Path Computation Element Communication Protocol for Source Address Validation

draft-song-pce-pcep-sav-01

Xueyan Song	ZTE Corp.
Weiqiang Cheng	CMCC.
Shengnan Yue	CMCC.

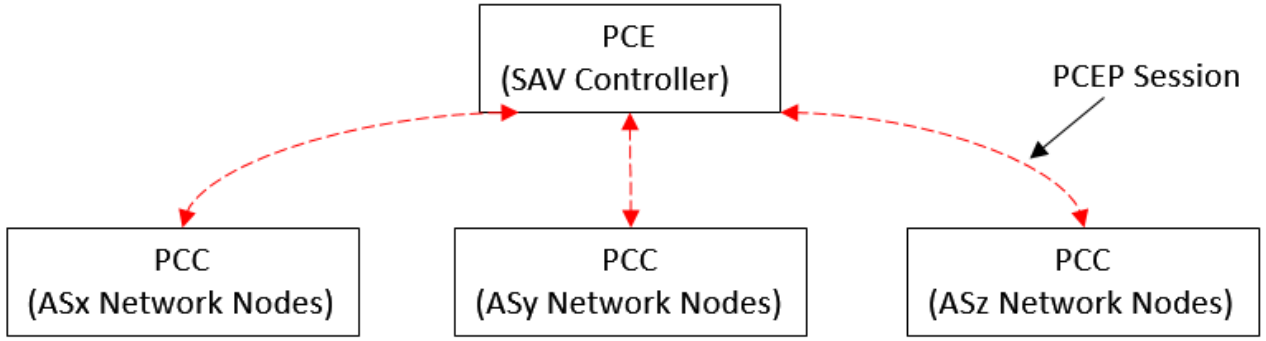
IETF 124 Meeting, November 2025

Overview

- **Source Address Validation (SAV)**
  - A critical security mechanism to prevent IP spoofing by validating source prefixes against ingress interfaces.
- **Challenges with Traditional Methods**
  - ACL-based filtering, strict/loose uRPF have high operational overhead and may improperly block/permit traffic.
  - Issues documented in SAVNET problem statements.
- **PCE for SAV Support**
  - Path Computation Element (PCE) provides centralized control for SAV policies.
  - PCEP (PCE Communication Protocol) is extended for dynamic SAV policy enforcement.

Why is PCE

- **Why to Use PCE**
  - The centralized control capability of PCE can enhance the dynamics of SAV strategies and the efficiency of cross-domain coordination.
- **Centralized Advantage**
  - Network controllers manage and deliver SAV-specific information. Underlay routers acquire SAV-specific information and policies directly from the controller, eliminating the need for mutual communication between network nodes.
- **PCE as SAV Controller**
  - PCE provides a centralized control framework for SAV policy computation.
  - Provides the visibility of global SAV policy across network domains.
  - Provides global filtering policy optimization and across-domains coordination.



PCE for SAV Support

- **Data Collection**
  - PCE collects SAV data via mechanisms like BGP-LS or NETCONF/YANG interfaces from edge/border routers.
- **Policy Computation**
  - PCE computes validation paths (e.g., mapping prefixes to valid interfaces).
  - PCE generates SAV policies based on the source prefixes, prefix path and incoming interfaces.
- **Policy Delivery**
  - Delivers SAV policies to edge/border nodes acting as PCCs of network through PCEP protocol.
- **Policy Update**
  - Executes filtering actions (such as forward, drop, redirect, etc.) and report policies implement status.
  - Re-computes validation paths and adjusts filtering policies to reflect network topology updates or abnormal traffic detection.
- **Multi-Domain**
  - Enables cross-domain SAV policy coordination.

SAV Information

- Follows draft-ietf-savnet-general-sav-capabilities.

