

ASPA-based AS_PATH Verification for BGP Export

draft-zhang-sidrops-aspa-egress-04

Jia Zhang

Zhongguancun Laboratory

Yangyang Wang

Tsinghua University

Maria Matějka

CZ.NIC

Mingwei Xu

Tsinghua University

Kotikalapudi Sriram

NIST

Nan Geng

Huawei

IETF 125 SIDROPS

March 2026

Versions

- IETF 122 - **draft-zhang-sidrops-aspa-egress-01**
 - Define the process of ASPA based AS-PATH Verification at eBGP Egress
- IETF 123 - **draft-zhang-sidrops-aspa-egress-02**
 - Add motivation for ASPA based AS-PATH Verification at eBGP Egress

- IETF 125 - **draft-zhang-sidrops-aspa-egress-04 (Current)**

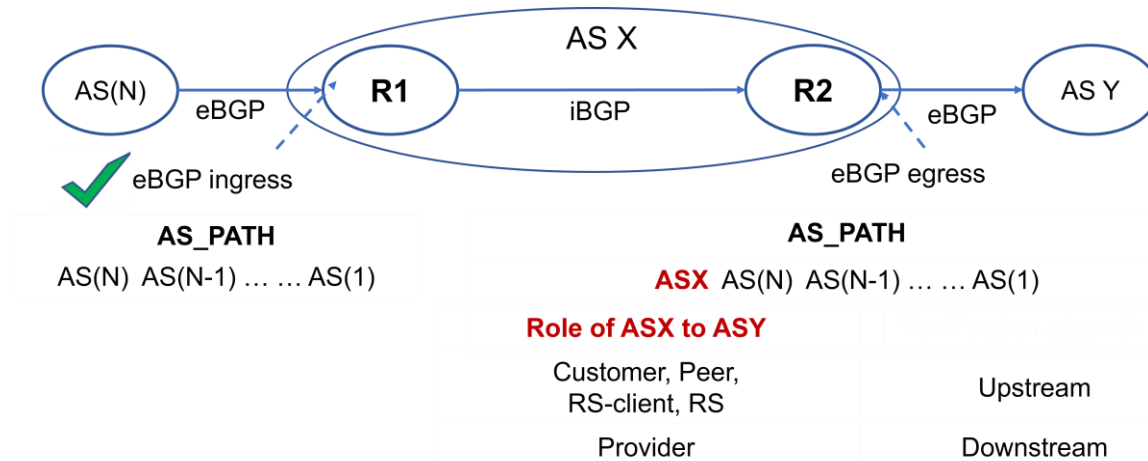
- Clarified the utility of OTC Attribute & handling of Complex BGP Sessions
- Added Optimizations to minimize processing overhead
- Welcome new co-authors: K. Sriram and Nan Geng

- [3. Procedure of ASPA-based AS_PATH Verification at eBGP Egress](#)
 - [3.1. Utility of Only to Customer \(OTC\) Attribute](#)
 - [3.2. Consideration of Complex BGP Sessions](#)
- [4. Optimizations](#)

- **draft-zhang-sidrops-aspa-egress-05** – coming soon

Recap: Verification at eBGP Egress

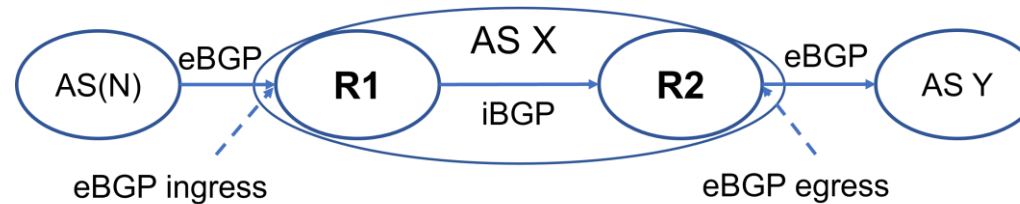
- What is it?
 - Performing ASPA-based AS_PATH verification on outbound eBGP updates (before sending to a neighbor).



