Route Leaks Solution

Merger of RLP and eOTC Drafts

ietf-idr-route-leak-detection-mitigation-09

K. Sriram (Ed.), A. Azimov (Ed.), D. Montgomery, B. Dickson, K. Patel, A. Robachevsky, E. Bogomazov, and R. Bush

IDR Working Group Meeting, IETF-102
July 2018

Acknowledgements: The authors are grateful to many folks in various IETF WGs for commenting, critiquing, and offering very helpful suggestions (see acknowledgements section in the draft.)

Draft Merger Efforts

- Authors from the two drafts met in Chicago (March 2017) and in London (March 2018)
- Support and encouragement from IDR Chairs John and Sue, and Ignas
- Productive authors' meeting in London (IETF 101) followed by substantial discussions via email
- Authors happy to report on convergence to a merged solution and draft

Merged Solution and Design Discussion Drafts

- Merged Solution: https://tools.ietf.org/html/draft-ietf-idr-route-leak-detection-mitigation-09

- Design Discussion: https://tools.ietf.org/html/draft-sriram-idr-route-leak-solution-discussion-00

Format of RLP Attribute

Optional Transitive Attribute

Design A (original RLP)

ASN: N	Most Recently Added
RLP: N	
⋮	
ASN: 2	
RLP: 2	
ASN: 1	Least Recently Added
RLP: 1	

UP: RLP = 0 DOWN/LATERAL: RLP = 1

Design B

ASN: N	Most Recently Added
⋮	
ASN: 2	Least Recently Added
ASN: 1	

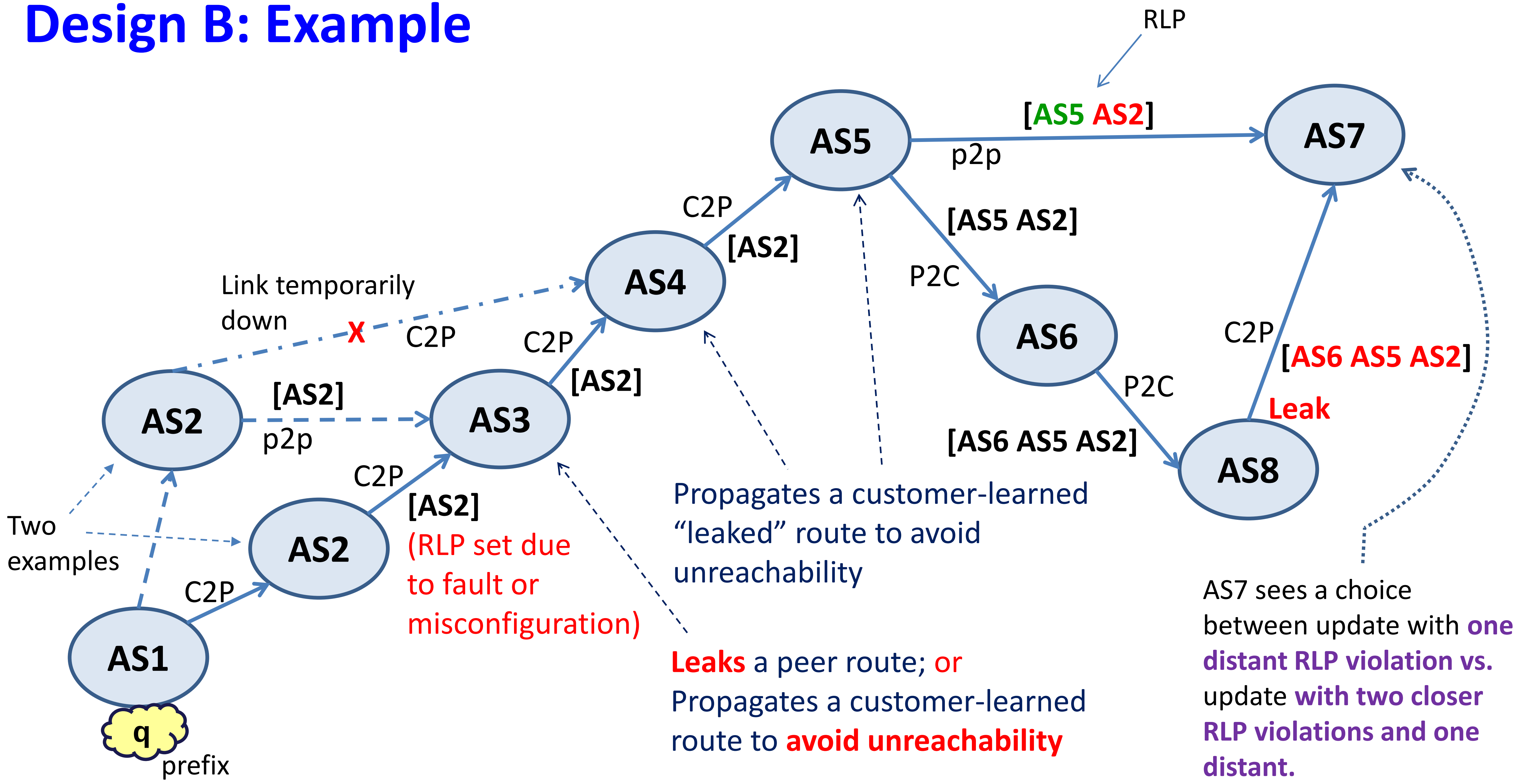
- **eOTC: Design B with only one ASN in the attribute is the original eOTC**

