isolation to avoid IP conflicts.

Together, SSE-ID and DST—augmented with SOPP/SPID and M&A mode—provide a unified, interoperable, and tunnel-less architecture for SSE integration, SD-WAN optimization, inter-domain routing, and enterprise-to-enterprise access.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at https://www.ietf.org/1id-abstracts.html

The list of Internet-Draft Shadow Directories can be accessed at https://www.ietf.org/shadow.html

Copyright Notice

Table of Contents

1. Introduction

Current Secure Service Edge (SSE) deployments rely heavily on GRE or IPsec tunnels between enterprise edge devices and cloud SSE providers. This design introduces operational overhead, lacks flexibility for mobile endpoints, creates path inefficiencies, and increases onboarding complexity and cost.

To address these issues, this document defines a universal and tunnel-less mechanism for SSE steering using a new SSE Identification Header (SSE-ID). The SSE-ID enables endpoints, operating systems, and SD-WAN spokes to signal traffic that must be routed to a designated SSE provider. The SSE-ID contains identity and policy metadata, including an Enterprise ID, Tenant ID, Application ID, and optional attributes.

This document also defines an SD-WAN extension, the Direct Switchover Token (DST). DST provides vendor-agnostic authorization for SD-WAN

spokes to migrate traffic from hub-routed to direct spoke-to-spoke encrypted paths when SSE inspection is not required. DST integrates with the SSE-ID identity and policy model.

Two deployment extensions are included. First, a Participating ISP model defines how ISPs may carry an SSE-Only Public Pool (SOPP) and use an SSE POP ID (SPID) to locate participating SSE edges; the SOPP is exclusively routed across SSE-enabled circuits, and traffic from the SSE provider to the public Internet does not originate from this pool. Second, a Merger & Acquisition (M&A) access mode allows two enterprises to interconnect via SSE using Enterprise IDs; the SSE cloud splices traffic using those identities and isolates address domains to avoid IP conflicts.

2. Terminology

SSE: Secure Service Edge.
SSE-ID: SSE Identification Header.
EID: IANA-assigned Enterprise ID.
TID: Tenant ID.
AID: Application ID.
DST: Direct Switchover Token.
Spoke: SD-WAN edge device.
Hub: Central SD-WAN aggregation or policy node.
Controller: Central policy engine.
Participating ISP: An ISP that implements SOPP/SPID handling as in Section 10.
SOPP: SSE-Only Public Pool. A provider-allocated prefix or set of prefixes routed only across SSE-enabled circuits and not used for SSE egress to the public Internet.
SPID: SSE POP ID. A unique identifier for an SSE Point of Presence.
M&A Access Mode: A policy mode enabling cross-enterprise access via SSE, with identity-spliced traffic and address-domain isolation.
Peer-EID: The Enterprise ID of the remote enterprise in M&A mode.
ADID: Address-Domain ID. An identifier that scopes overlapping IP spaces per enterprise within the SSE fabric.

3. Problem Statement and Motivation

SSE adoption is increasing across enterprises. However, steering traffic to SSE providers still relies heavily on tunnel-based architectures that are operationally complex, inefficient for endpoints, and limited in mobility scenarios.

Meanwhile, SD-WAN direct routing remains vendor-specific and lacks a standard method for secure, authorized spoke-to-spoke direct paths.

In addition, enterprises struggle with (a) consistent, policy-based routing behavior across ISP underlays toward SSE edges, and (b) seamless, low-friction interconnection during mergers and acquisitions when address spaces overlap.

This specification addresses all three issues by defining:
* A universal, tunnel-less SSE signaling mechanism (SSE-ID).
* A vendor-neutral SD-WAN extension for direct spoke-to-spoke communication (DST).
* A Participating ISP model for routing to SSE edges using SOPP/SPID.
* An M&A access mode with identity-based splicing and address-domain isolation to avoid IP conflicts.

4. Tunnel-less SSE Architecture

The tunnel-less SSE architecture uses the SSE-ID header to signal enterprise identity and SSE routing intent. Endpoints insert SSE-ID metadata into flows that require SSE routing. SD-WAN spokes or enterprise gateways detect SSE-ID and steer traffic based on policy.

SSE providers use the SSE-ID to authenticate and authorize flows.

5. SSE Identification Header (SSE-ID)

The SSE-ID header contains:
* Version, Flags, Header Length.
* Enterprise ID (EID).
* Tenant ID (TID).
* Application ID (AID).
* Nonce/Flow Token.
* Signature or MAC.
* Optional TLVs (SSE provider target, device class, geofence, etc.).

New TLVs introduced by this document (see also Section 15):
* SSE-POP-ID (SPID) TLV: carries a provider-scoped or global ID that identifies the target SSE POP for admission and localization.
* SOPP-Indicator TLV: indicates that the packet's next-hop resolution is expected via the SOPP routing context on SSE-enabled circuits.
* Access-Mode TLV: indicates M&A when set accordingly.
* Peer-Enterprise-ID TLV: carries a Peer-EID for cross-enterprise access in M&A mode.
* Address-Domain-ID (ADID) TLV: indicates the address domain associated with the originating enterprise to resolve IP overlaps.

