

Advertisement of Multi-Sourced SAV Rules using BGP Link-State

(BGP-LS for Advertising SAV Rules)

draft-tong-idr-bgp-ls-sav-rule-02

Tian Tong (China Unicom)

Dan Li (Tsinghua University)

Nan Geng (Huawei)

Nan Wang (China Unicom)

Shunwan Zhuang(Huawei)

Jing Zhao (China Unicom)

IETF123

Summary of Comments (IETF 122)

- **Comment 1:** How to distribute SAV rules within the IGP domain when BGP-LS runs on only one router per autonomous system but SAV rules exist on every router.
- **Comment 2:** Whether SAV rules should be flooded throughout the entire BGP-LS domain, suggesting that they should only be sent to the controller and that the BGP-LS operational procedures should be modified.

Updates have been made in the draft-tong-idr-bgp-ls-sav-rule-02 in response to the above comments.

- ✓ Update Section 3: BGP-LS Attribute for SAV Mode
- ✓ Added Section 4: Specify the BGP-LS attribute for SAV actions.
- ✓ Added Section 5: Example of Validation Modes and SAV rule NLRI Configuration
- ✓ Added Section 6: Procedures

Update **Section 3: BGP-LS Attribute for SAV Mode**

□ draft-tong-idr-bgp-ls-sav-rule-00

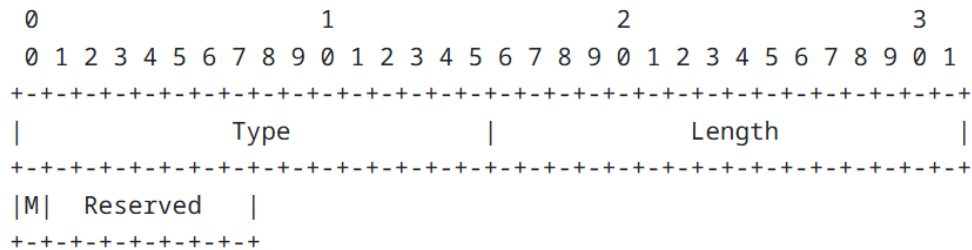


Figure 7: SAV Mode TLV

The SAV Mode TLV carries a Mode Flag (M flag shown in the figure) describing the validation mode attribute.

- * When M flag is **unset**, the mode is **blocklist** mode.
- * When M flag is **set**, the mode is **allowlist** mode.

□ draft-tong-idr-bgp-ls-sav-rule-02

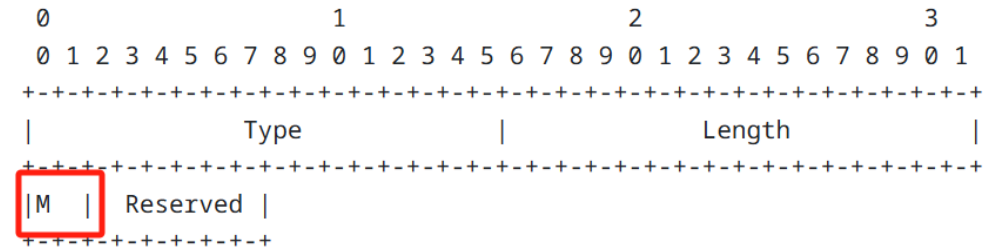


Figure 7: SAV Mode TLV

The SAV Mode TLV carries a Mode Flag (M flag is shown in the figure and occupies **two bits**) describing the validation mode attribute.

- * When M flag is set to **00**, the mode is Mode 1: **interface-based source prefix allowlist**.
- * When M flag is set to **01**, the mode is Mode 2: **interface-based source prefix blocklist**.
- * When M flag is set to **10**, the mode is Mode 3: **prefix-based interface allowlist**.
- * When M flag is set to **11**, the mode is Mode 4: **prefix-based interface blocklist**.

Section 4: BGP-LS Attribute for SAV Actions

- ✓ SAV actions in this document adopt the traffic filtering actions defined in [RFC8955] and [RFC8956].

community Oxttss	action	encoding
0x8006	traffic-rate-bytes (Section 7.1)	2-octet AS, 4-octet float
0x800c	traffic-rate-packets (Section 7.2)	2-octet AS, 4-octet float
0x8007	traffic-action (Section 7.3)	bitmask
0x8008	rt-redirect AS-2octet (Section 7.4)	2-octet AS, 4-octet value
0x8108	rt-redirect IPv4 (Section 7.4)	4-octet IPv4 address, 2-octet value
0x8208	rt-redirect AS-4octet (Section 7.4)	4-octet AS, 2-octet value
0x8009	traffic-marking (Section 7.5)	DSCP value

Table 8: Traffic Filtering Action Extended Communities

[RFC 8955] Dissemination of Flow Specification Rules

- ❑ Traffic filtering actions defined in [RFC 8955] are applicable to IPv4 and IPv6.
- ❑ Rt-redirect-ipv6 is a new traffic filtering action defined in [RFC 8956], which is applicable to IPv6.