Comparison / Tradeoffs

	Design A (Original RLP)	Design B	Original eOTC (Design B with only one ASN)
Functionality	• Detect multiple leaks • Provide up link info also	• Detect multiple leaks • Only down/peer info	• Can't detect multiple leaks • Lack of differentiation in some cases
Detection / mitigation stength	Best	Very good	See above
Memory use* (per update)	~ 136 bytes	~ 72 bytes	~ 32 bytes

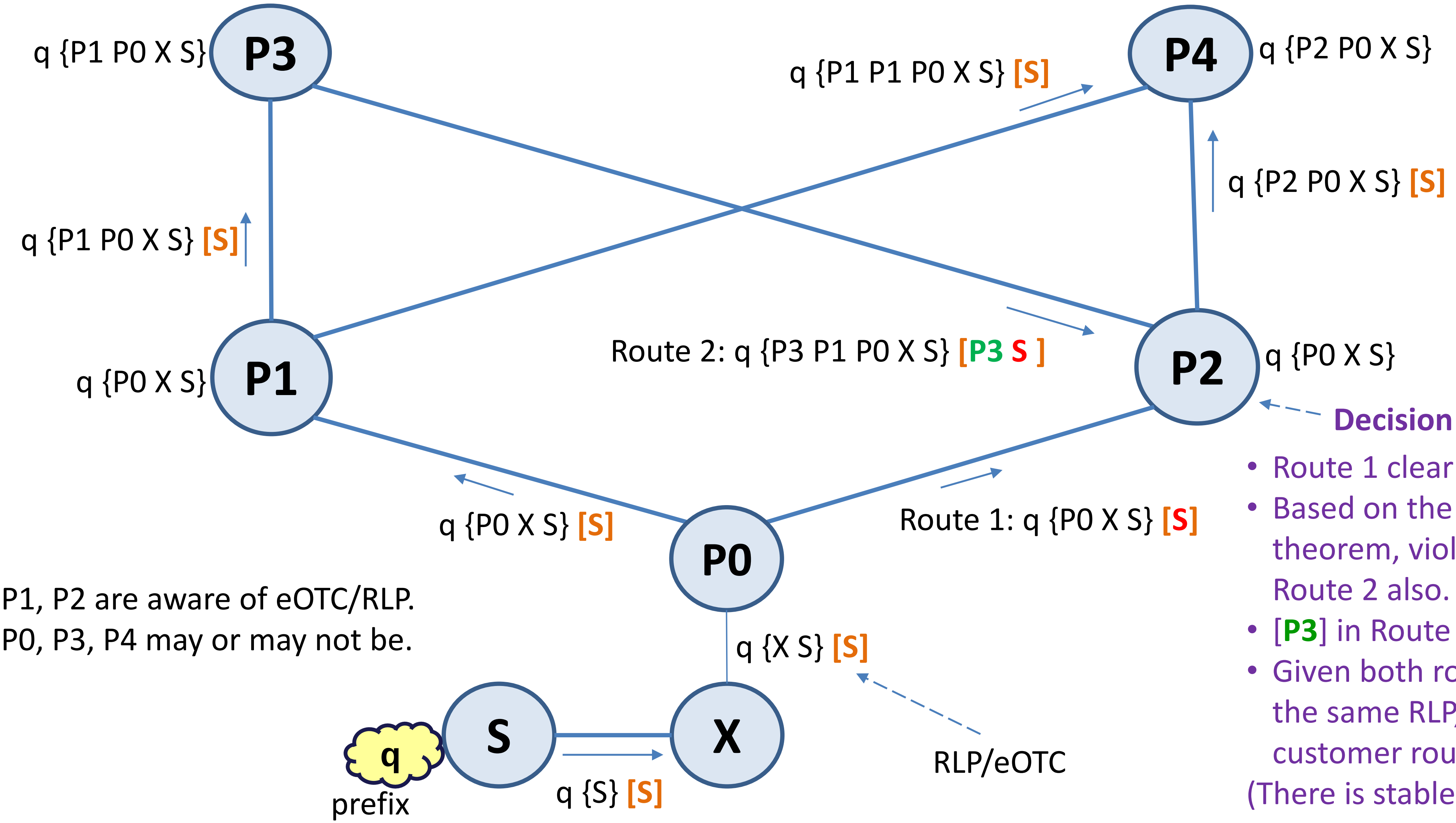
* Assume average 4 hop AS path

Design B: Example



Alexander's scenario:

Avoid Persistent Oscillation Possibility



P1, P2 are aware of eOTC/RLP.
P0, P3, P4 may or may not be.

Decision Policy (Algorithm):

- Route 1 clearly violated [S].
- Based on the route-leak detection theorem, violation of [S] applies to Route 2 also.
- [P3] in Route 2 is expected (good).
- Given both routes are in violation of the same RLP, P2 prefers the customer route.

(There is stable convergence.)

Examine Provider Route vis-à-vis Customer’s

- If customer route is a leak, and alternative route via provider includes the customer AS in the path, then prioritize customer route over the provider route.