6. SSE-ID Carriage Methods

The SSE-ID may be carried through:
* IPv6 Destination Options.
* TCP Options.
* QUIC Transport Parameters.
* HTTP Structured Header.
* UDP First-Packet Shim (fallback for NAT environments).

When present, SPID, SOPP-Indicator, Access-Mode, Peer-EID, and ADID TLVs MUST be preserved end-to-end to enable the behaviors in Sections 10 and 11.

7. Onboarding and Authorization

Enterprises obtain an Enterprise ID from IANA. Devices are provisioned with credentials via enterprise onboarding systems. Endpoints sign the SSE-ID. SSE providers validate signatures and apply policy. For M&A mode, both enterprises authorize the relationship by exchanging trust anchors and policy scopes at the SSE control plane.

8. Data Plane Operation

An endpoint inserts SSE-ID metadata into outbound flows that require SSE. SD-WAN devices detect the SSE-ID and forward traffic to the nearest SSE POP. SSE POPs validate authenticity and enforce policy.

When SOPP-Indicator is set, participating ISPs apply the SOPP routing policy (Section 10). When Access-Mode is M&A, SSE POPs splice traffic by EID and enforce ADID isolation (Section 11).

9. SD-WAN Direct Switchover Extension (DST)

9.1 DST Motivation

Certain flows, such as internal application access, VOIP, OT communication, or branch-to-branch data transfer, do not require SSE inspection. Today, spoke-to-spoke direct path features are proprietary to individual SD-WAN vendors. DST defines a universal, multi-vendor mechanism for authorizing spoke-to-spoke direct routing.

9.2 DST Architecture

* Initial packets of a flow reach the Hub or are exported as metadata.
* The Controller evaluates enterprise policy and SSE-ID.
* If SSE inspection is not required, the Controller issues a DST to both spokes.
* Both spokes validate and establish a direct encrypted adjacency using a supported suite (IKEv2, DTLS, QUIC, SRv6-TE).

9.3 DST Format

DST includes:
* Version, Flags, Token ID.
* Issue Time and Expiry.
* Source and Destination Spoke IDs.
* Traffic Selectors.
* Crypto Suite ID.
* Optional TLVs: App Class, Region, Posture Level, QoS Class.
* Controller Signature.

9.4 Controller Procedures

The Controller:
* Receives first-packet metadata.
* Determines whether SSE-ID requires SSE.
* Issues DST if direct path is allowed.
* Supports revocation and rekey.

9.5 Spoke Behavior

Spokes:
* Validate DST signature, time, and policy.
* Establish secure adjacency.
* Migrate flow to direct path.
* Revert to hub if adjacency fails.

9.6 Interaction Between DST and SSE-ID

* If SSE-ID Flags indicate "Require SSE", DST MUST NOT be issued.
* DST is only used for flows classified as "SSE not required".
* Identity and policy fields from SSE-ID may inform DST decisions.

10. Participating ISP Routing with SOPP and SPID

10.1 Concept and Scope

Participating ISPs can provide deterministic and policy-aligned reachability to SSE edges by routing a dedicated SSE-Only Public Pool (SOPP) of addresses and honoring an SSE POP ID (SPID) locator. SOPP routes exist only on SSE-enabled circuits and within participating ISP/partner domains. They are not used by the SSE provider for egress toward public Internet destinations.

10.2 SOPP Semantics and Constraints

* SOPP is a dedicated public IP prefix or set of prefixes assigned to the SSE provider for service ingress from enterprises and participating ISPs.
* Packets destined to SOPP addresses terminate at SSE POPs; they MUST NOT be sourced by the SSE provider for outgoing Internet traffic.
* SOPP routes MUST be advertised and accepted only over SSE-enabled circuits and participating ISP interconnects.
* Non-participating networks SHOULD NOT receive SOPP advertisements.

10.3 SPID: SSE POP Identification

* SPID uniquely identifies an SSE POP. It MAY be globally unique or

provider-scoped.
* SPID can guide selection among multiple POPs when several SOPP prefixes are available; it can also serve as a hint for SLA, policy region, or regulatory constraints.

10.4 Routing and Policy Rules for Participating ISPs

* When SOPP-Indicator TLV is present, participating ISPs SHOULD steer traffic to the nearest or policy-compliant SOPP next-hop derived from their routing system and MAY use SPID for tie-breaking or region enforcement.
* SOPP routes MUST NOT be used by the SSE provider to originate traffic to the public Internet; such egress MUST use normal (non-SOPP) provider addresses.
* Filtering policies MUST ensure SOPP leakage to the general Internet does not occur. Route-policy SHOULD tag SOPP with a distinctive community or attribute (out of scope for this document).
* ISPs MAY participate without inspecting SSE-ID payloads if they rely solely on destination SOPP reachability. If SSE-ID is available, SPID can augment selection.

10.5 Operational Guidance

* Capacity planning and DDoS controls SHOULD be applied at SOPP borders.
* Outage handling SHOULD prefer alternate SOPP paths, then revert to non-participating default routing where enterprise edges steer directly to SSE as needed.

