

BGP AS_PATH Verification Based on ASPA Objects

<https://datatracker.ietf.org/doc/draft-ietf-sidrops-aspa-verification/>

Presenter: K. Sriram

Authors: A. Azimov, E. Bogomozov, R. Bush, K. Patel, J. Snijders, and K. Sriram

SIDROPS WG Meeting

IETF 117

July 2023

Status

New version 15 of the ASPA-based path verification draft:

<https://datatracker.ietf.org/doc/html/draft-ietf-sidrops-aspa-verification>

New version 16 of the ASPA profile draft:

<https://datatracker.ietf.org/doc/html/draft-ietf-sidrops-aspa-profile>

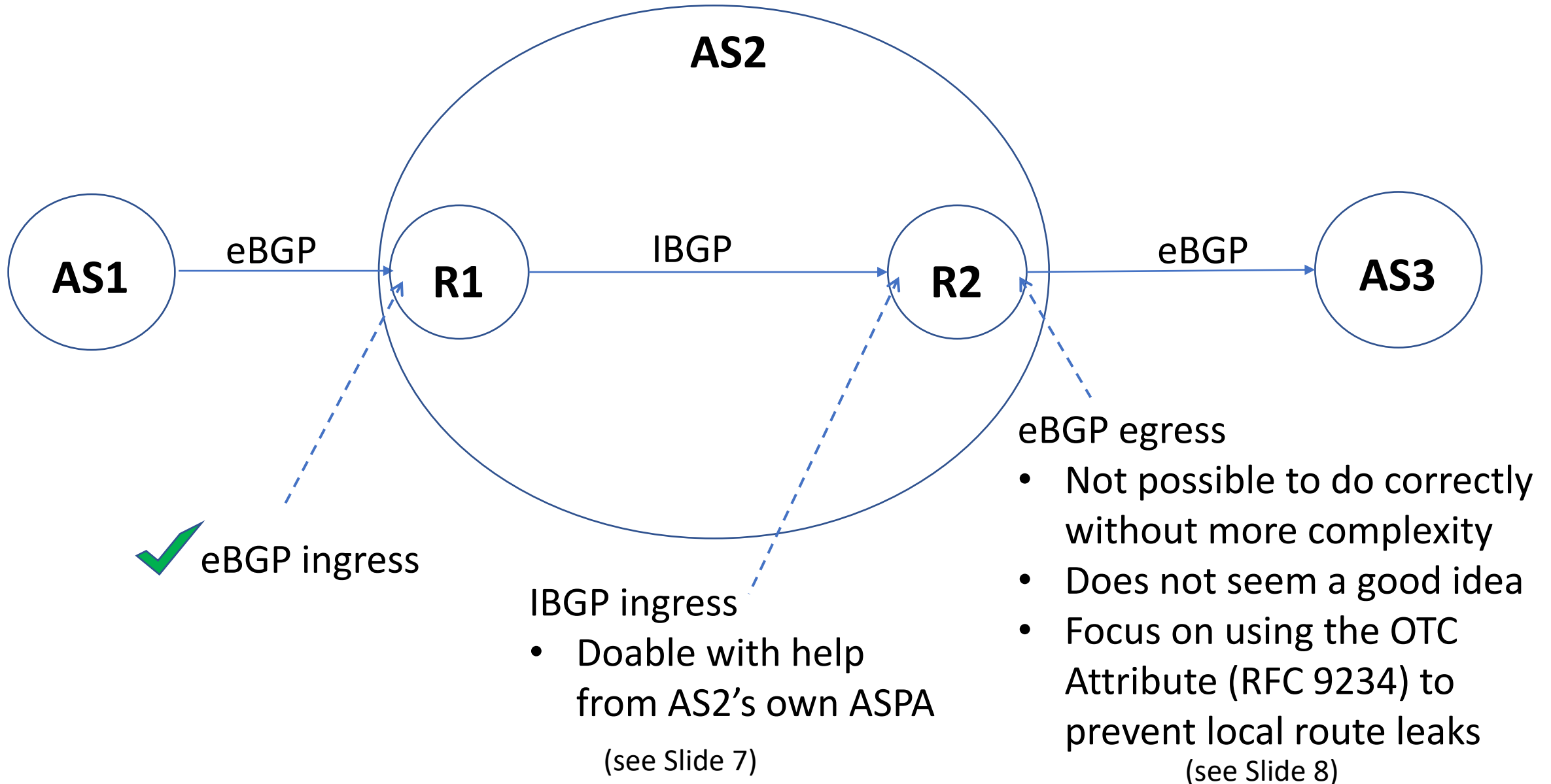
➤ Removes afiLimit

- Many thanks once again for the support during WGLC with comments and suggestions from many SIDROPS members.

