BGP Operations for Inter-domain SAV

draft-song-savnet-inter-domain-bgp-ops-00

Xueyan Song (ZTE)

Chunning Dai (ZTE)

Shengnan Yue (CMCC)

IETF 118 Meeting, November 2023

Agenda

- Terminology
- Method Considerations
- Operation Considerations
- Next Steps

Terminology

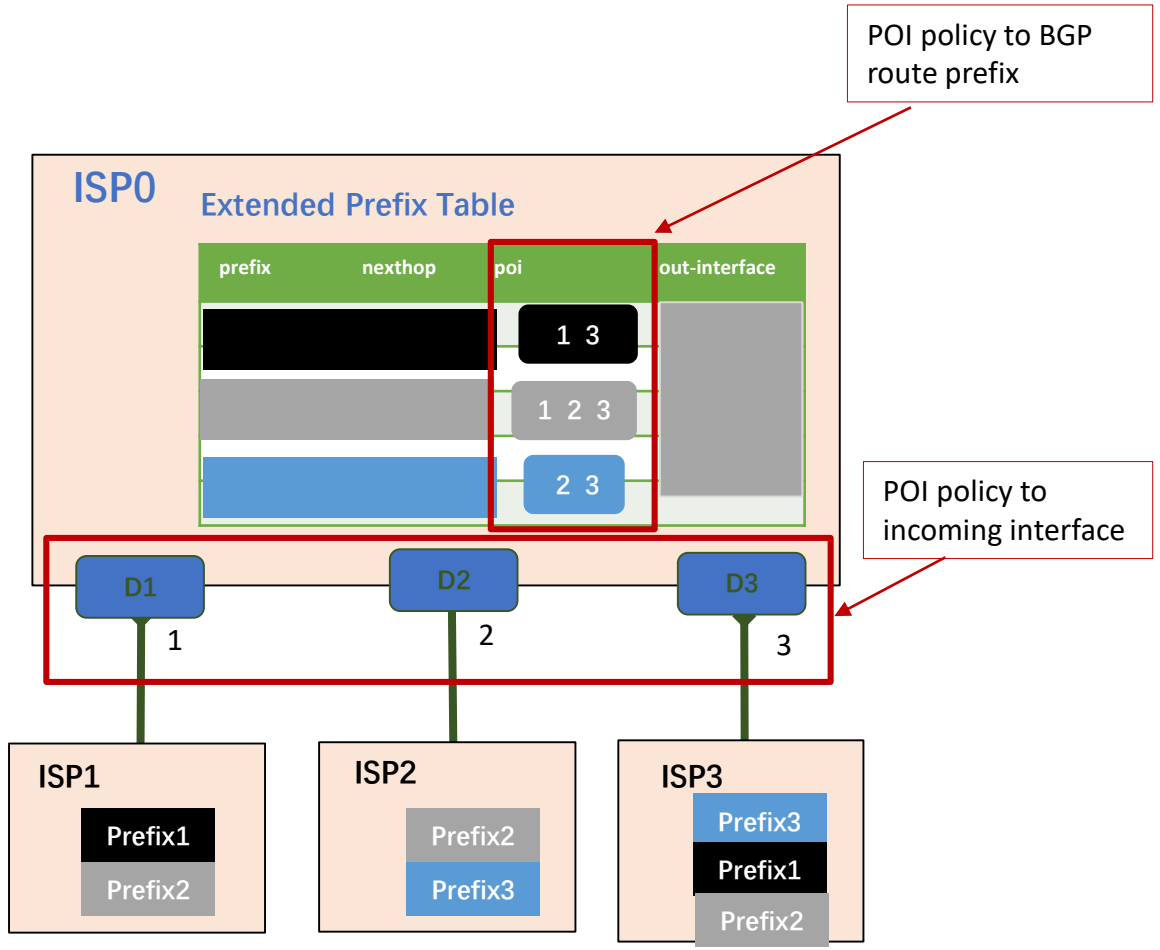
- Prefix Originated Indicator (POI)
  - A tag for IGP/BGP source Prefix Originated Identification
- Prefix
  - Has the content (IP address, prefix length), interpreted as customary (see [RFC4632])
- Route Prefix
  - The prefix derived from a route
- Incoming Interface
  - The interface which received the traffic of source route prefixes

Method Considerations

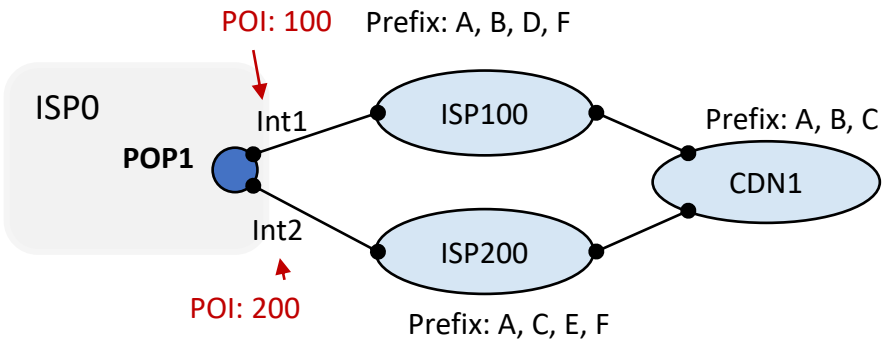
- The BGP AS inter-domain networks MAY be managed by different Operators.
- BGP operation policy for Inter-domain SAV is recommended to use local policy in ASBR.
- The BGP validation mechanism aims to reduce false positives regarding invalid incoming interface, mitigate source address spoofing, resolve the inflexibility about directionality of strict-URPF to improve accuracy of source address validation in inter-domain networks.
- The requirement for the BGP validation mechanism is the ability to validate the accuracy of incoming interface of the traffic for specific IP address prefixes.