- Why do we need it?
 - **Crucial for Partial Deployment Scenarios:** Prevents legacy, un-upgraded ingress routers from leaking invalid routes to eBGP peers.
 - **Prevent Local Misconfigurations:** Stop route leaks or invalid AS_PATHs originating from the local AS before they propagate to the Internet. (Like ROV-egress[RFC8893])
 - **Detect ASPA Registration Errors:** Catch invalid AS_PATHs locally and alert operators early.

New: Positioning Egress ASPA & Synergy with OTC

New Section 3.1 describing role of Egress ASPA and OTC



✓ What R1 Knows

- Direct knowledge of peering relation with AS(N) via local configuration
- Knows if route arrived on P2P vs C2P session

✗ What R2 Doesn't Know

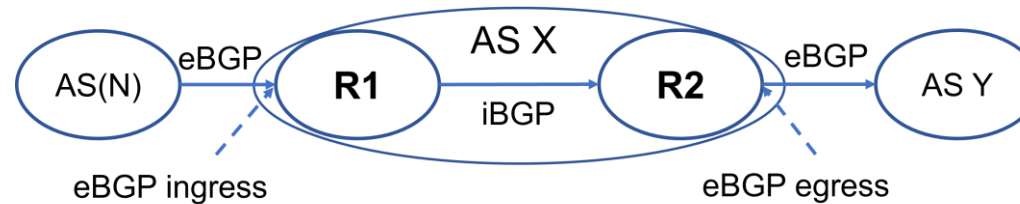
- Cannot distinguish ingress session type, depend on ASPA record
- May produce Valid outcome for route that should be blocked

1. Core Value Proposition: Partial Deployment

- Complementary Role
 - Egress ASPA is designed to complement Ingress ASPA verification.
- Filling the Gap
 - It provides crucial verification coverage during Partial Deployment scenarios (e.g., when the ingress eBGP router is not yet upgraded).

New: Positioning Egress ASPA & Synergy with OTC

New Section 3.1 describing role of Egress ASPA and OTC

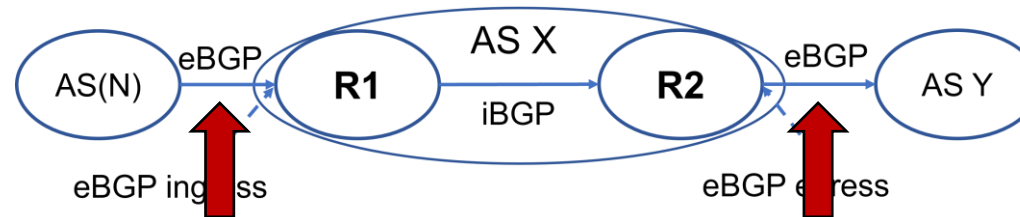


2. Synergy and Fallback with OTC

- Clear Priority (OTC First):
 - R1 MUST attach OTC Attribute on ingress.
 - If OTC is deployed, it MUST NOT be overridden by egress verification.
- Vital Fallback (When OTC is absent):
 - While OTC is highly recommended and likely to be adopted earlier, Egress ASPA serves as a critical alternative and safety net in environments where OTC is not deployed or unavailable.

New: Handling Complex BGP Sessions

New Section 3.2 addressing complex peering relationships



Relationships are not always strictly C2P, P2C, or P2P

Scenario 1: Segregatable

Multiple eBGP sessions can separate complex relationship into normal relationships

Action: Select appropriate algorithm for each session based on its peering relation type

Scenario 2: Non-Segregatable

Complex relationship occurs within a single BGP session

Option A: Apply algorithm on per-prefix basis

Option B: Apply downstream path algorithm to avoid false positives

New: Optimizations

New Section 4 Practical strategies to reduce processing overhead

- The Concern:
 - Redundant workload: Performing ASPA verification at both ingress and egress may increase processing overhead.
- Proposed Optimizations:
 - Opt 1: Centralized Processing for Full Tables
 - Process egress ASPA once centrally for all customer-facing interfaces.
 - Push the verified full table to RIBs-out, saving significant CPU cycles.

Next Steps: Plan for v5

Already worked on it!

- 1.Verification Procedure: Prepend Neighbor AS Option
 - Prepending Neighbor AS enables early detection of local misconfigurations and registration errors.
 - Actively discussing the trade-off between these security benefits and the potential computational overhead.
 - Future Plan: Position this prepending optimization as an **off-line verification process** rather than an **in-line requirement**, aligned with ASPA Ingress Draft (v-23).

