ASPA-based AS_PATH Verification for BGP Export

draft-zhang-sidrops-aspa-egress-02

Jia Zhang

SIDROPS WG Meeting

IETF 123

July 2025

Versions

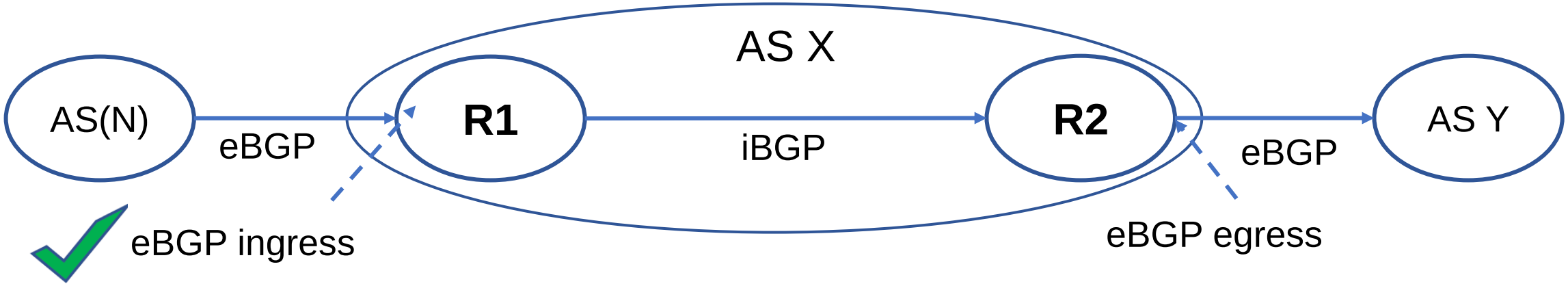
- IETF 122 - **draft-zhang-sidrops-aspa-egress-01**
  - Define the process of ASPA based AS-PATH Verification at eBGP Egress

4. Necessity and Benificial Cases 4
4.1. Complete ASPA-based Verification Method 5
4.2. Prevent Local Misconfigurations 5
4.3. Detect ASPA Registration Errors 5

- IETF 123 - **draft-zhang-sidrops-aspa-egress-02**
  - Add motivation for ASPA based AS-PATH Verification at eBGP Egress
  - Modify the procedure accordingly
  - Thanks **Maria Matejka** for providing beneficial cases

- **draft-zhang-sidrops-aspa-egress-03** – coming soon

Recap of Verification Procedure



AS_PATH

AS(N) AS(N-1) … … AS(1)

AS_PATH

ASX AS(N) AS(N-1) … … AS(1)

Role of ASX to ASY

Customer, Peer, RS-client, RS — Upstream

Provider — Downstream

Necessity for ASPA Egress

Egress verification solves three critical gaps in ASPA deployment

- Blocks misconfigurations at source
  - Like ROV-egress*[RFC8893]* for AS_PATH
- Completes ASPA's security model
  - Prevents local route leaks
- Accelerates error detection
  – Detect ASPA registration errors more quickly

Necessity and Beneficial Cases

- **Prevent Local Misconfigurations**:
  - Case 1: AS federation risks (multiple AS numbers)
    - Accidentally adding internal ASes to AS_PATH
  - Case 2: AS_PATH manipulation
    - Errors during prepending/aggregation
  - Prevent the local AS from advertising routes with invalid AS_PATHs
  - Just like ROV-egress blocks invalid origins at the source – we need equivalent for AS_PATH.

Necessity and Beneficial Cases

- **Complete ASPA-based Verification Method**:
  - Strengthen ASPA mechanisms to mitigate local route leaks through ASPA-based egress verification
  - *draft-ietf-sidrops-aspa-verification-22* defines ingress-only
  - Egress verification requires different algorithm/procedure

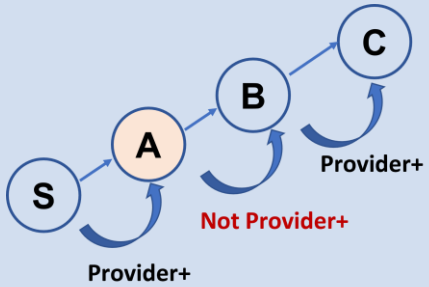
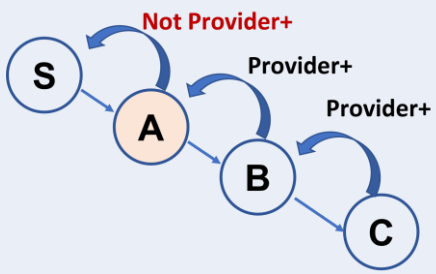
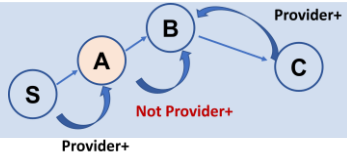
Necessity and Beneficial Cases