Mode	Scale	SAV rule	validation result
IBA	interface	interface-based source prefix allowlist	invalid if not matched
IBB	interface	interface-based source prefix blocklist	invalid if matched
PBA	router	prefix-based interface allowlist	invalid if not matched
PBB	router	prefix-based interface blocklist	invalid if matched

PCEP Extensions

SAV-Capability Advertisement

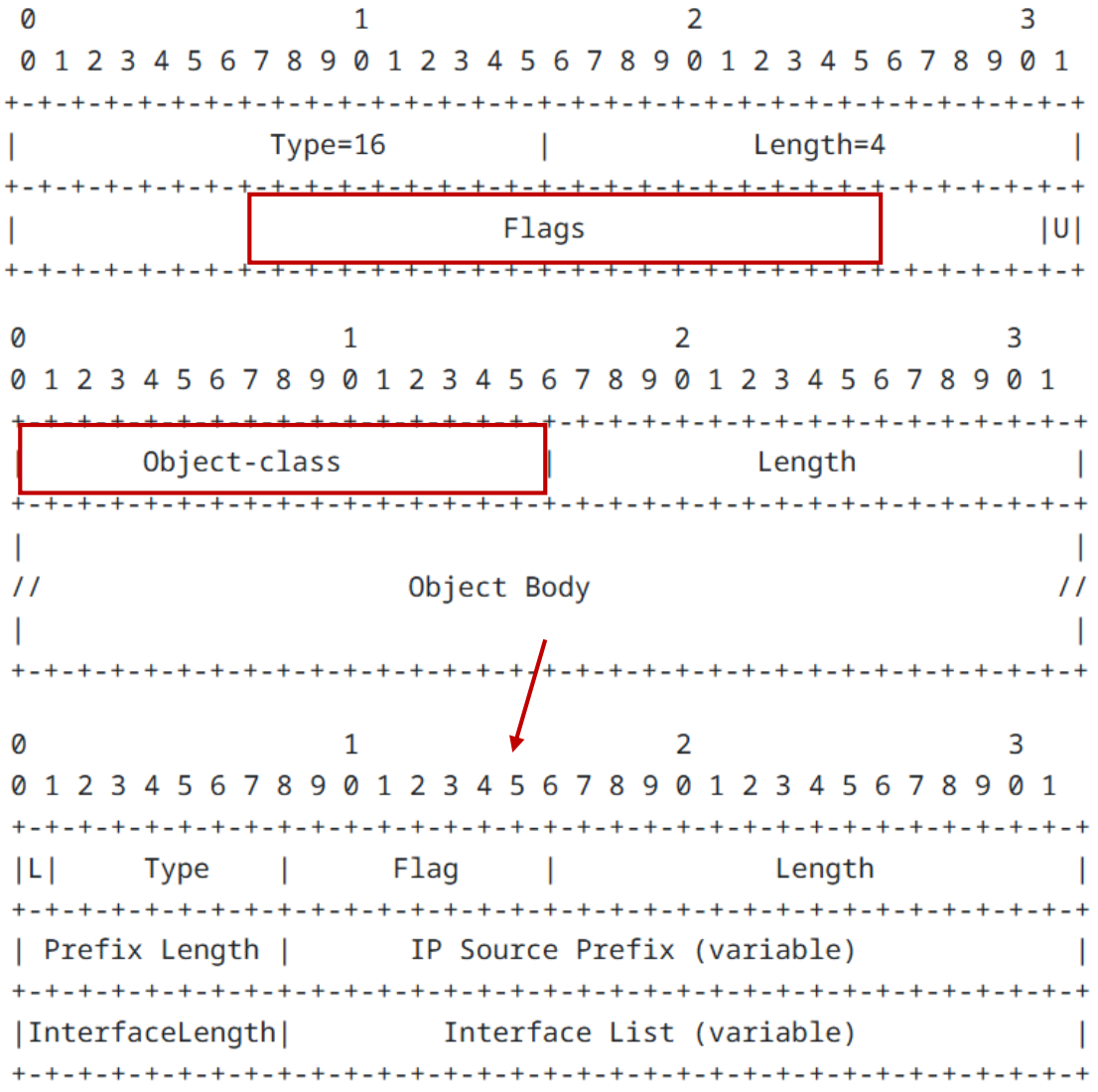
- New TLV in OPEN messages for negotiating SAV support.
- "STATEFUL-PCE-CAPABILITY" TLV Flag Field, reference RFC8231.

SAV-Policy Object

- New object class to carry SAV policy information in PCEP updates
- SAV-POLICY object class value is TBD.

SAV-Policy Object Body

- L: IPv4 and IPv6 types
- Type: to be assigned by IANA
- Flag: 4 validation modes
- Interface List: Legitimate or illegitimate interfaces allow-list/block-list
- IP source prefix: IPv4 or IPv6 prefix



Next Steps

- Request working group review and feedback.
- Keep update the details of PCEP extension at the PCE working group.