Next Steps: Plan for v5

Already worked on it!

- 2.Optimizations: reduce Egress ASPA performance overhead
 - Actively discussing how to reduce Egress ASPA performance overhead while maintaining security benefits.
 - E.g., Partial Verification: Leverage local signaling to reuse known verification outcomes from ingress routers.
- 3. Draft Restructuring & Refining
 - Reorganizing the document.
 - Detailing specific scenarios where Egress checks add value.

We welcome your feedback and suggestions on this draft.

Thank you !

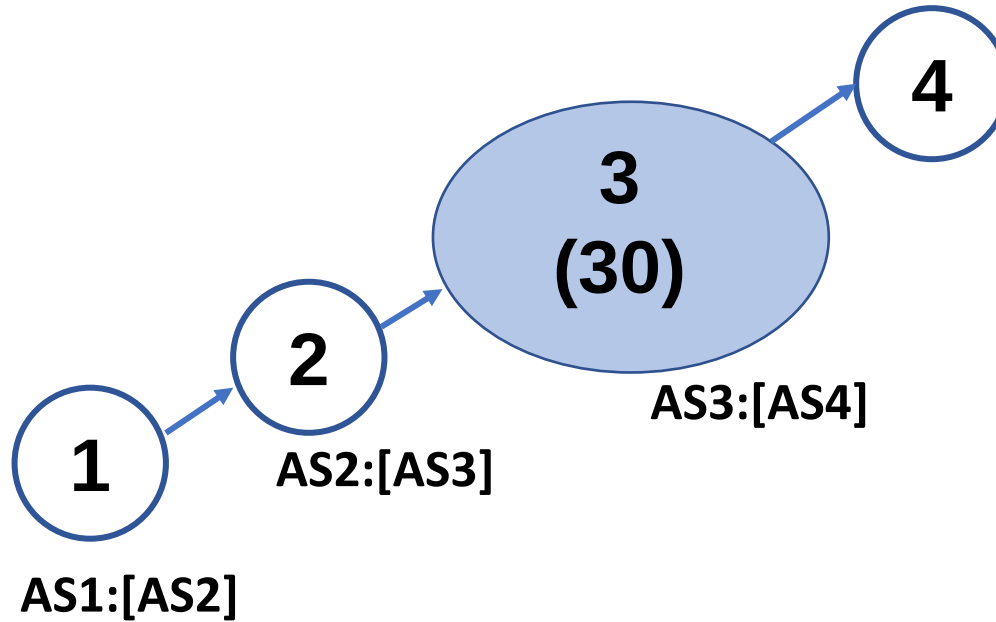
ASPA-based AS_PATH Verification for BGP Export

zhangj@mail.zgclab.edu.cn

IETF 125 SIDROPS Meeting

Scenario 1: Local misconfiguration

If the local AS has multiple AS numbers, AS 3 is used for route advertising, AS 30 is used internally.