11. Enterprise-to-Enterprise (M&A) Access Mode

11.1 Objectives and Use Cases

M&A Access Mode enables two enterprises to interconnect via SSE without renumbering or complex bilateral overlays, and without IP conflicts. Typical uses include staged integration, shared services, and selective application access during post-merger periods.

11.2 M&A Control Plane and Identity Model

* Access-Mode TLV is set to M&A in SSE-ID for flows that require cross-enterprise access.
* The initiating enterprise includes a Peer-Enterprise-ID (Peer-EID) TLV naming the remote enterprise.
* Each enterprise’ s address space is scoped by an Address-Domain ID (ADID) so that overlapping IPs can coexist.
* Both enterprises must onboard with the SSE provider and authorize a bilateral policy scope. Trust anchors and policy exchanges occur in the SSE control plane.

11.3 In-Cloud Splicing and Address-Domain Isolation

* At the SSE POP, traffic is spliced between the two enterprises based on (EID, Peer-EID, Access-Mode=M&A) and confined to an M&A-scope policy context.
* ADID scoping isolates address domains; overlapping RFC1918 or other private prefixes are disambiguated by ADID rather than renumbering.
* The SSE fabric MAY implement per-flow NAT, translation, or VRF-like segmentation keyed by (EID, ADID) while preserving connectivity and auditability.

11.4 M&A Data Plane Behavior

* Endpoints include SSE-ID with Access-Mode=M&A, Peer-EID, and ADID.
* Enterprise edges forward to SSE per normal SSE-ID behavior.
* The SSE POP enforces bilateral policy and performs in-cloud splicing.

* Return traffic follows the same identity context; no site renumbering is required.

11.5 Error Handling and Rollback

* If M&A authorization is absent or expired, the SSE POP MUST drop or reroute traffic per enterprise policy, and SHOULD signal the condition via telemetry.
* Conflicting ADID assignment MUST be rejected with a clear error for operator remediation.

12. Error Handling (General)

* Malformed SSE-ID: drop and log.
* Invalid DST: ignore and revert to hub.
* Expired DST: tear down direct path.
* Unsupported carriage: fall back to defined alternative.
* SOPP route leakage detected: withdraw and alarm.
* SPID unknown: select default SOPP policy or nearest POP.
* M&A authorization failure: drop or splice-deny and alert.

13. Security Considerations

* Integrity via signatures or MAC; POPs validate.
* Replay protection via Nonce and Expiry.
* Zero trust alignment: controller-issued DST; explicit M&A consent.
* Participating ISPs MUST treat SOPP as service ingress only; egress to public Internet MUST use non-SOPP space to prevent spoofing or reflection abuse.
* M&A traffic MUST remain segmented by (EID, ADID); only authorized applications are exposed across enterprises.

14. Privacy Considerations

* SSE-ID avoids user identifiers.
* DST uses opaque device identifiers.
* SPID reveals only POP selection hints.
* ADID confines address metadata to SSE scope; avoid exposing ADID on the open Internet.

15. IANA Considerations

This document requests the creation of the following registries:

* SSE-ID TLV Types:
  - 0x01 SSE-Target
  - 0x02 Policy Class
  - 0x03 Device Class
  - 0x04 Geofence Hint
  - 0x05 Expiry
  - 0x06 Attestation Evidence
  - 0x07 Enterprise Attribute
  - 0x08 SSE-POP-ID (SPID) [NEW]
  - 0x09 SOPP-Indicator [NEW]
  - 0x0A Access-Mode [NEW]
  - 0x0B Peer-Enterprise-ID [NEW]
  - 0x0C Address-Domain-ID (ADID) [NEW]
  - 0xFE Experimental
  - 0xFF Padding

* Access-Mode Values:
  - 0x00 Default
  - 0x01 Require-SSE
  - 0x02 M&A [NEW]

* DST TLV Types (initial set unchanged unless aligned with M&A).

* New codepoints for SSE-ID carriage:
  - IPv6 Destination Option Type (SSE-ID)
  - TCP Option Kind (SSE-ID compressed)
  - QUIC Transport Parameter ID (sse_id)

16. Examples

* Internet-bound traffic with SSE-ID (Require-SSE): normal SSE handling; SOPP unrelated.
* Enterprise traffic to SSE via Participating ISP: destination is SOPP; SPID guides POP choice; egress to Internet from SSE uses non-SOPP addresses.
* M&A mode: Enterprise A (EID=123) to Enterprise B (EID=456), overlapping 10.0.0.0/8. SSE-ID carries Access-Mode=M&A, Peer-EID=456, ADID=A. SSE splices flows at the POP; ADID enforces isolation and resolves conflicts without renumbering.

17. References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, May 2017.

Appendix A. Non-Normative YANG Tree

(Omitted for brevity)

Appendix B. Example Controller API

```
POST /dst/issue
POST /dst/revoke
```

Appendix C. Example State Machine

```
INIT -> POLICY_PENDING -> DIRECT_NEGOTIATION -> DIRECT_ACTIVE
```

Author’s Address

Prasad Kulangara
Email: prasad_k1@persistent.com

Expires: July 2026