* Stated simply here. See formal statement and explanation in the drafts.

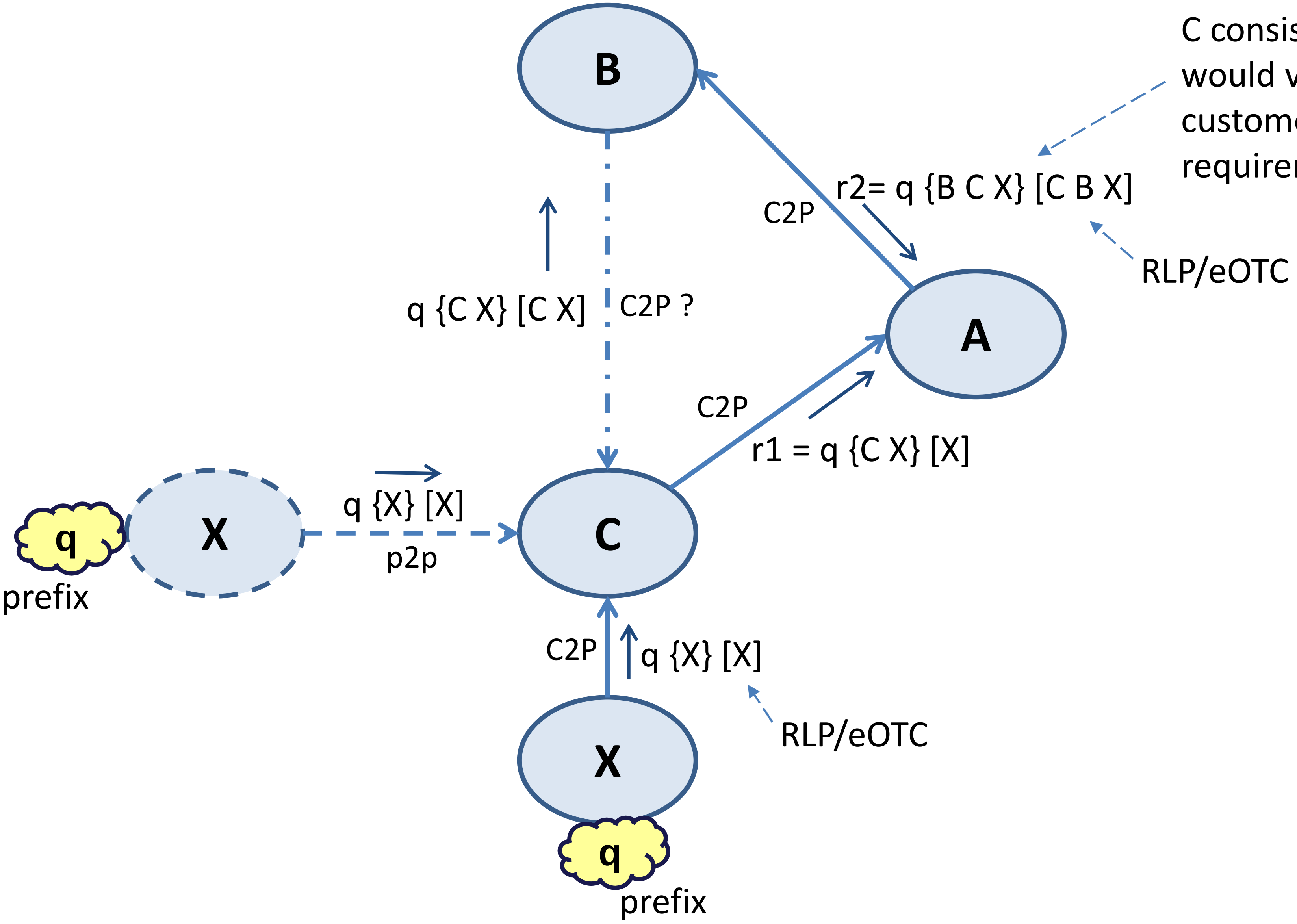
Next Steps

- Request WG feedback on Design A vs. Design B
    - How much utility for the additional information in the RLP attribute in Design A?
        - Indicating when update is sent to transit provider
- Request WG feedback on Attribute vs. Community
- Prepare a finalized version for WGLC

Backup slides

Route-Leak Detection Theorem: Illustration

The only possible way that [X] is not violated in r2 is if the path from B to C consists of C2P links only. But that would violate the "No cycle of customer-provider relationships" requirement [Gao-Rexford].



Route-Leak Detection Theorem

The "Gao-Rexford" Stability Conditions

[Gao-Rexford] http://www.cs.princeton.edu/courses/archive/spr11/cos461/docs/lec17-bgp-policy.ppt (slide 27)

- Topology condition (acyclic)
  - No cycle of customer-provider relationships

Route-Leak Detection Theorem: Let it be given that ISP A receives a route r1 from customer AS C and another route r2 from provider AS B (for the same prefix), and both routes r1 and r2 contain AS C and AS X in the path and also contain [X] in their RLP/eOTC. Then, clearly r1 is in violation of [X]. It follows that r2 is also necessarily in violation of [X].

