BGP Flow Specification for Source Address Validation

draft-geng-idr-flowspec-sav-01

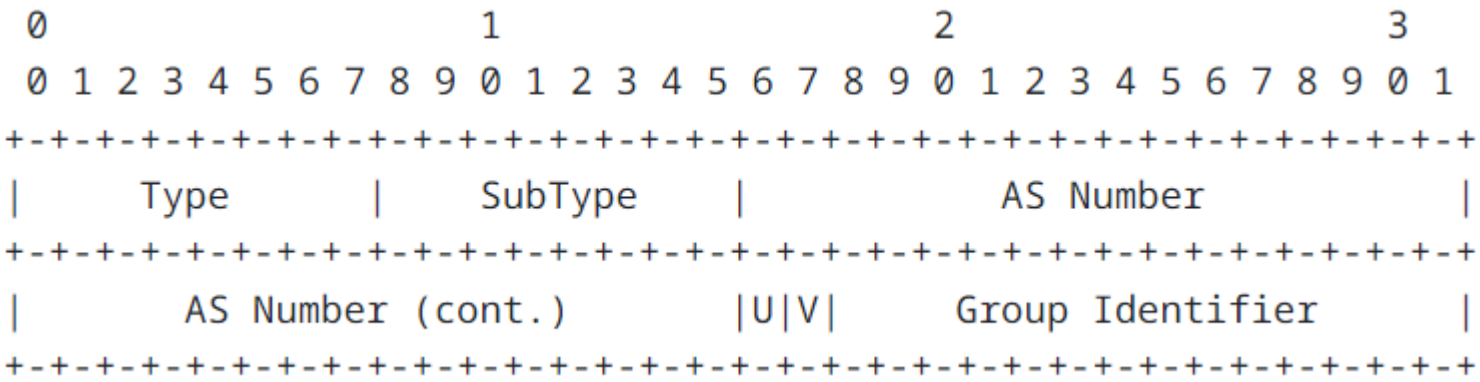
Nan Geng (Huawei), Dan Li (Tsinghua University)

Feb. 2024

BGP FlowSpec for SAV

- **Background:**
  - **SAV rule:** <source prefix, interface set, validity indicator>.
  - To facilitate SAV management and improve SAV accuracy, additional SAV rule dissemination is necessary [I-D.wu-savnet-inter-domain-architecture].
  - **BGP FlowSpec** is a convenient and flexible tool for traffic filtering/controlling ([RFC8955], [RFC8956]). It has supported source prefix matching and various traffic filtering actions but **does not support** binding **valid/invalid** incoming interfaces to source prefixes.
- **This document:**
  - Defines a new BGP extended community named **SAV Interface-set extended community**. SAV rules can be disseminated through BGP FlowSpec by combining the new extended community with source prefix component and filtering actions of existing BGP FlowSpec.
  - **Example use cases:** remotely install SAV rules from manual configuration or centralized SAV mechanism; collaborate with distributed SAV mechanisms for improving accuracy;

SAV Interface-set Extended Community



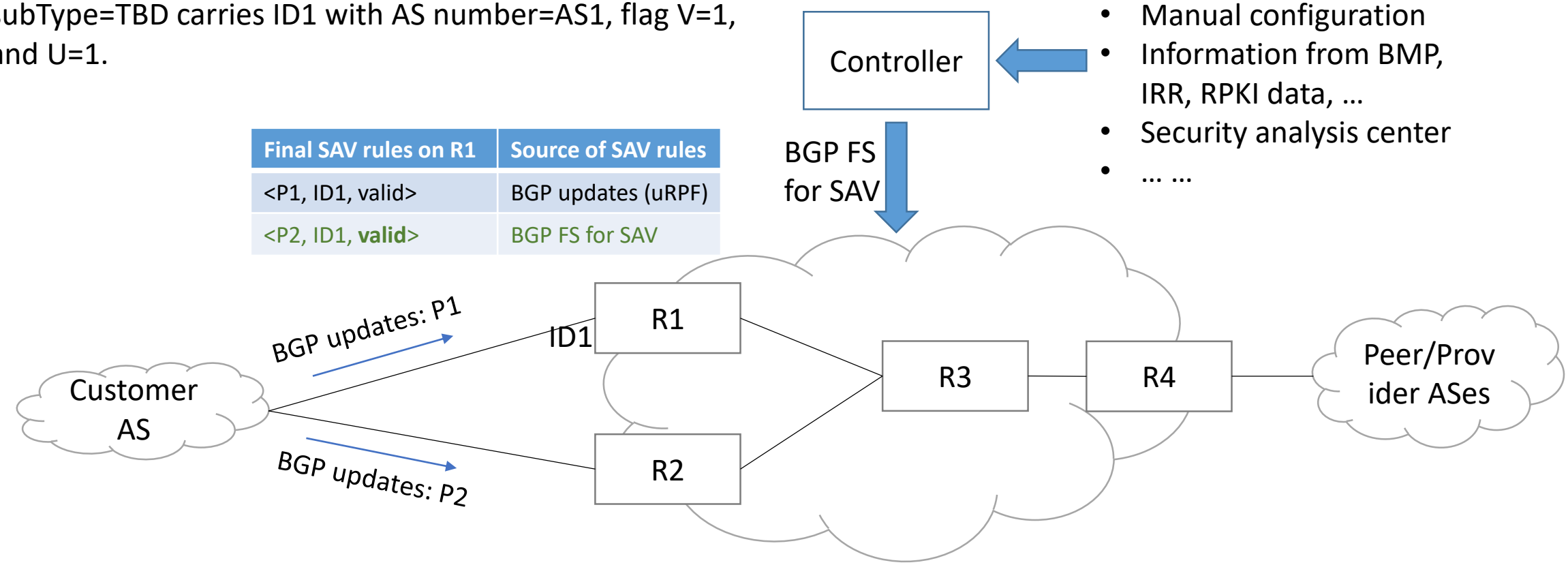
The extension is similar to I-D.ietf-idr-flowspec-interfaceset

- **Type (1 octect):** The value of 0x07 is for FlowSpec Transitive Extended Communities, and 0x47 represents FlowSpec Non-Transitive Extended Communities [**I-D.ietf-idr-flowspec-interfaceset**].
- **SubType (1 octect):** TBD. SubType field indicates SAV Interface-set extended community.
- **AS Number (4 octects):** 4-octect AS number indicates the target AS where the SAV rule takes effect.
- **Group Identifier (14 bits):** Group identifier is a local property and identifies a set of interfaces for the source prefix carried in NLRI. The meaning of a group identifier depends on the configuration.
- **Flag V (1 bit):** 1 means the identified interface set is valid for the source prefix, while 0 means the interface set is invalid for the source prefix.
- **Flag U (1 bit):** 1 means the rest of interfaces (not included in the interface set) are unknown for the source prefix. 0 means the rest of interfaces are invalid (when V=1) or valid (when V=0) for the source prefix.

Example

- Example: Configure source prefix P2 as valid at R1's interfaces (Group Identifier=ID1) connecting a multi-homed customer AS.
- Encoding description: NLRI with source prefix P2. The SAV Interface-set community with Type=0x07 and subType=TBD carries ID1 with AS number=AS1, flag V=1, and U=1.

Notes: About why purely relying on BGP routes are not enough for SAV, please refer to draft-ietf-savnet-intra-domain-problem-statement and draft-ietf-savnet-inter-domain-problem-statement



Thanks!