BGP Extensions for Source Address Validation Networks (BGP SAVNET)

draft-geng-idr-bgp-savnet-02

N. Geng, Z. Li, Z. Tan, M. Liu, D. Li, F. Gao

Nov. 2023

Source Address Validation

□ Source address validation (SAV) is important for defending against source address spoofing attacks

□ Our focus:

- Route-based SAV: Validate source address by checking whether its incoming interface is valid
- Intra- and inter-domain SAVs: Do validation at edge/border routers

□ Not our focus:

- Cryptology-based SAV
- Access SAV: Do validation at access devices using techniques such as RADIUS/DIAMETER, SAVI (e.g., IP Source Guard), Cable Source-Verify, etc.

Existing SAV Mechanisms and Gaps

□ ACL-based ingress filtering [RFC2827][RFC3704]

□ Source-based RTBH filtering [RFC5635]

Not specific for SAV.
High operational overhead especially in dynamic or complex networks.

□ Loose uRPF [RFC3704]

□ Strict uRPF [RFC3704]

□ FP-uRPF [RFC3704]

□ VRF-uRPF [RFC8704]

□ EFP-uRPF [RFC8704]

uRPF generates SAV rules based on local FIB/RIB: Good automation but inaccurate under asymmetric routing.

Observation: Purely relying on local routing information for SAV is not enough for achieving both good automation and high accuracy

draft-ietf-savnet-inter-domain-problem-statement-02   draft-ietf-savnet-intra-domain-problem-statement-02

BGP SAVNET

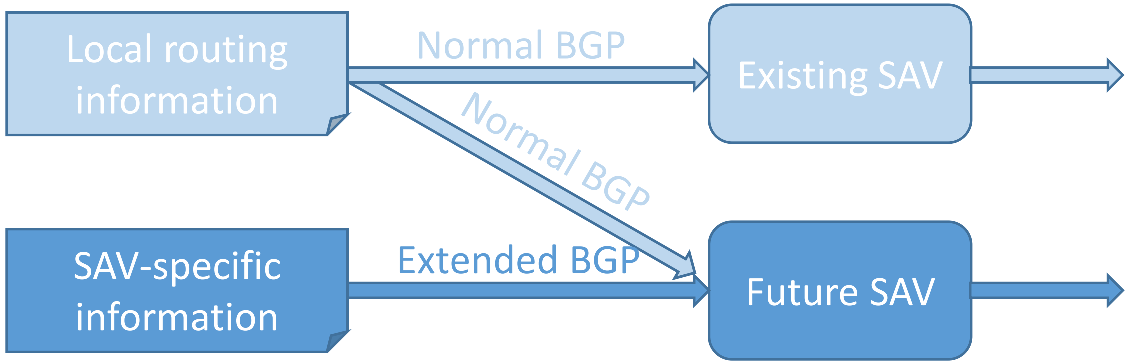
□ Extend BGP protocols to advertise SAV-specific information between edge/border routers of one or multiple ASes

- ◆ Follow draft-li-savnet-intra-domain-architecture-05 and draft-wu-savnet-inter-domain-architecture-05

□ SAV-specific information examples (Will explain in the following slides)

- ◆ Asymmetrically advertised routes
- ◆ Prefixes tagged as internal ones
- ◆ Target source prefixes with expected incoming directions