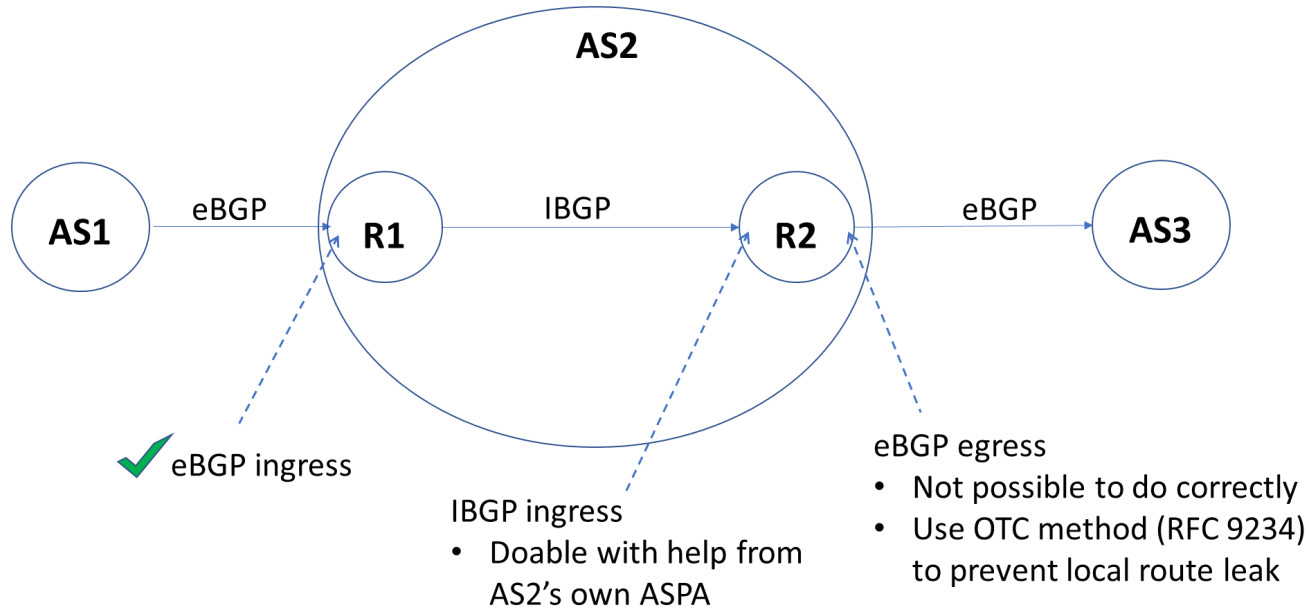
Changes in v-15 of sidrops-aspa-verification draft

- Updates due to the removal of afiLimit from the ASPA profile
- Sections 7 and 8 are better organized
- New Section 7.2 "Verification and Mitigation at Egress eBGP Router"
 - Does not seem like a good idea anymore (see slides 4, 8)
- New Section 9.4 "DoS/DDoS Mitigation Service Provider" added
- Other edits for text improvements