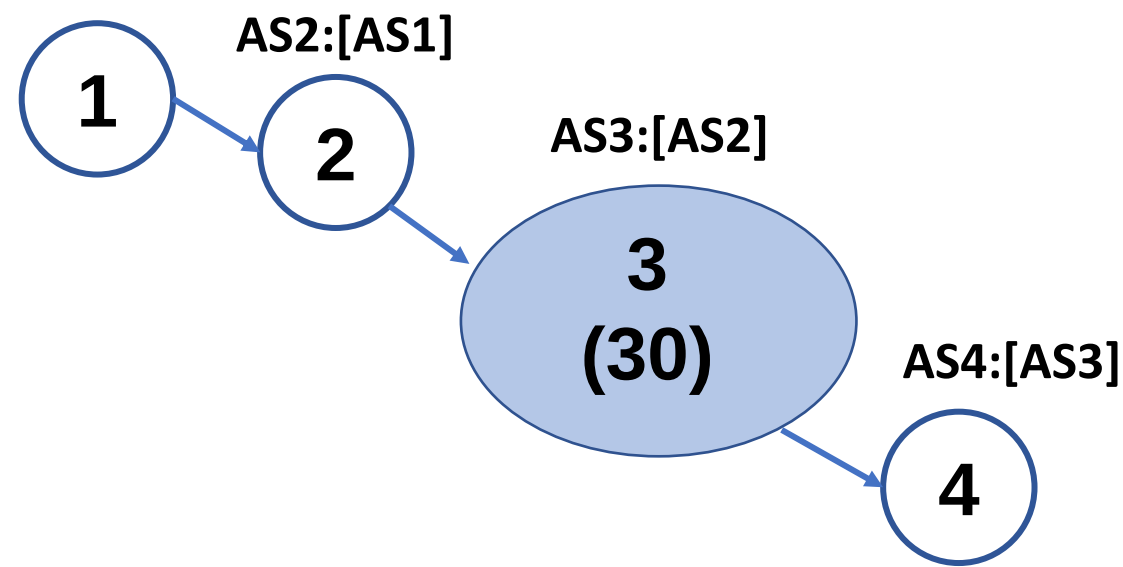


Advertised Route	AS3 egress	AS4 ingress
[AS3 AS2 AS1]✓	Upstream, [AS3 AS2 AS1]	Upstream, [AS4 AS3 AS2 AS1]
	Valid	Valid
[AS30 AS2 AS1]✗	Upstream, [AS30 AS2 AS1]	Upstream, [AS4 AS30 AS2 AS1]
	Invalid	Invalid

Egress verification allows for quick detection of issues and correction of local configuration errors.

Scenario 1: Local misconfiguration

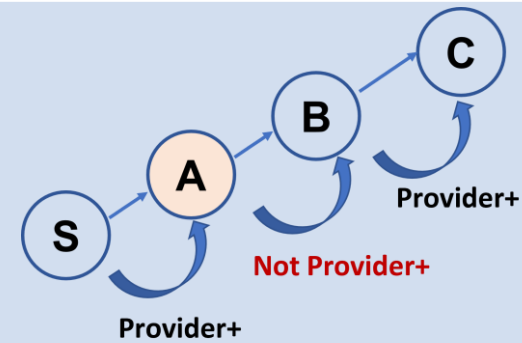
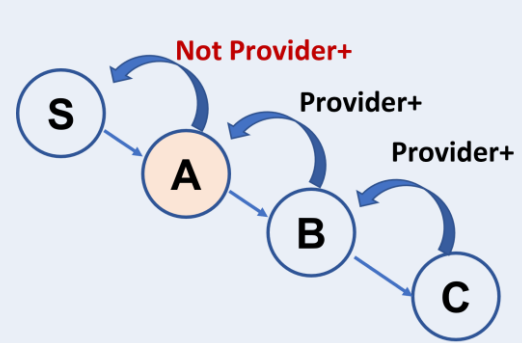
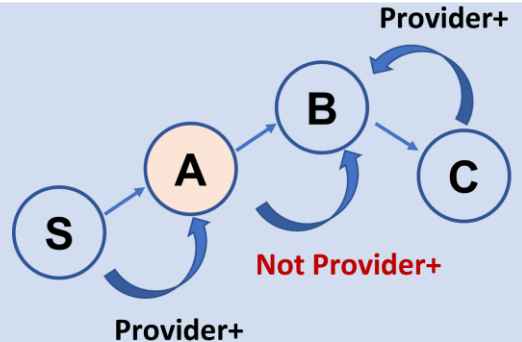
If the local AS has multiple AS numbers, AS 3 is used for route advertising, AS 30 is used internally.



Advertised Route	AS3 egress	AS3 egress with Prepend	AS4 ingress
[AS3 AS2 AS1]✓	Downstream, [AS3 AS2 AS1]	Downstream, [AS4 AS3 AS2 AS1]	Downstream, [AS4 AS3 AS2 AS1]
	Valid	Valid	Valid
[AS30 AS2 AS1]✗	Downstream [AS30 AS2 AS1]	Downstream [AS4 AS30 AS2 AS1]	Downstream [AS4 AS30 AS2 AS1]
	Unknown	Invalid	Invalid

Egress verification with prepending next-hop AS allows for quick detection of issues and correction of local configuration errors.

Scenario 2: Registration Error

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
	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-ingress: Valid S-egress: Invalid A-ingress: Invalid A-egress: Invalid
	peeking point	Can not detect	Can not detect	Can not detect