Section 5: Example of Validation Modes and SAV rule NLRI Configuration

✓ Mode 1: Interface-based prefix allowlist

* SAV rule NLRI:

prefix = 192.168.1.0/24, interfaces = [Interface A]

* Validation:

Any packet with a source prefix of 192.168.1.0/24 arriving at Interface A is valid.

All other prefixes on Interface A are invalid.

✓ Mode 2: Interface-based prefix blacklist

* SAV rule NLRI:

prefix = 10.0.0.0/8, interfaces = [Interface B]

* Validation:

Any packet with a source prefix of 10.0.0.0/8 arriving at Interface B is invalid.

All other prefixes on Interface B are valid.

✓ Mode 3: Prefix-based interface allowlist

* SAV rule NLRI:

prefix = 172.16.0.0/16, interfaces = [Interface C, Interface D]

* Validation:

Packets with a source prefix of 172.16.0.0/16 are valid only if they arrive at Interface C or Interface D.

This prefix arriving at other interfaces is invalid.

Other prefixes are not checked.

✓ Mode 4: Prefix-based interface blacklist

* SAV rule NLRI:

prefix = 192.168.2.0/24, interfaces = [Interface E]

* Validation:

Packets with a source prefix of 192.168.2.0/24 arriving at Interface E are invalid.

This prefix arriving at other interfaces is valid.

Other prefixes are not checked.

Section 6: Procedures

- ✓ The Routers running SAV mechanisms/protocols establish BGP-LS sessions with the controller respectively to report multi-sourced SAV rules.

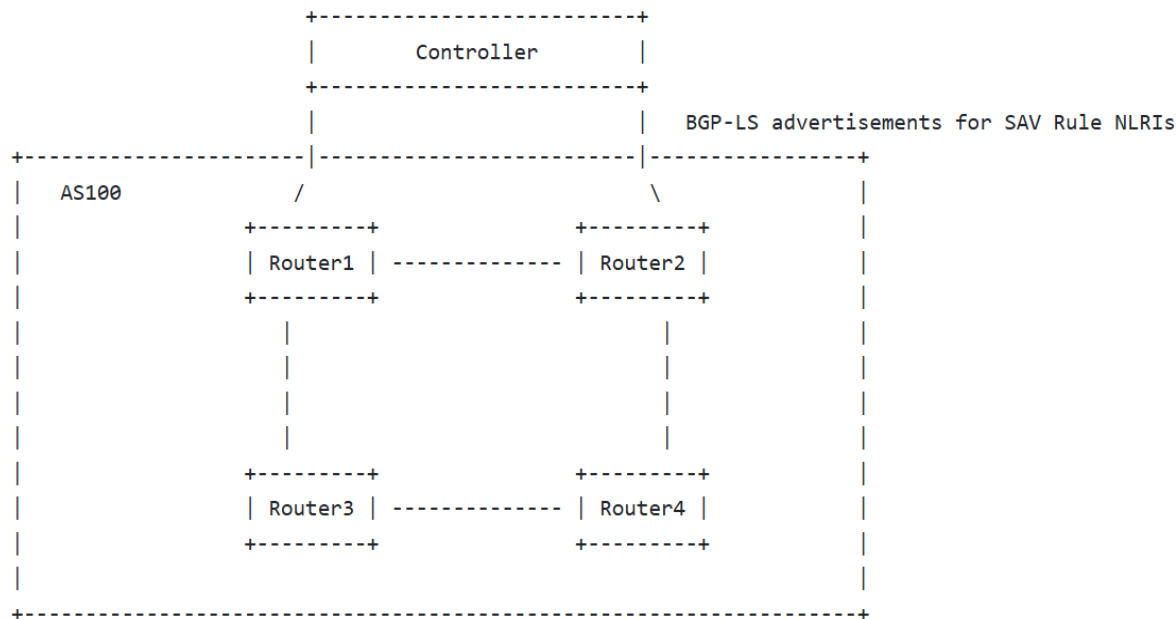


Figure 8: Advertisement of SAV Rules using BGP-LS

The process of reporting SAV rules via BGP-LS

Step 1: R1 and R2 run SAV mechanism/protocol, and generate multi-sourced SAV rules.

Step 2: R1 and R2 respectively establish BGP-LS sessions with the controller.

Step 3: R1 and R2 generate BGP-LS advertisements for the SAV Rule NLRIs.

Step 4: R1 and R2 report multi-sourced SAV rules to the controller through the sav rule NLRIs.

More comments and discussion welcomed

Thank you!