BGP AS_PATH Verification Based on Route Path Authorizations (RPA)

draft-guo-sidrops-rpa-profile-00
draft-xu-sidrops-rpa-verification-00

Yangfei Guo, Shenglin Jiang

IETF 123 SIDROPS

Jul. 2025

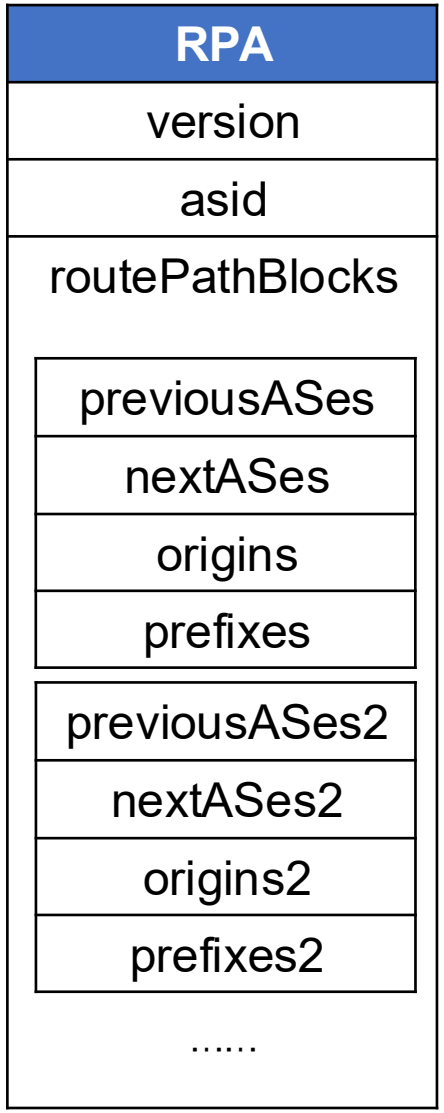
RPA Goals

- Basic BGP route propagation pattern
  - Receive routes from Previous AS and accept them
  - Update routes to Next AS according to local routing policy

- Only three ASes are involved
  - Previous, can be null (i.e., the originator)
  - Local
  - Next, can be null (i.e., the destination)
- Detect route propagation that violates local routing path
- Prevent route leaks
  - Verify the validity of BGP AS_PATH according to RPAs

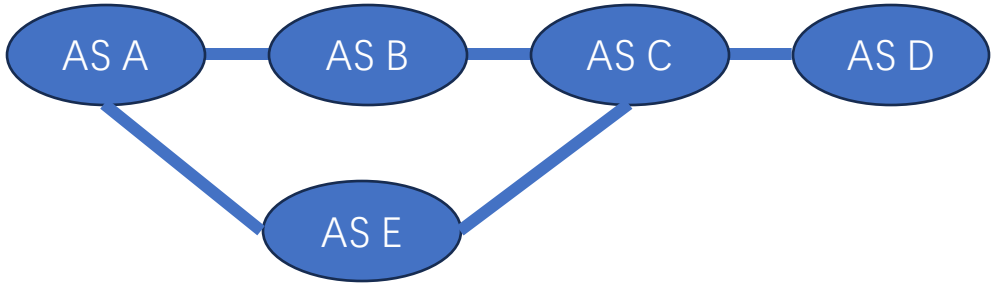
RPA signed object

- IRR-autnum
  - As stated in RFC7682, issues with data quality have limited the practical use of the autnum object's policy attributes
- Route Path Authorizations (RPA)
  - version: 0
  - asid: local AS number, issuer's AS number
  - routePathBlocks: routing path description
    - previousASes: upstream ASes. If it is None, it means local AS is originator
    - nextASes: downstream ASes
    - origins: optional field, origin ASes, references to ROA/SPL/... Default is None for any
    - prefixes: optional field, default is None for any



Register RPAs (1)

Scenario1: The permitted routing path from AS A to AS D is {D, C, B, A} or {D, C, E, A}