Considerations for Verification in IBGP and at eBGP Egress



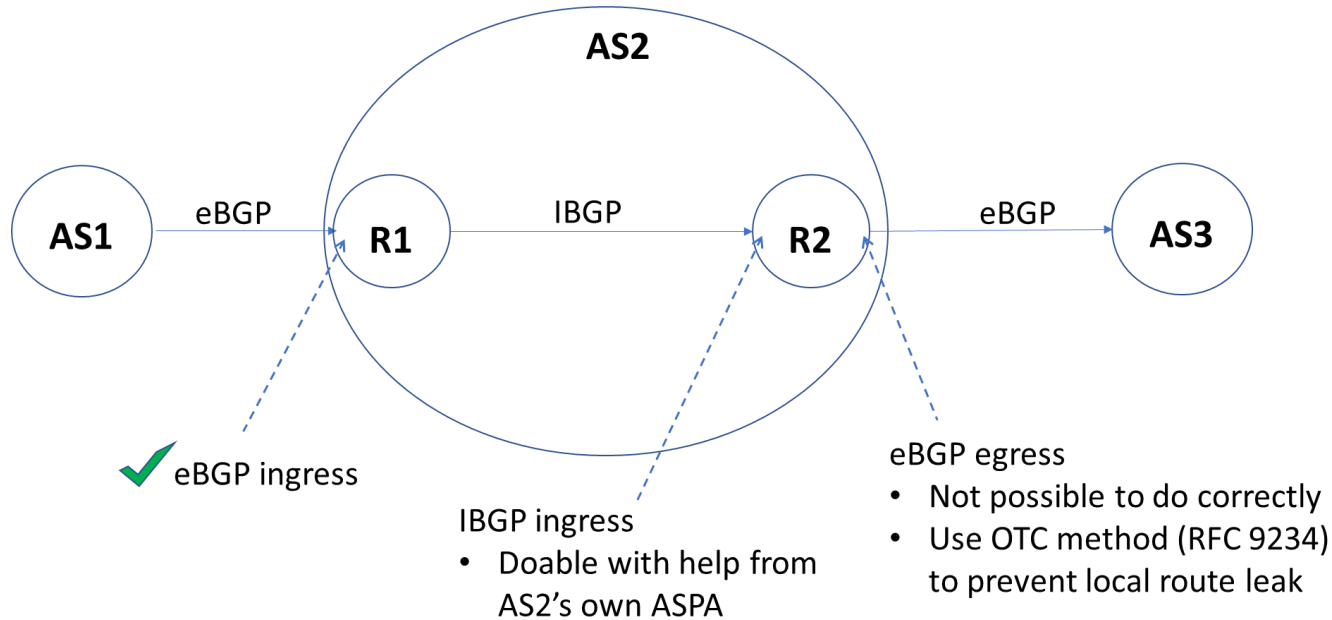
Considerations for Verification in IBGP



- Authors will try to discuss it this week and decide

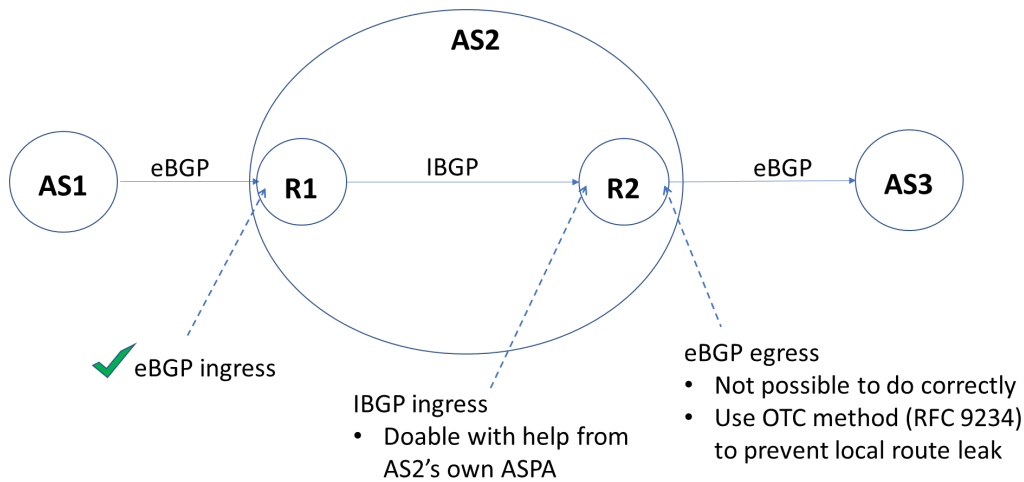
Backup slides (for discussion)

Verification in IBGP



- Seems possible to do it correctly
- R2 looks up AS2's own ASPA
 - If AS1 is listed as a Provider, then apply the Downstream algorithm
 - If AS1 is not listed as a Provider, then apply the Upstream algorithm
 - Works correctly, including RS and RS-client scenarios

Verification at eBGP Egress: Not a good idea



- To try to do this, R2 would add its own AS (i.e., AS2) to the AS_PATH, then perform verification using Section 7.2 (v-15 draft), and decide to propagate or not (to AS3)
- But the preceding AS (i.e., neighbor AS1) may be a lateral peer or provider and not have an ASPA registered
 - This could cause R2 to evaluate the path as Unknown (rather than Invalid) and propagate causing a route leak
- R1 can send a signal (Community) to R2 to convey the configured relationship with AS1 but that adds more complexity
- All that is needed is the ability to prevent a local route leak at AS2 and the OTC Attribute based filtering (RFC 9234) serves the purpose well!

Possible Recommendations

- Verification in IBGP – we can decide ‘Yes’ (IMO)
- Verification on eBGP egress – runs into issues
- OCT Attribute based filtering (RFC 9234) serves the purpose to prevent local route leaks
- Emphasize that an AS compliant with this RFC-to-be is expected to:
 - Register ASPA
 - Perform verification (eBGP ingress and IBGP)
 - Perform OCT Attribute based filtering (RFC 9234)