# Draft Update: ASPA-based AS Path Verification

K. Sriram

Email: ksriram@nist.gov

IETF SIDROPS Meeting, IETF 123, July 2025

"BGP AS_PATH Verification Based on Autonomous System Provider Authorization (ASPA) Objects,"
https://datatracker.ietf.org/doc/draft-ietf-sidrops-aspa-verification/

Acknowledgements: Thanks to Maria Matejka, Jia Zhang, and others for the discussions.

# Updated Test Cases for ASPA-based AS Path Verification Implementations

- A slightly updated list of test cases is available at:

  https://github.com/ksriram25/IETF/blob/main/ASPA_path_verification_examples.pdf

- There was a typo (now fixed) that was causing a mismatch in implementation testing for one case. Jakob noticed it first.

- Several implementations have verified correctly against the test cases: Cisco, BIRD (cz.nic), APNIC POC, BGP-SRx (NIST), RTRlib (TU Dresden) (to be confirmed)

# How best to deal with network operator error in creation of ASPA?

SIDROPS list discussion threads:

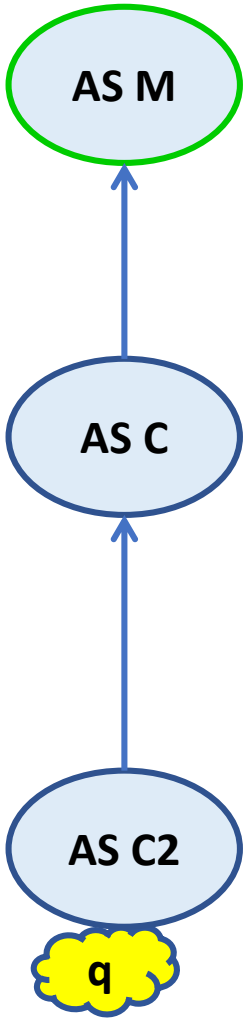
https://mailarchive.ietf.org/arch/msg/sidrops/ng_HTmYkIyp9sprB5bKk-K9UYLA/

https://mailarchive.ietf.org/arch/msg/sidrops/Rcgnx8p4JaZZTJYqJE4OFRic3r8/

# Customer AS Creates Faulty ASPA: Omits Provider

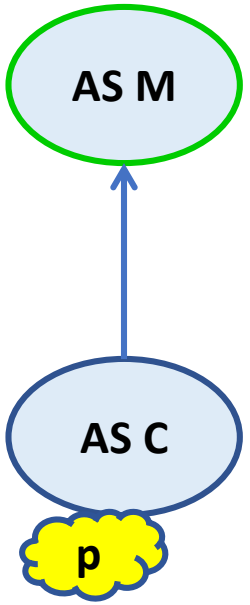
Customer's customer makes error

- ASPA verification detects Invalid route and marks it ineligible
- No issues




**Faulty ASPA: AS C2, {AS X}**

Direct customer makes error




**Faulty ASPA: AS C, {AS W}**

- ASPA verification does not label this route Invalid at AS M
- Long standing customer with established BGP session
- Provider would want to avoid cutting off the customer
- Fix the ASPA error asap in co-ordination with the customer
- Better yet, proactively prevent such errors from happening

# Efficacy of Ingress Verification plus OTC

- ASPA draft specifies using ingress verification plus OTC
- If ASPA error of omission is prevented, then ingress verification + OTC inherently work to prevent sending Invalid routes at egress.
- Multiple proactive methods for detecting mismatch between BGP session configuration and ASPA should be available. The draft describes/will describe them. That also makes sure that OTC Attribute errors are prevented.

# Proactive Measures to Prevent Mismatch Between BGP Session Configuration and ASPA (1 of 3)

- Each AS periodically monitors relevant ASPAs in global RPKI repositories and checks that:
  1. All their Provider ASes are included in their own ASPA.
  2. Their AS number is included in the SPAS of their Customer ASes.
  3. Their own ASPA and their Customer ASPAs are consistent with their BGP Role configurations.