Method Considerations

- Add POI attribute associated with the prefix source to BGP route via BGP neighbor configuration
- Bind POI mapping policy to the incoming interface of source traffic received from the packets of one specific address prefix
- Generate extended prefix table with SAV specific information (i.e., POI) for indicating the prefix source location or direction
- Perform source packets filtering and take actions based-on prefix-to-interface SAV rules



Multi-homing Scenario 1



Policy:

- AS level Prefix Originated Indicator (AS POI)

1 POI-to-Interface Mapping

Neighbor	POI	Interface
ISP100	100	1
ISP200	200	2

2 Prefix-to-Interface Rule

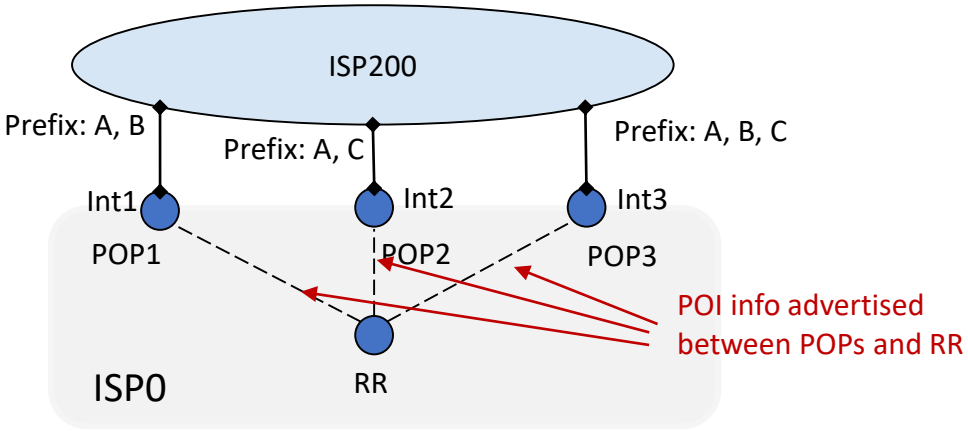
Prefix	POI	Interface
A (CDN1)	100 200	1 2
B (CDN1)	100	1
C (CDN1)	200	2
D (ISP1)	100	1
E (ISP2)	200	2
F (ISP1/ISP2)	100 200	1 2

3 SAV Action

Interface	Prefix	POI	Action
1	A	100	Permit
	B	100	Permit
	C	200	Deny
	D	100	Permit
	E	200	Deny
	F	100	Permit
2	A	200	Permit
	B	100	Deny
	C	200	Permit
	D	100	Deny
	E	200	Permit
	F	200	Permit

- Strict-URPF does not work well in the multi-homing scenario.
- BGP SAV method overcomes the limitation of strict-URPF and improves source address validation accuracy.

Multi-homing Scenario 2



Policy:

- 1. AS level Prefix Originated Indicator (AS POI)
- 2. Router level Prefix Originated Indicator (Router POI)

NOTE: In this case, BGP MAY need extensions to carry POI information along prefix advertisement.

Policy1:

1 Prefix carrying the same POI

POP	Neighbor	POI	Interface
1	ISP200	200	1
2	ISP200	200	2
3	ISP200	200	3

2 Prefix-to-Interface Rule at POP1

Interface	POI	Prefix
1	200	A, B, C

3 SAV Action at POP1

Interface	Prefix	POI	Action
1	A	200	Permit
1	B	200	Permit
1	C	200	Permit

Policy2:

POP	Neighbor	POI	Interface
1	ISP200	1	1
2	ISP200	2	2
3	ISP200	3	3

Interface	POI	Prefix
1	1	A, B

Interface	Prefix	POI	Action
1	A	1	Permit
1	B	1	Permit
1	C	1	Deny

Operation Considerations

- Source Address Validation (SAV) should provide a feasible way to filter invalid address and mitigate source address spoofing attacks in the data plane. For control plane processing, RPKI-based BGP Prefix Origination Validation and BGP AS-path validation are out of the scope.
- SAV method can be deployed at current routers without significant software and hardware upgrades.
- SAV method should fit into the routers existing policy and allows a network to deploy incrementally or partially.
- SAV rules used by the ASBR routers are expected to be updated based-on the real network requirement.
- NOTE: ZTE has deployed the BGP SAV method proposed in this draft in existing routers and applied it to Operator's network equipment.

Next Steps

- Make analysis on possible BGP extensions
- Keep be consistent with the SAVNET inter-domain architecture draft
- Ask for WG reviews and suggestions