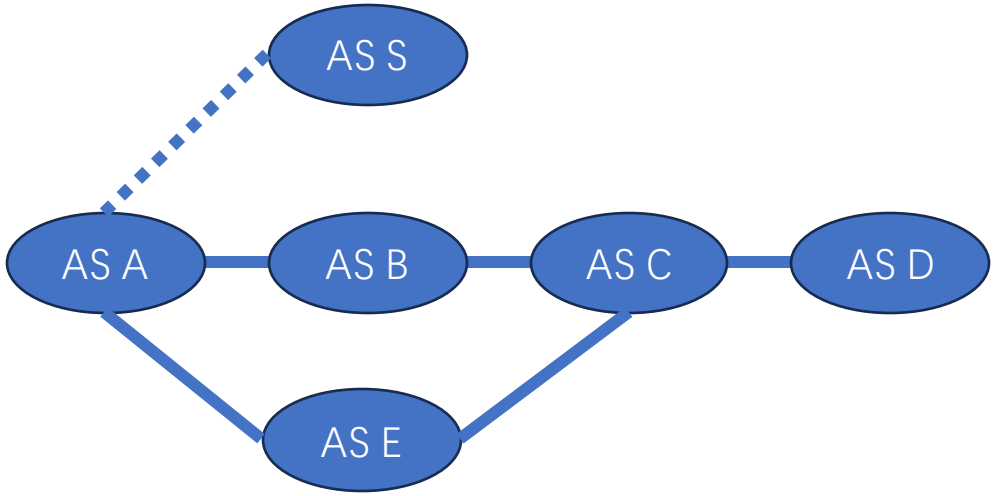


- RPA_A[A, <[], [B, E], [], []>]
- RPA_B[B, <[A], [C], [], []>]
- RPA_E[E, <[A], [C], [], []>]
- RPA_C[C, <[B, E], [D], [], []>]
- RPA_D[D, <[C], [], [], []>

ex. RPA_{ASN} [asid, <[previousASes], [nextASes], [origins], [prefixes]>, ...]

Register RPAs (2)

Scenario2: The prefix belonged to AS S
MUST be routed following this path
{D, C, E, A, ^, S}



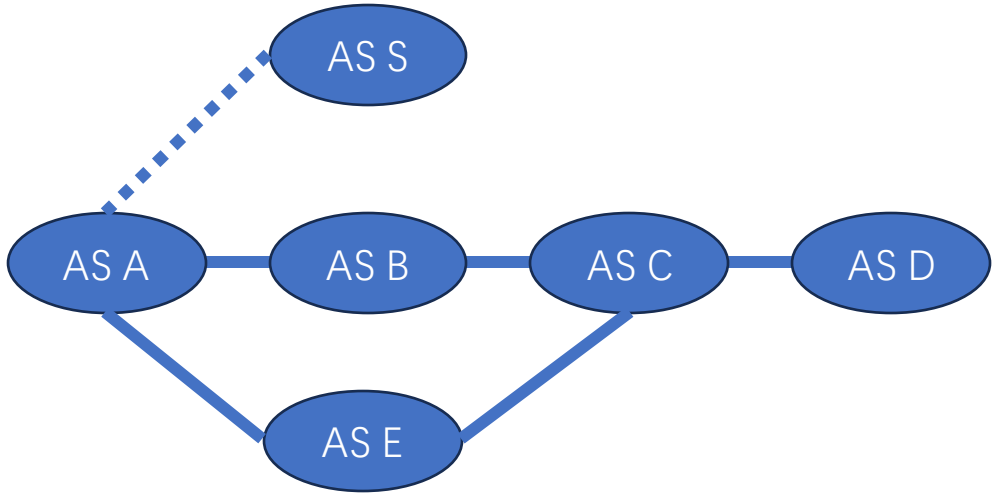
- AS S has registered ROA/SPL
  - $ROA_S[p_S; AS\ S]$ $SPL_S[AS\ S; p_S]$

- RPA_A[A, <[], [B, E], [], []>]
- RPA_B[B, <[A], [C], [], []>]
- RPA_E[E, <[A], [C], [], []>]
- RPA_C[C, <[B, E], [D], [], []>, **<[E], [D], [S], []>**]
- RPA_D[D, <[C], [], [], []>

ex. RPA_{ASN} [asid, <[previousASes], [nextASes], [origins], [prefixes]>, ...]