# Proactive Measures to Prevent Mismatch Between BGP Session Configuration and ASPA (2 of 3)

- Implementation can optionally make available a tool to detect mismatch between BGP session configuration and ASPA.
- For customer interfaces, it can form a test path that is {local AS, customer AS} and does an upstream path verification on this path. If Invalid, that alerts about a mismatch.
- For provider interfaces, it can form a test path that is {provider AS, local AS} and does an upstream path verification on this path. If Invalid, that alerts about a mismatch.

# Proactive Measures to Prevent Mismatch Between BGP Session Configuration and ASPA (3 of 3)

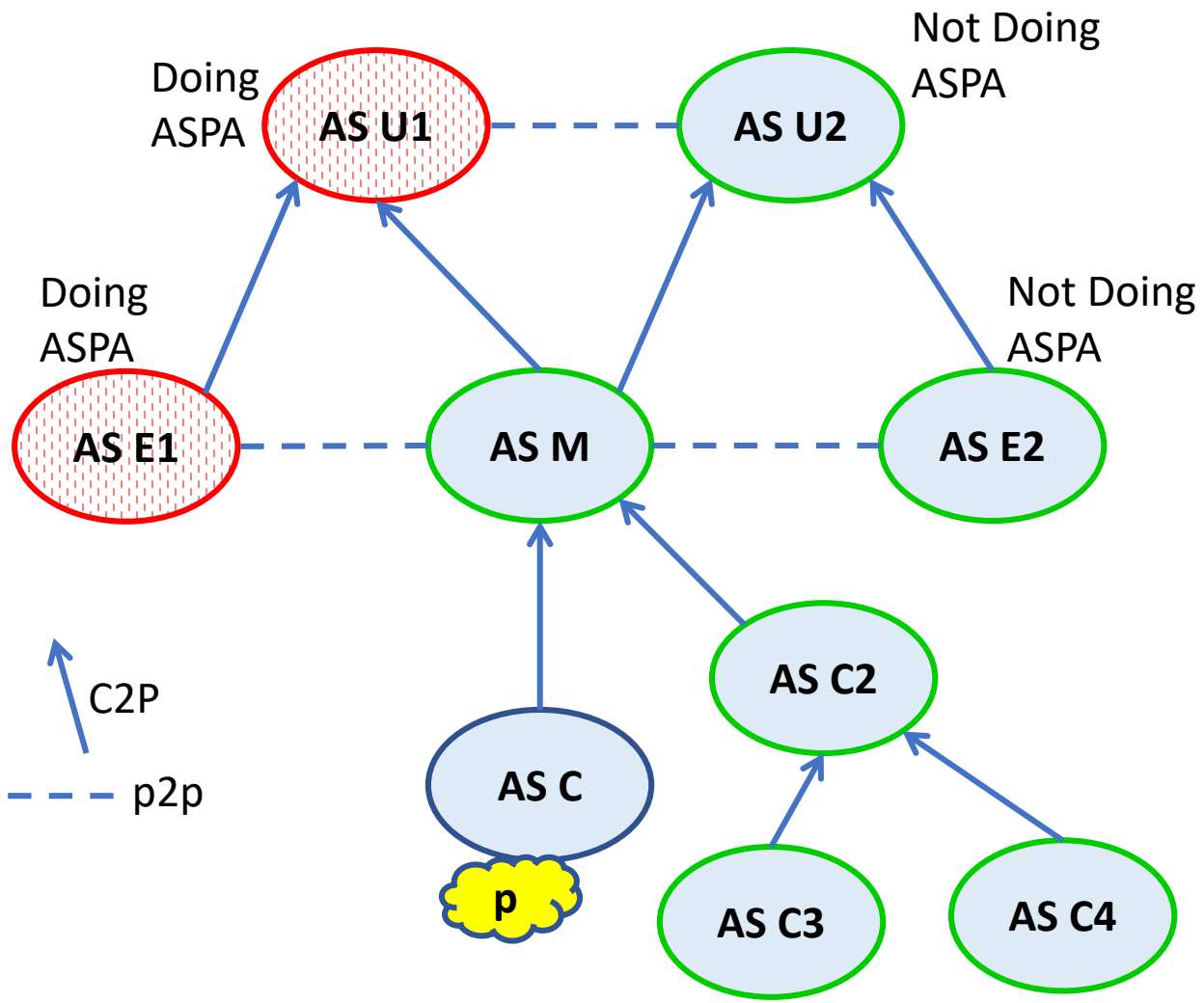
- Encourage the development and use of features in ASPA creation systems (e.g., RIR hosted systems, delegated CAs) that would preview and warn the user that the ASPA they are about to create would render some existing routes invalid.
- Encourage tools that provide continuous monitoring of ASPA invalid routes from global BGP trace data.