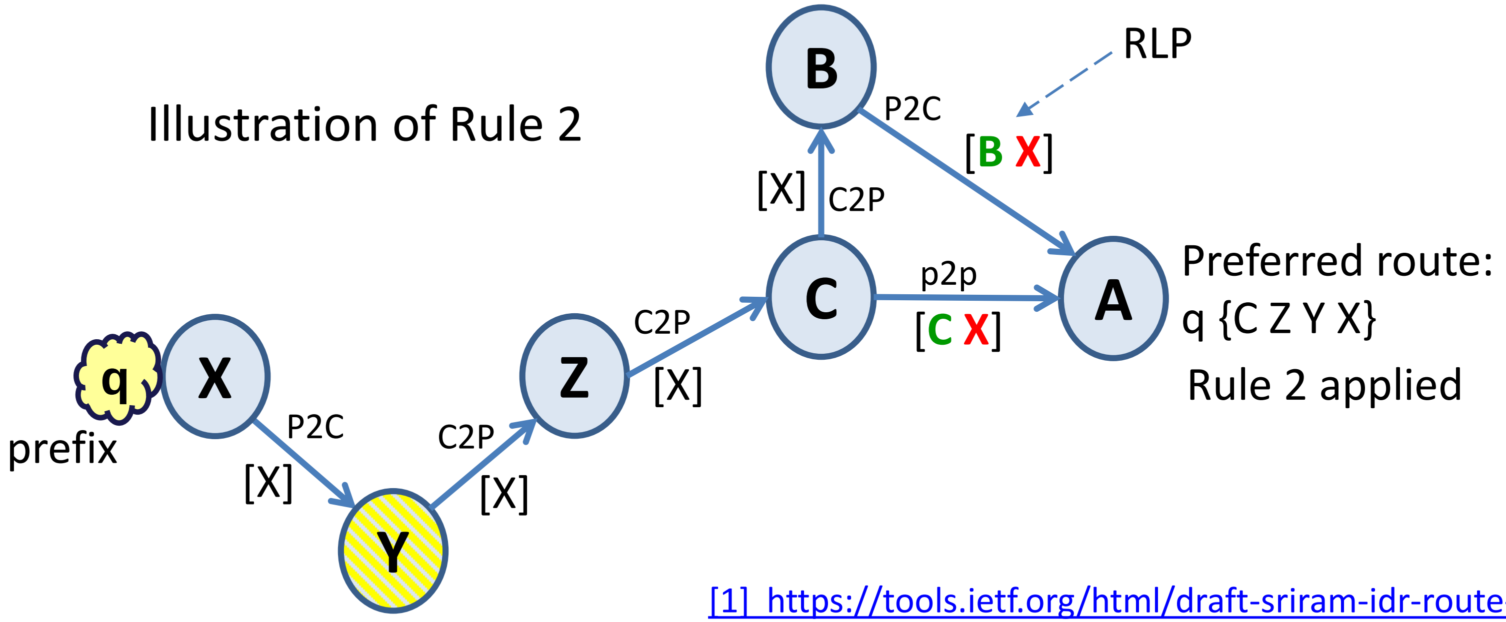
Proof: Let us suppose that r2 is not in violation of [X]. That implies that r2's path from C to B to A included only P2C links. That would mean that there is a cycle of customer-provider relationships involving the ASes in the AS path in r2. However, any such cycle is ruled out in practice as a necessary stability condition [Gao-Rexford]. QED.

Route-Leak Mitigation Rules

Rule 1: If ISP A receives a route r1 from customer AS C and another route r2 from provider (or peer) AS B (for the same prefix), and both routes r1 and r2 contain AS C and AS X (any X not equal to C) in the path and also contain [X] in their RLP, then prioritize the customer (AS C) route over the provider (or peer) route.
(Rationale: This rule is based on the theorem (slide 8). See detailed rationale in Section 3.1 in [1].)

Rule 2: If ISP A receives a route r1 from peer AS C and another route r2 from provider AS B (for the same prefix), and both routes r1 and r2 contain AS C and AS X (any X not equal to C) in the path and also contain [X] in their RLP, then prioritize the peer (AS C) route over the provider (AS B) route.
(Rationale: See illustration below. See detailed rationale in Section 3.1 in [1].)

Illustration of Rule 2



[1] https://tools.ietf.org/html/draft-sriram-idr-route-leak-solution-discussion-00