- Compare to other methods, e.g. OTC and DO (Down Only):
  - Out-of-band route validation, decoupling from BGP configurations
    - mitigate misconfiguration risks
  - ASPA's security and operational advantages

	OTC	ASPA
Security Considerations	• No built-in anti-tampering mechanisms • Missing integrity verification	• Resource Certification • Authentication
Operational Complexity	• BGP Role configuration per router per session • Remote Peer also need Router upgrade for RFC9234	• Remote Peer just need ASPA registration

Necessity and Beneficial Cases

- **Detect ASPA Registration Errors**:
  - Routes are affected by local or customer registration omissions/errors

AS A has ASPA, but omit at least one provider	Type	Ingress (Current ASPA Method)	Egress (This draft Method)	Prepend Ingress + one more Prepend Egress (Maria Method)
	Upstream	2-hop A: Valid B: Valid C: Invalid	**1-hop** **A: Valid** **B: Invalid**	0-hop (Local) A-ingress: Valid A-egress: Invalid B-ingress: Invalid
	Downstream	1-hop A: Valid B: Invalid	**0-hop (Local)** **A: Invalid**	0-hop (Local) S-egress: Invalid A-ingress: Invalid A-egress: Invalid
	peaking point	Can not detect	**Can not detect**	Can not detect

Necessity and Beneficial Cases

- **Detect ASPA Registration Errors**:
  - Routes are affected by local or customer registration omissions/errors
  - Detect such registration errors immediately and point to its actual source clearly and noticeably.

Questions

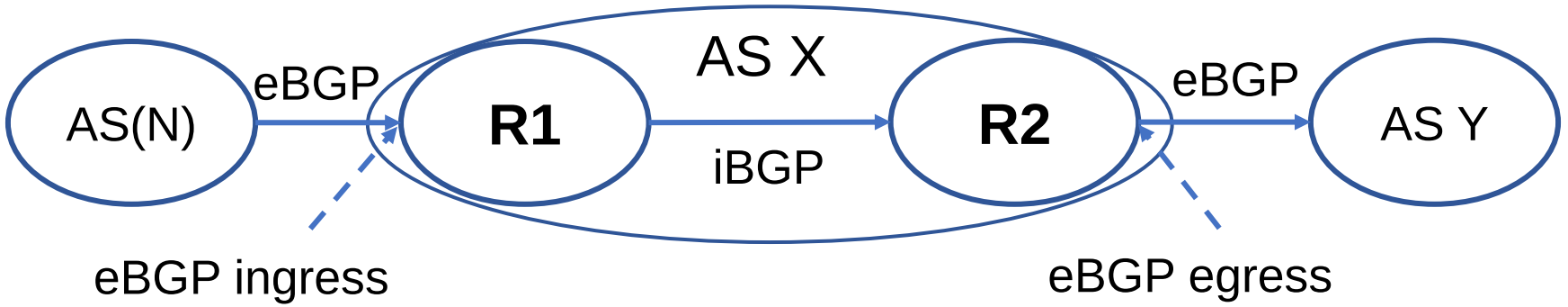
- Q1: Egress verification requires separate spec?
  - Implementation concern only?

- A1: Yes, requires separate specification:
  - *draft-ietf-sidrops-aspa-verification-22* defines ingress-only
  - Egress validation requires different algorithm/procedure
  - Defining implementation procedure for vendors supporting this feature

Questions

- Q2: Local configs are enough?
  - Local config with local AS's awareness of the neighbor relations.

- A2: No, Upstream relationships require propagation from ingress to egress:
  - R2 do not know the relation between AS(N) and AS X.
  - Obtain from ASPA record.



Takeaway

- Performing ASPA-based AS_PATH verification at the egress
  - Prepend Local AS to the received AS_PATH.
  - Verification based on the BGP Role of local AS to next-hop neighboring AS.
- Necessity to standardize egress ASPA-based AS_PATH verification
  - Prevent local misconfigurations.
  - Strengthen ASPA mechanisms to mitigate local route leaks.
  - Out-of-band route verification, decoupling from BGP configurations.
  - Detect ASPA registration errors.
- Questions, criticisms, and applause are welcome.

Thank you !

Special thanks to Yangyang Wang, Maria Matejka, Mingwei Xu, Sriram Kotikalapudi, Randy Bush, and Nan Geng for their valuable suggestions and comments.

ASPA-based AS_PATH Verification for BGP Export

zhangj@mail.zgclab.edu.cn

IETF 123 SIDROPS Meeting