Note: Some ASes and their historical (or backup) neighbor relations may be hidden from the BGP trace data

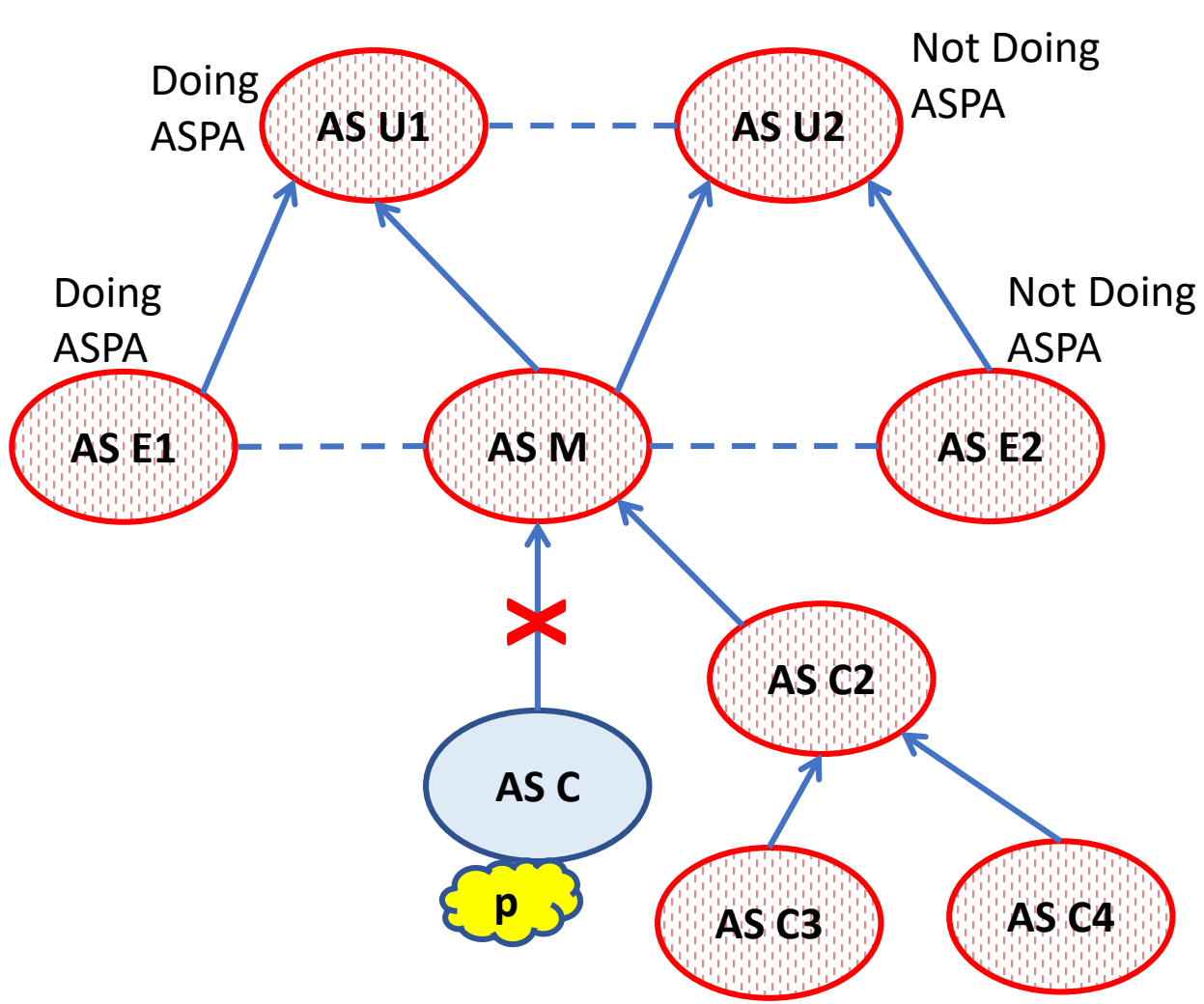
# Backup Slides

# Transient State - Single-Homed Customer

**Continue BGP session, fix ASPA error asap**




**Terminate BGP session**

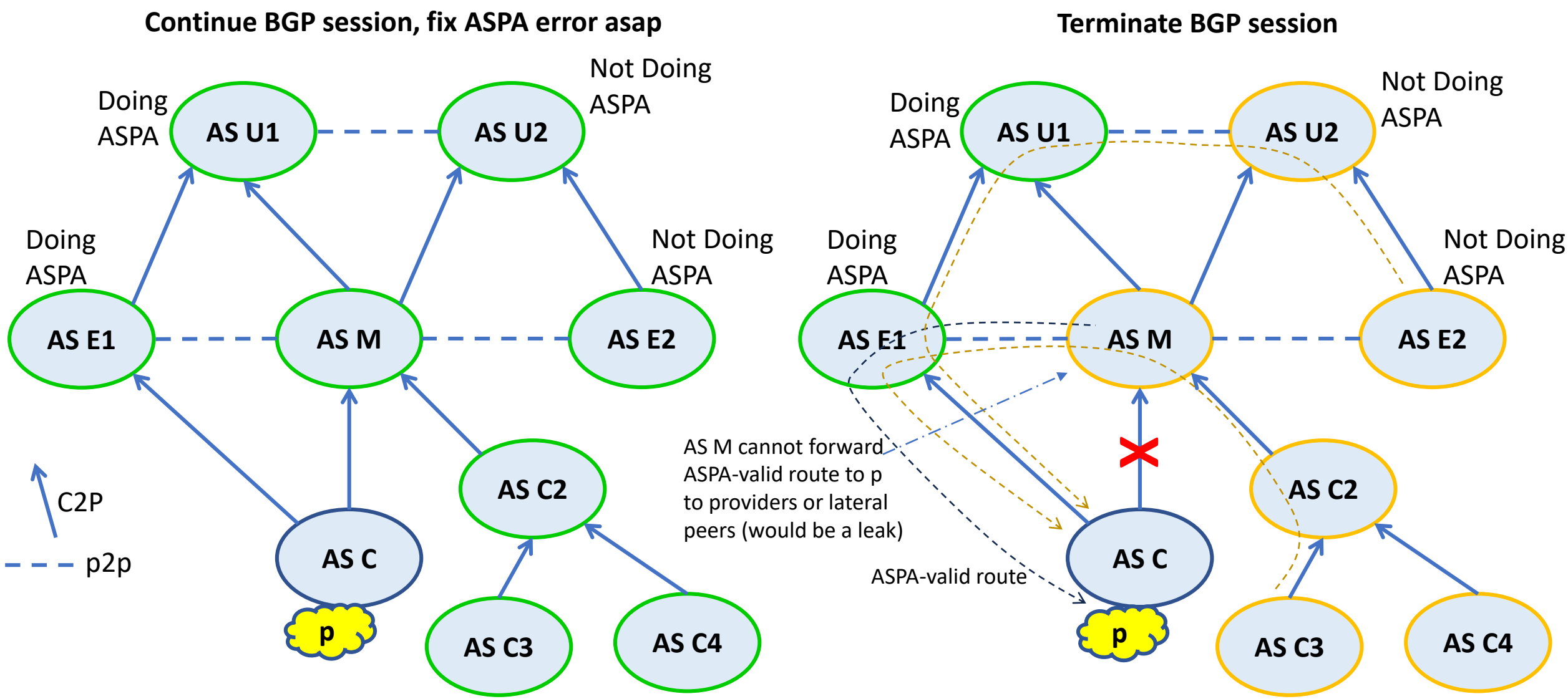



**Faulty ASPA: AS C, {AS W}**
**(AS M is missing erroneously)**

p is unreachable

p is reachable

# Transient State - Multi-Homed Customer




**Faulty ASPA: AS C, {AS W, AS E1}**
**(AS M is missing erroneously)**

p is unreachable

p is reachable

p is reachable via longer path