Default Route-Leak Mitigation Policy

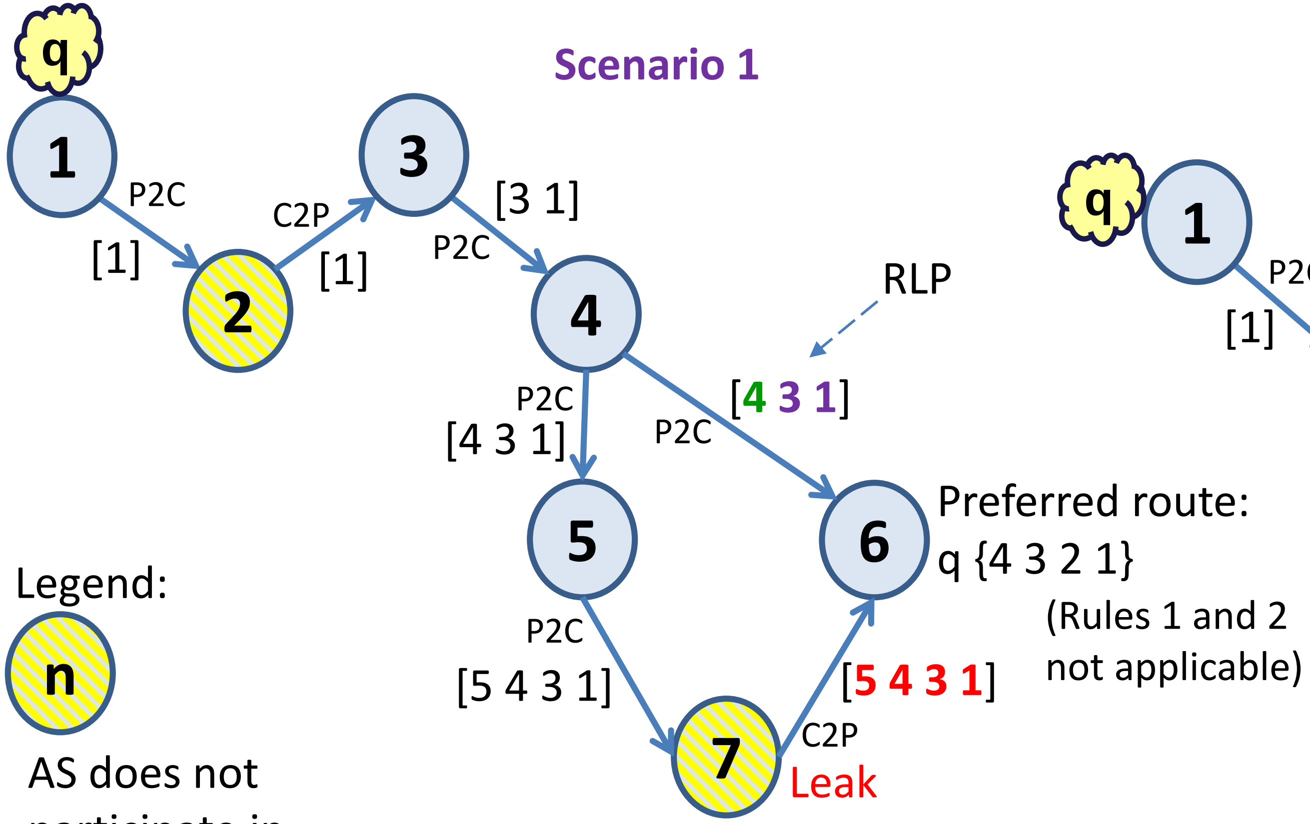
- **Given a choice between a customer route versus a provider (or peer) route,**
  - if no route leak is detected in the customer route, then prioritize the customer over the provider (or peer);
  - else (i.e., when route leak is detected in the customer route) and the conditions of Rule 1 apply, then too prioritize the customer over the provider (or peer);
  - else (i.e., when route leak is detected in the customer route and the conditions of Rule 1 DO NOT apply), then prioritize the provider (or peer) over the customer.

- **Given a choice between a peer route versus a provider route*,**
  - if no route leak is detected in the peer route, then prioritize the peer over the provider;
  - else (i.e., when route leak is detected in the peer route) and the conditions of Rule 2 apply, then too prioritize the peer over the provider;
  - else (i.e., when route leak is detected in the peer route and the conditions of Rule 2 DO NOT apply), then prioritize the provider over the peer.

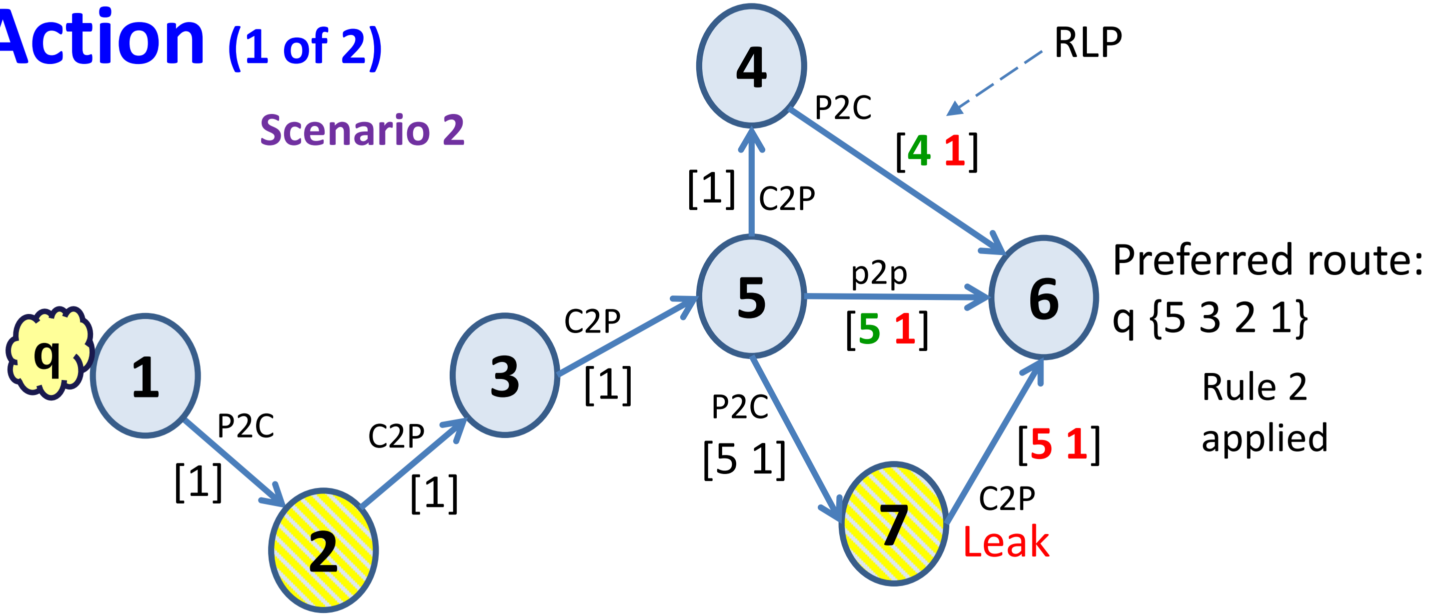
* Operator MAY override (the second bullet) to prefer provider route over peer route.

