Advertising SAV Rule-related Information using BGP Link-State

draft-tong-idr-bgp-ls-sav-rule-04

Tian Tong (China Unicom), Dan Li(Tsinghua University), Nan Geng (Huawei),
Nan Wang (China Unicom), Shunwan Zhuang(Huawei), **Jing Zhao(China Unicom）**

IETF-125

Commets from Mail List

- **Main Comment :** Using BGP-LS to distribute subnet/AS attachment information generally may face scalability issues, as SAV enforcement destinations per interface **can be very large.**

- **Response:**

This draft considers the extreme case of the AS Customer Cone (i.e., the largest prefix set used for SAV).

As defined in RFC 8704, Section 3.6.1:

Small/medium AS Customer Cone: ≤ 10,000 prefixes

Large AS Customer Cone: ~30,000 prefixes

When combined with BGP-LS incremental synchronization, the proposed mechanism is feasible in most deployment scenarios.

Updates after IETF 124

☐ Purpose: What BGP-LS used for in this draft?

Instead of collecting SAV rules from the data plane of an individual device 

- It collects all SAV rule-related information for the entire subnet or ASes to which the router is connected.

This information enables SAV rule monitoring, attack traceback, and service anomaly analysis, for which dynamic, real-time acquisition is critical.

Updates after IETF 124

☐ Procedure: How BGP-LS is used?

Routers that support SAV mechanisms/protocols establish BGP-LS sessions with the controller, to report their multi-sourced SAV rule-related information.

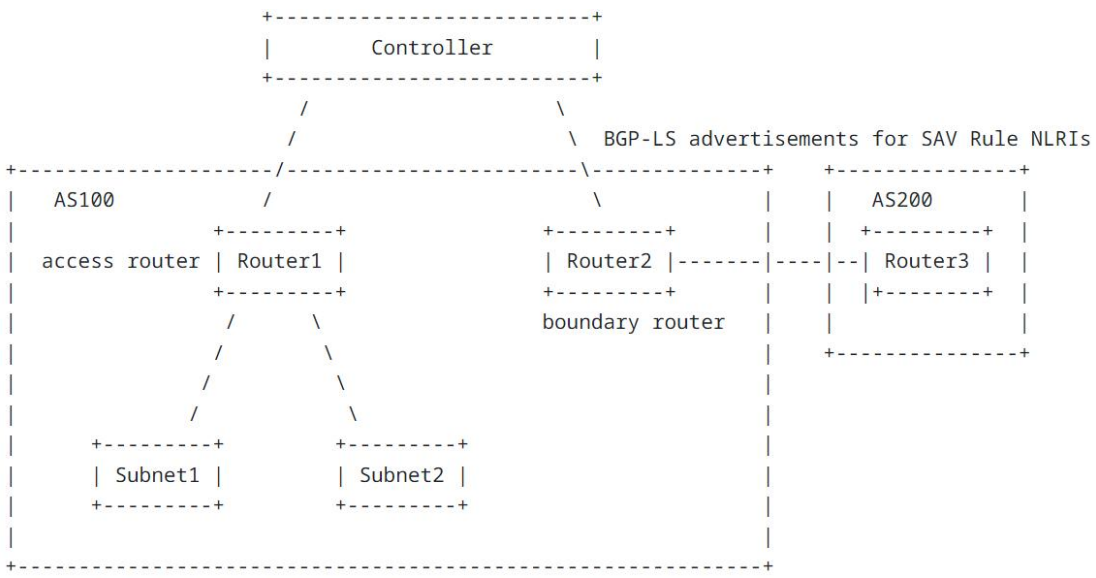
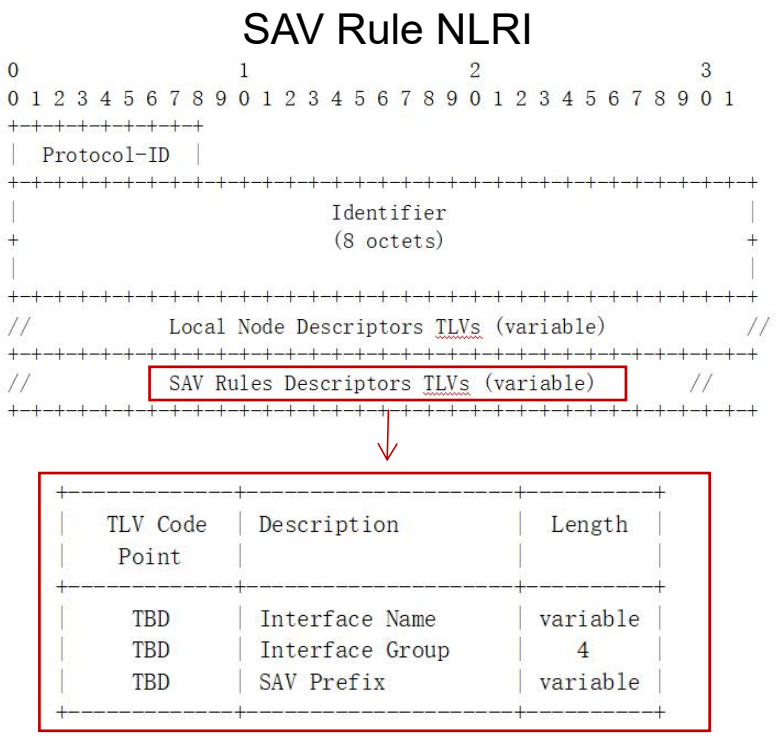


Figure 8: Advertisement of SAV Rules using BGP-LS

SAV Rule-related Information Carried in BGP-LS

- **What SAV rule-related information is to be carried?**



Information	Description	fields
Source	The source of SAV rule-related Information, i.e., generated by which protocol.	Protocol-ID: Specifies the source of SAV rule-related information.
Node	Which node (router) maintains the carried SAV rule-related information.	Local Node Descriptors TLV: Contains Node Descriptors for the nodes storing SAV rules.
Interface	Interfaces enabled SAV.	SAV Rule Descriptors TLVs: There can be one or more SAV Rule Descriptors TLVs for carrying SAV rules.
Source prefix	Prefix list of the specified interface.	
Validation mode	Blocklist mode or allowlist mode.	

BGP-LS Attribute for SAV Mode

☐ SAV mode TLV

An optional and non-transitive BGP attribute that carries the validation mode information [I-D.ietf-savnet-general-sav-capabilities].

It is not **restricted to the four existing validation modes,** in order to support forward compatibility and future extensibility.

M Flag	Mode	Description
00	IBA-SAV	Interface-based prefix allowlist
01	IBB-SAV	Interface-based prefix blocklist
10	PBA-SAV	Prefix-based interface allowlist
11	PBB-SAV	Prefix-based interface blocklist

☐ SAV action TLV

The SAV Action TLV uses the traffic filtering actions defined in [RFC8955] and [RFC8956].

A SAV rule may be associated with multiple SAV actions, and conflicts may exist among these actions.

More comments and discussion welcomed

Thank you!