Register RPAs (3)

Scenario3: The specified prefix p_A **MUST** be routed following this path {D, C, E, A}



- RPA_A[A, <[], [B, E], [], []>]
- RPA_B[B, <[A], [C], [], []>]
- RPA_E[E, <[A], [C], [], []>]
- RPA_C[C, <[B, E], [D], [], []>, <[E], [D], [**S**], []>, **<[E], [D], [], [p_A]>**]
- RPA_D[D, <[C], [], [], []>

ex. RPA_{ASN} [asid, <[previousASes], [nextASes], [origins], [prefixes]>, ...]

Verification

AS_PATH

Step 1
Per-AS:

RPA_A object	
PreviousASes	
NextASes	B,E
Origins	
Prefixes	

VALID ✅

RPA_B object	
PreviousASes	A
NextASes	C
Origins	
Prefixes	

VALID ✅

RPA_C object	
PreviousASes	B,E
NextASes	D
Origins	
Prefixes	

VALID ✅

RPA_D object	
PreviousASes	C
NextASes	
Origin	
Prefix	

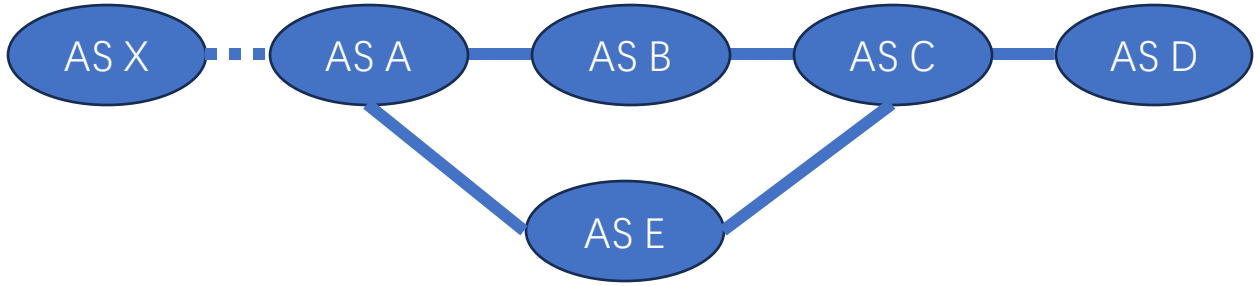
VALID ✅

Step 2
AS_PATH:

VALID ✅

Per-AS verification

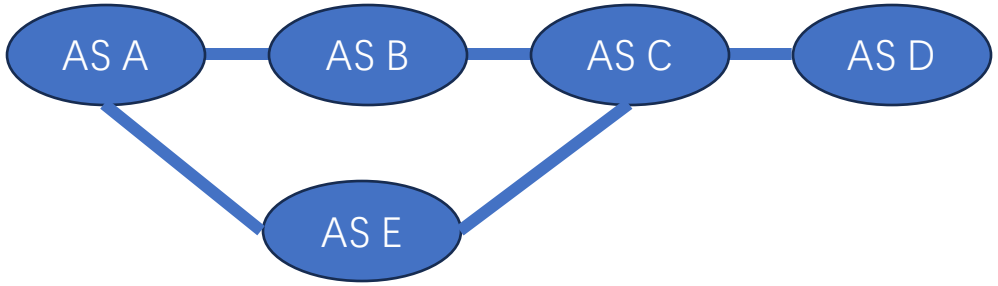
- For example, AS C receives:
  - Prefix: p
  - AS_PATH: {E, A, ^, X}