Examples Showing Policy in Action (1 of 2)

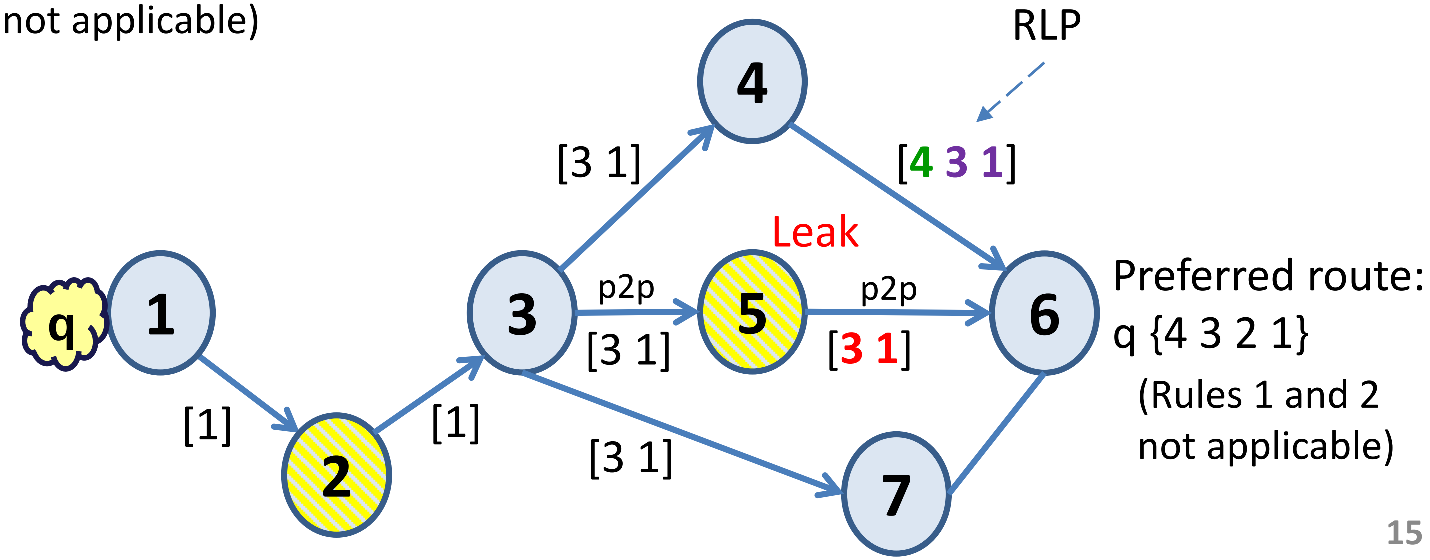
Scenario 1



Scenario 2



Scenario 3



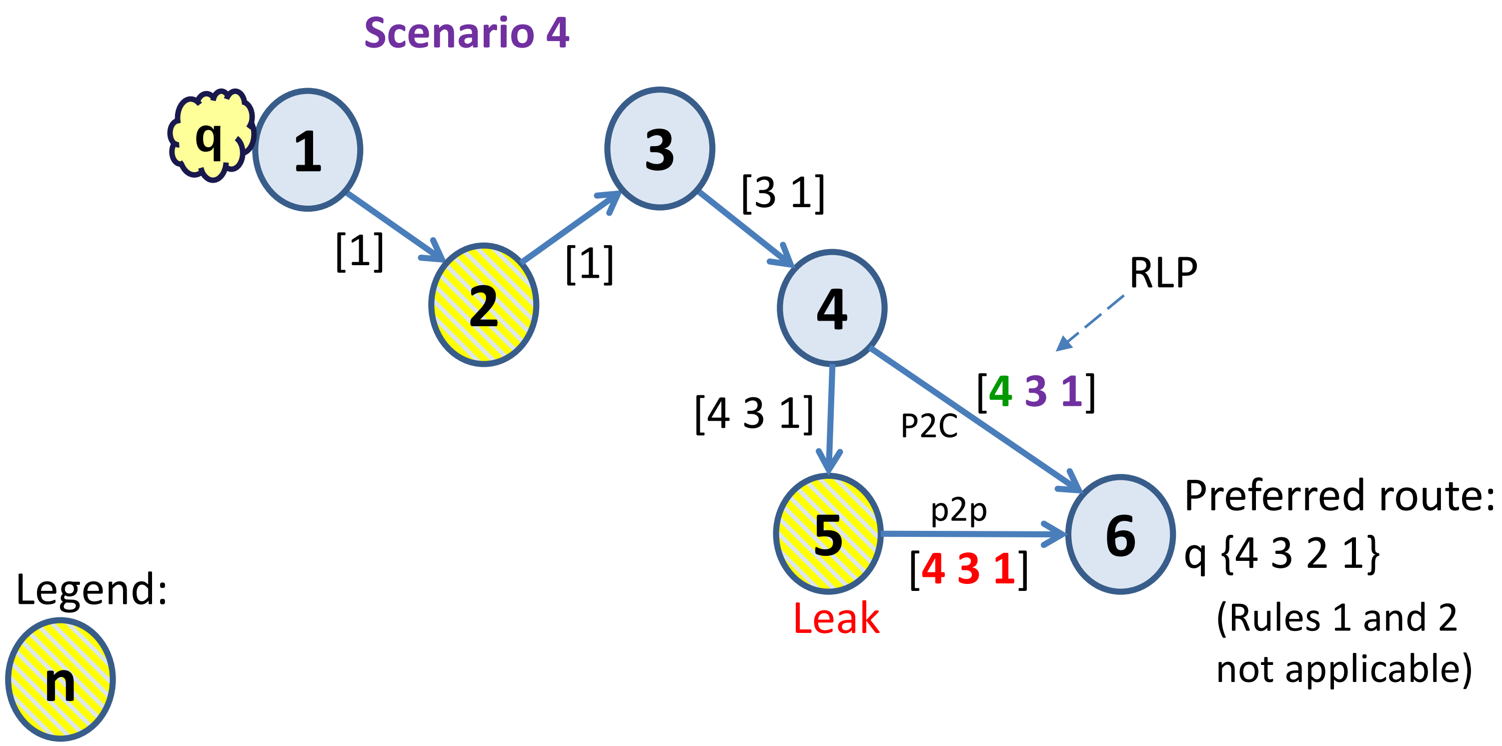
Legend:

n

AS does not participate in RLP and/or Propagates a route that violates RLP

Green – not violation
Red – violation
Purple – can't tell

Examples Showing Policy in Action (2 of 2)