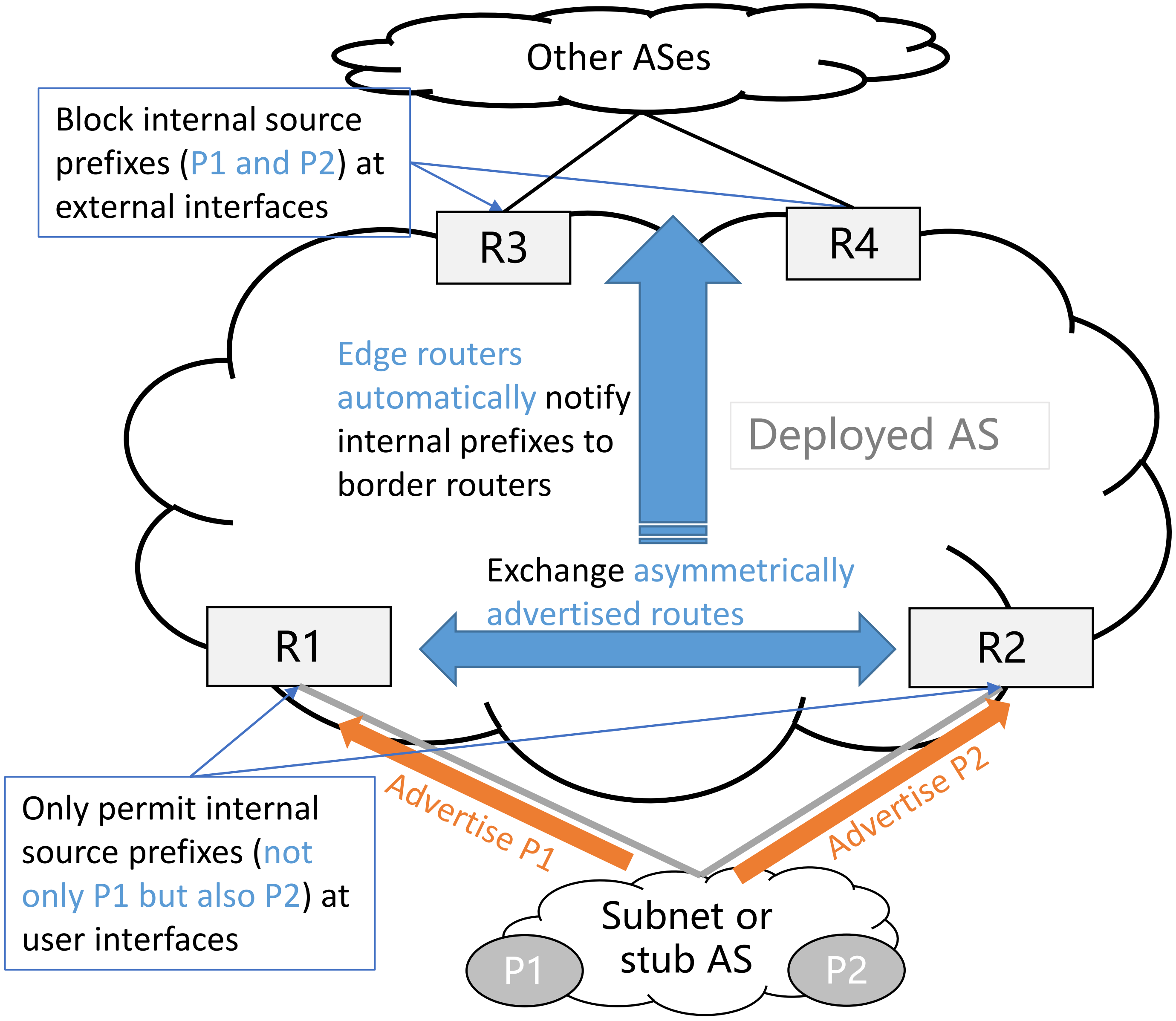
□ Assist edge/border routers on the network boundary to generate SAV rules



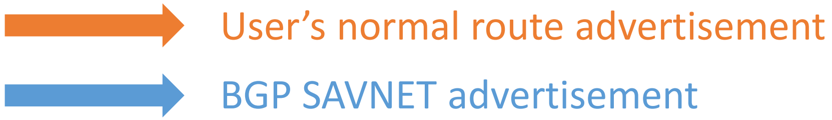
Sometimes inaccurate SAV rules

More accurate SAV rules and adaptive to various scenarios

BGP SAVNET for Protecting Internal Prefixes



Other ASes
Block internal source prefixes (P1 and P2) at external interfaces
R3
R4
Edge routers automatically notify internal prefixes to border routers
Deployed AS
Exchange asymmetrically advertised routes
R1
R2
Advertise P1
Advertise P2
Only permit internal source prefixes (not only P1 but also P2) at user interfaces
Subnet or stub AS
P1
P2



