An update on the SAV using BGP UPDATE messages, ASPA, and ROA (BAR-SAV)

Kotikalapudi Sriram, Igor Lubashev, Doug Montgomery

Email: ksriram@nist.gov

IETF SAVNET Meeting, IETF 122, March 2025

"Source Address Validation Using BGP UPDATEs, ASPA, and ROA (BAR-SAV),"
https://datatracker.ietf.org/doc/draft-ietf-sidrops-bar-sav/

Changes in v-06 relative to v-05

- Detailed algorithm for BAR-SAV on Provider Interface (BAR-SAV-PI)
- Minor tweak to the existing algorithm for BAR-SAV on customer/lateral peer interface
- Clarification: Direct Server Return (DSR) AS can be a customer or lateral peer

Pre-Condition for BAR-SAV on Provider Interface (BAR-SAV-PI)

The pre-condition for BAR-SAV-PI is that the following basic prerequisites for BAR-SAV in the customer cone (CC) of the AS must be met:

- An AS within the CC attaching NO_EXPORT must have ASPA registration
- A prefix within the CC associated with DSR must have ROA registration

The customer cone (CC) of the AS is determined using the BAR-SAV algorithm for customer interface (Section 4 in the draft).

Principles of BAR-SAV-PI

Refine ingress SAV by starting with loose uRPF allowlist for the provider interface at the AS and removing prefixes that meet the following criteria:

- Prefix is known to originate exclusively within the AS's CC
  - ➢ That is, the prefix has ROA(s) and no ROA indicates an origin AS outside of the CC
- AND every feasible route from the prefix origin to the AS is known to propagate exclusively within the AS's CC
  - ➢ That is, all ASes in the AS path of the route have ASPAs and no ASPA indicates a provider AS outside the AS's CC

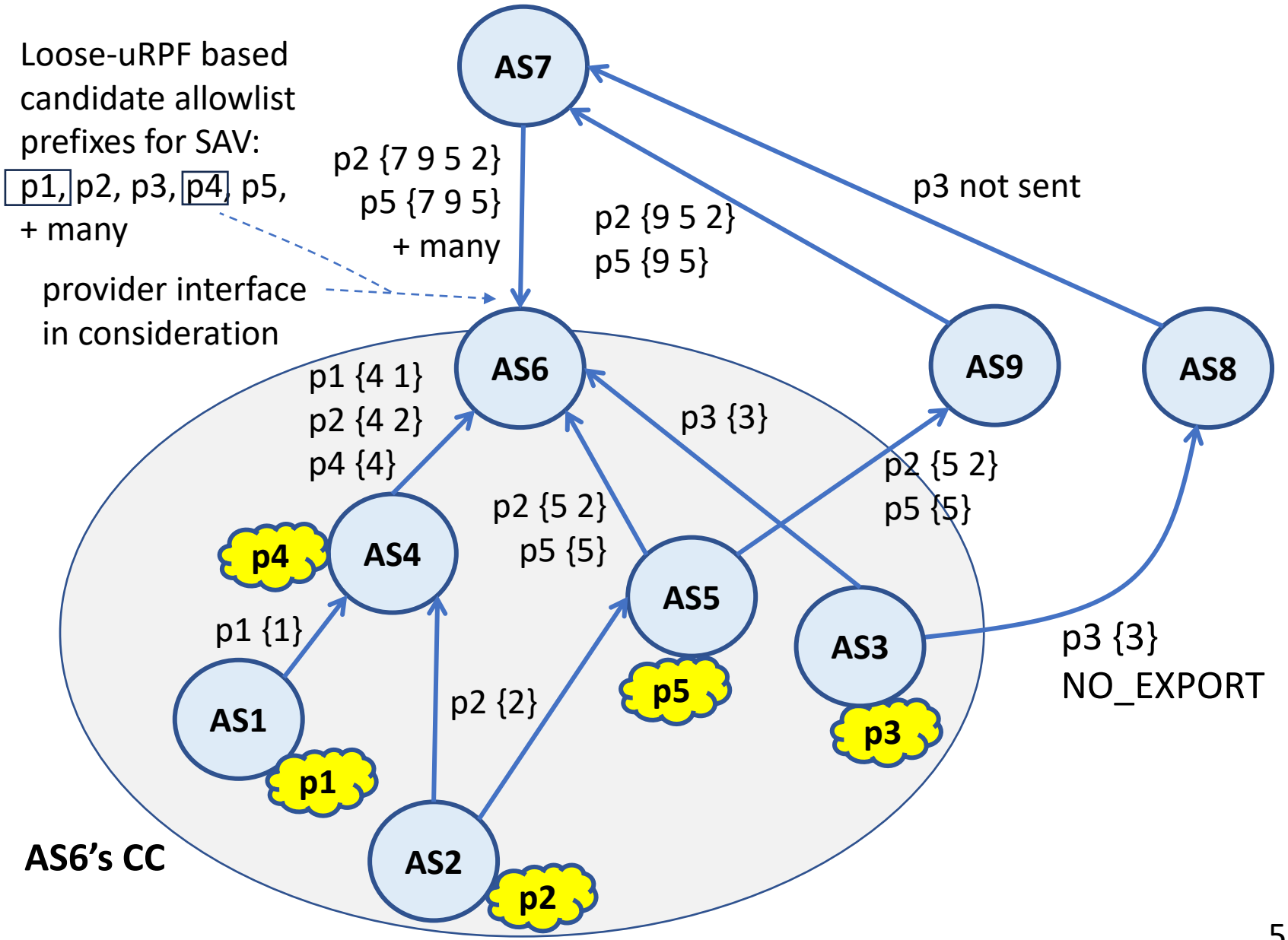
Illustration of BAR-SAV-PI

ROAs:
p1, AS1
p2, AS2
p3, AS3
p4, AS4

ASPAs:
AS1, {AS4}
AS2, {AS4}
AS3, {AS6, AS8}
AS4, {AS6}

p1 and p4 are deleted using the criteria on the previous slide

p2, p3, and p5 do not meet the criteria and are allowed



Added a sanity check step in the existing algorithm for BAR-SAV on customer/lateral peer interface

5. Create AS-set A(i) of all ASNs whose ASPA data declares at least one ASN in AS-set Z(i-1) as a Provider.
6. If AS-set A(i) contains AS 0 or any ASes with IANA special purpose AS numbers [IANA-sp-ASN], remove such ASes from the set and proceed.
7. Create AS-set B(i) of all customer ASNs each of which is a customer of at least one ASN in AS-set Z(i-1) according to unique AS_PATHs in Adj-RIBs-In of all interfaces at the BGP speaker computing the SAV filter.

Clarification: Direct Server Return (DSR) AS can be a customer or lateral peer

Responding to a question at the last IETF

- DSR AS can be a customer or lateral peer of the AS doing BAR-SAV
- The BAR-SAV procedure works fine in either case
- The anycast prefix is required to have a ROA with the DSR AS as origin AS

Thank you!

Q & A