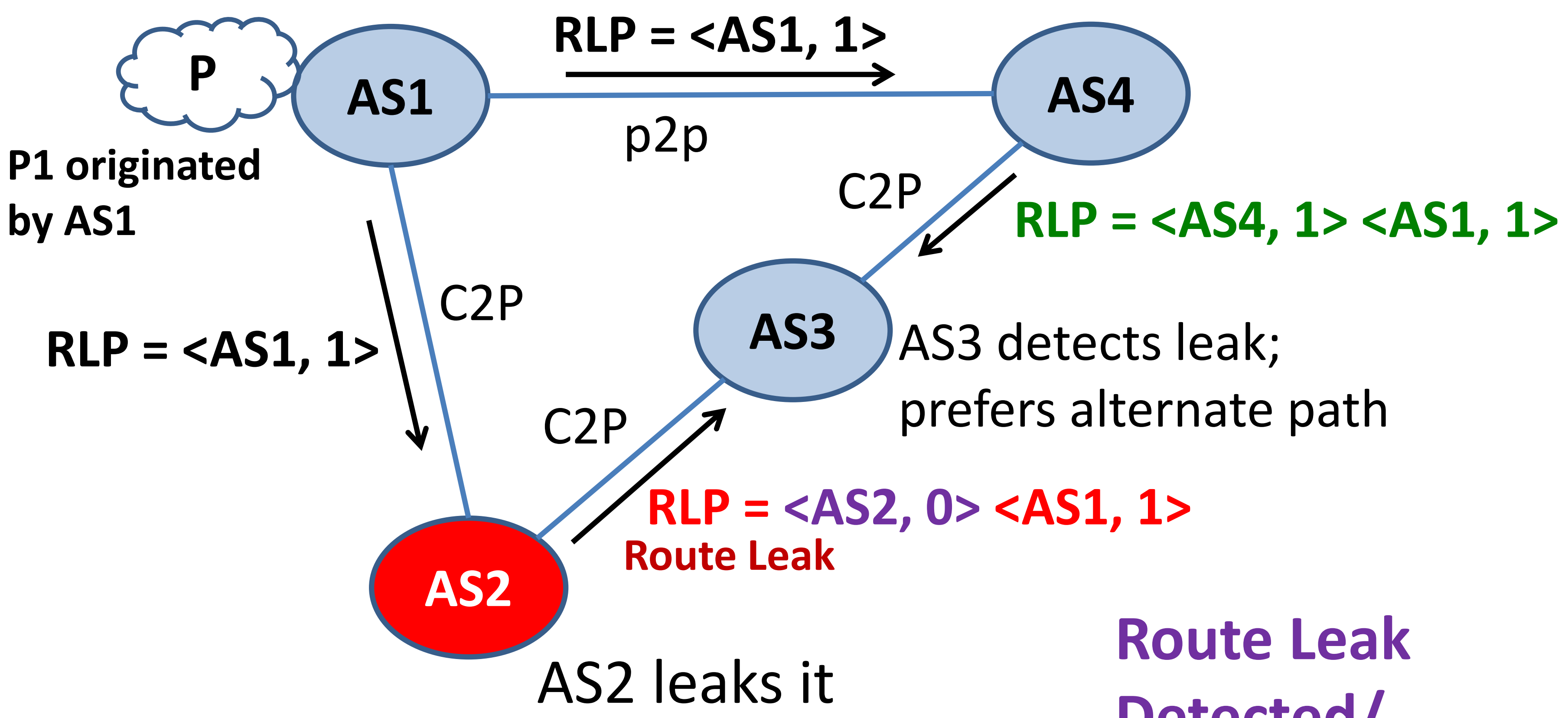


AS does not participate in RLP and/or Propagates a route that violates RLP

Green – not violation
Red – violation
Purple – can't tell

Design A – RLP Attribute

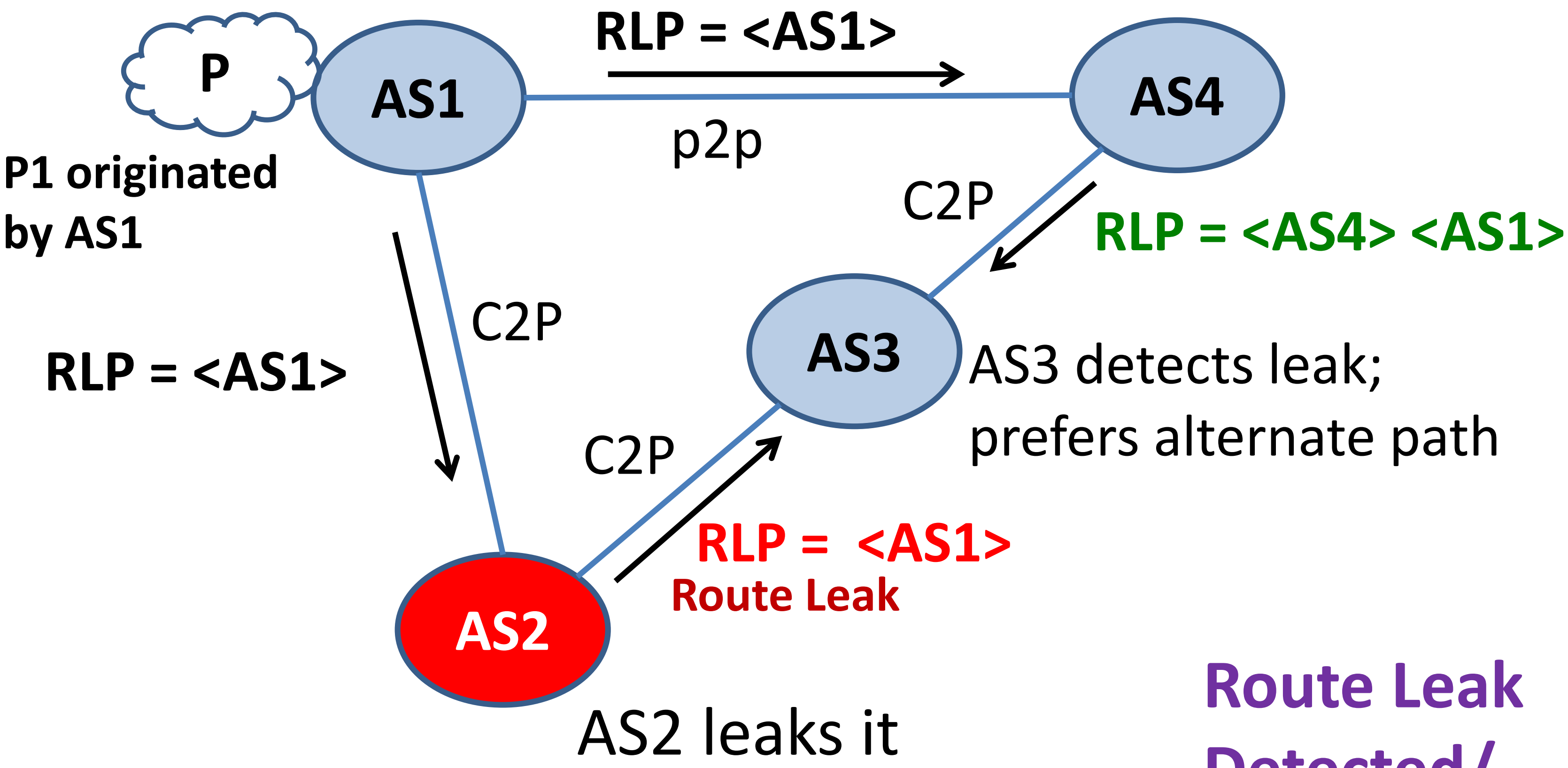
- Insert <ASN, 1> if sending to Customer or Peer
- else, insert <ASN, 0>



Route Leak Detected/ Mitigated ☺

Design B – RLP Attribute

- Insert <ASN> if sending to Customer or Peer
- else, insert nothing



Route Leak Detected/ Mitigated ☺