- **IF** RPA_C is issued
  - **IF** RPA_C contains [C, < previousASes, nextASes, [], prefixes >] **and** $p \in$ prefixes
    - **IF** E ∈ previousASes **and** D ∈ nextASes => **VALID**
    - **ELSE** => **INVALID**
  - **ELIF** RPA_C contains [C, < previousASes, nextASes, origins, []>] **and** X ∈ origins
    - **IF** E ∈ previousASes **and** D ∈ nextASes => **Perform $ROV_X(P)$ and $SPL_X(P)$**
    - **ELSE** => **INVALID**
  - **ELIF** RPA_C contains [C, < previousASes, nextASes, [], []>] **and** E ∈ previousASes **and** D ∈ nextASes => **VALID**
  - **ELSE** => **INVALID**
- **ELIF** RPA_C doesn't be issued
  - => **UNKNOWN**

BGP AS_PATH verification

- For AS_PATH{D, C, B, A}
  - AS D verifies each RPA



- Each RPA verification result is VALID
  - **VALID**
- Any RPA verification result is VALID and others' results are UNKNOWN
  - **WEAKLY VALID**
- Any RPA verification result is INVALID
  - **INVALID**
- Others
  - **UNKNOWN**

Analysis: total number of RPAs

- *Total RPA objects*: One AS only needs to register one RPA object. Refer to the autnum objects[1], it has about 80,000 RPA objects

Table 1: IRRs used, grouped and ordered by priority.

IRR	Size (MiB)	*aut-num*	*route*	*import*	*export*
APNIC	929	20,680	988,665	15,615	15,905
AFRINIC	128	2,314	105,835	331	340
ARIN	33	3,047	94,365	6,940	7,359
LACNIC	11	1,847	12,759	0	0
RIPE	5,184	38,573	533,159	368,008	357,317
IDNIC	4	2,276	6,114	3,918	3,938
JPIRR	3	455	14,013	305	307
RADB	487	9,471	1,619,366	12,655	12,834
NTTCOM	176	549	375,836	921	1,016
LEVEL3	66	300	79,152	6,228	5,826
TC	16	4,205	25,333	3,911	3,964
REACH	15	2	20,238	3	3
ALTDB	8	1,680	29,517	3,241	3,143
Total	7,073	78,701	3,367,914	416,312	405,895

[1] S. He, I. Cunha, and E. Katz-Bassett, “RPSLyzer: Characterization and Verification of Policies in Internet Routing Registries,” in Proceedings of the 2024 ACM on Internet Measurement Conference, in IMC ’24. New York, NY, USA: Association for Computing Machinery, Nov. 2024, pp. 365–374. doi: 10.1145/3646547.3689018.

Q & A

- **Scalability（ RPA object scale） （by Jakob , Job & Sriram ）**

Per-AS has only one RPA object.
The total number of RPA objects is similar to the active AS numbers in the Internet.

- **How does RPA Object get bootstrapped? (by Sriram)**

Each AS needs to register RPA objects based on its own policies and peer relationships.
This is similar to `import / export` policies in aut-num object.

- **Security under partial deployment（ by Randy & Sriram & Chris）**

***Deploying brings immediate benefits**: once an AS is deployed, it can prevent malicious actions from the upstream-AS **and** also prevent route leaks caused by misconfigurations at the downstream-AS.*

- **Compared with ASPA/ASRA, what are the advantages? (by Sriram & Chris & Nan)**

By taking prefixes into consideration, RPA provides more fine-grained anti-hijacking protection and traffic engineering capabilities.

- **Privacy（by Jakob & Chris）**

It is recommended that ASes that are vulnerable to route hijacking or route leaks register first.

Thank you!

Many many thanks to those who give us suggestions and comments:
Jakob Heitz, Job Snijders, Randy Bush, Sriram Kotikalapudi,
Christopher Morrow, Nan Geng, and so on.

IETF 123 SIDROPS

Jul. 2025