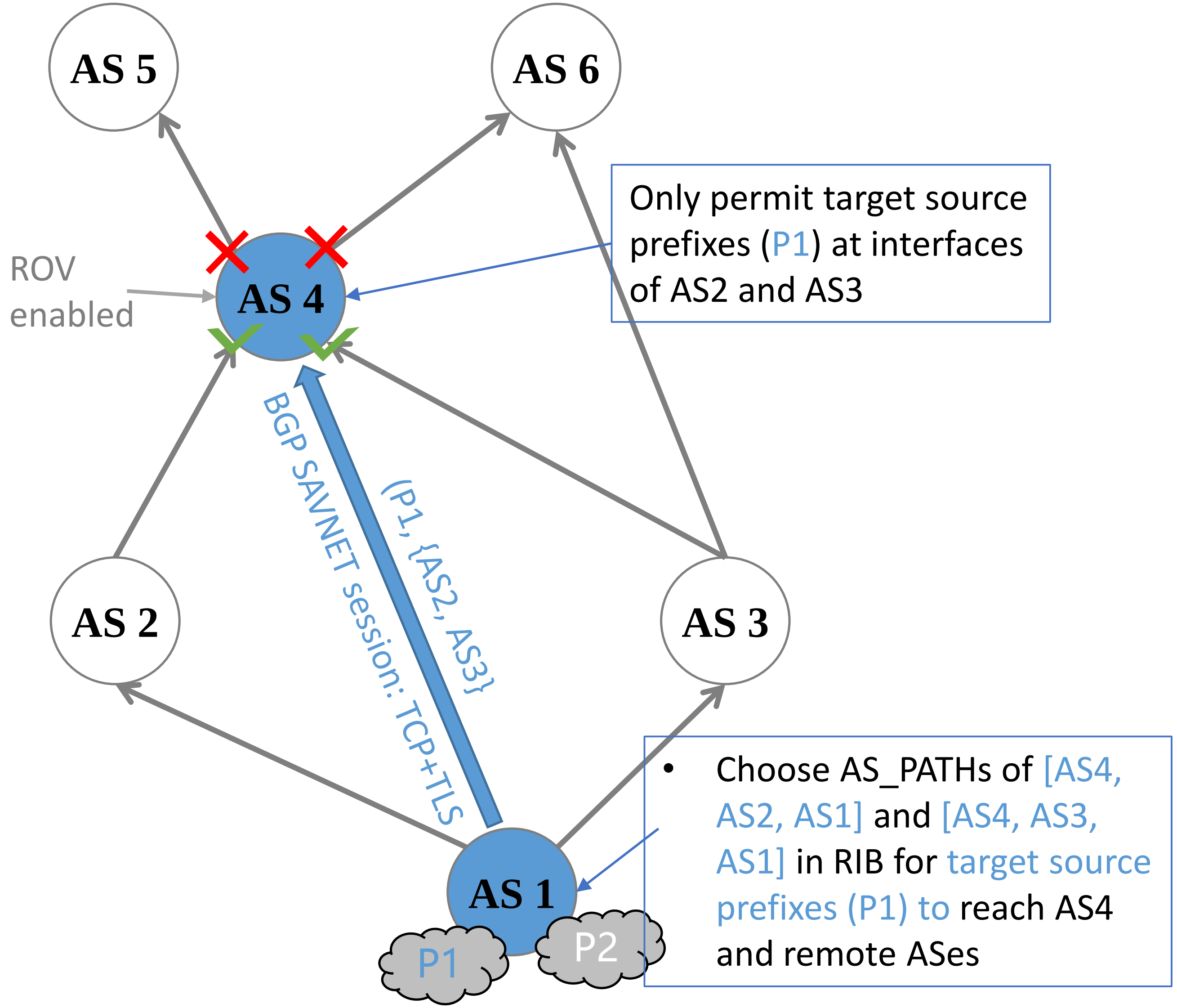
Features:

- Border routers can automatically collect internal prefixes and simplifies operations compared to manually configuring ACL rules.
- Edge routers can exchange asymmetrically advertised routes and avoids improper block of strict uRPF.
- Good deployability, i.e., upgrading part of routers can also work well
- Good convergence, i.e., 1) similar propagation speed to route and 2) support independent and incremental update (no need to wait for complete information)

BGP SAVNET for Protecting Remote Prefixes

● BGP SAVNET-deployed AS

➡ BGP SAVNET advertisement



Only permit target source prefixes (P1) at interfaces of AS2 and AS3

- Choose AS_PATHs of [AS4, AS2, AS1] and [AS4, AS3, AS1] in RIB for target source prefixes (P1) to reach AS4 and remote ASes

Features:

- Source AS (AS1) can notify target source prefixes that need to be specially protected.
- Source AS (AS1) can notify the legitimate incoming directions of target source prefixes.
- Validation AS (AS4) can provide services like 1) proactive SAV, 2) reactive source address filtering for mitigating DDoS, 3) key source address forwarding path protection
- Good deployability, i.e., any pair of upgraded ASes can work well
- Good convergence, i.e., 1) similar propagation speed to route and 2) support independent and incremental update (no need to wait for complete information)
- Simple trust model

Design Considerations

- Extending routing protocols for carrying SAV-specific information is an intuitive method
  - Existing SAV mechanisms primarily rely on local routing information.
- Extending BGP for advertising intra- and inter-domain SAV-specific information
  - Focus on doing validation on the network boundary for protecting internal and remote source prefixes. Using one protocol can adapt to various scenarios and simplify design workload
  - Reuse existing basic design and quality attributes to reduce design and development workload and facilitate application
  - Easy to extend and provide good service isolation
  - Explicit update and withdrawal without unnecessary periodic flooding
- Define new SAFIs (AFI:1, SAFI:TBD) and (AFI:2, SAFI:TBD)
  - New SAFIs provide good service isolation, and only the interested routers will receive the information

Next Step

□ Make the design complete

□ Comments are welcome

Thanks!