# Detection and Mitigation of BGP Route Leaks

## ietf-idr-route-leak-detection-mitigation-08

(Route leak definition: RFC 7908)

**K. Sriram, D. Montgomery, B. Dickson, K. Patel, and A. Robachevsky**

**IDR Working Group Meeting, IETF-101**
**March 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.)

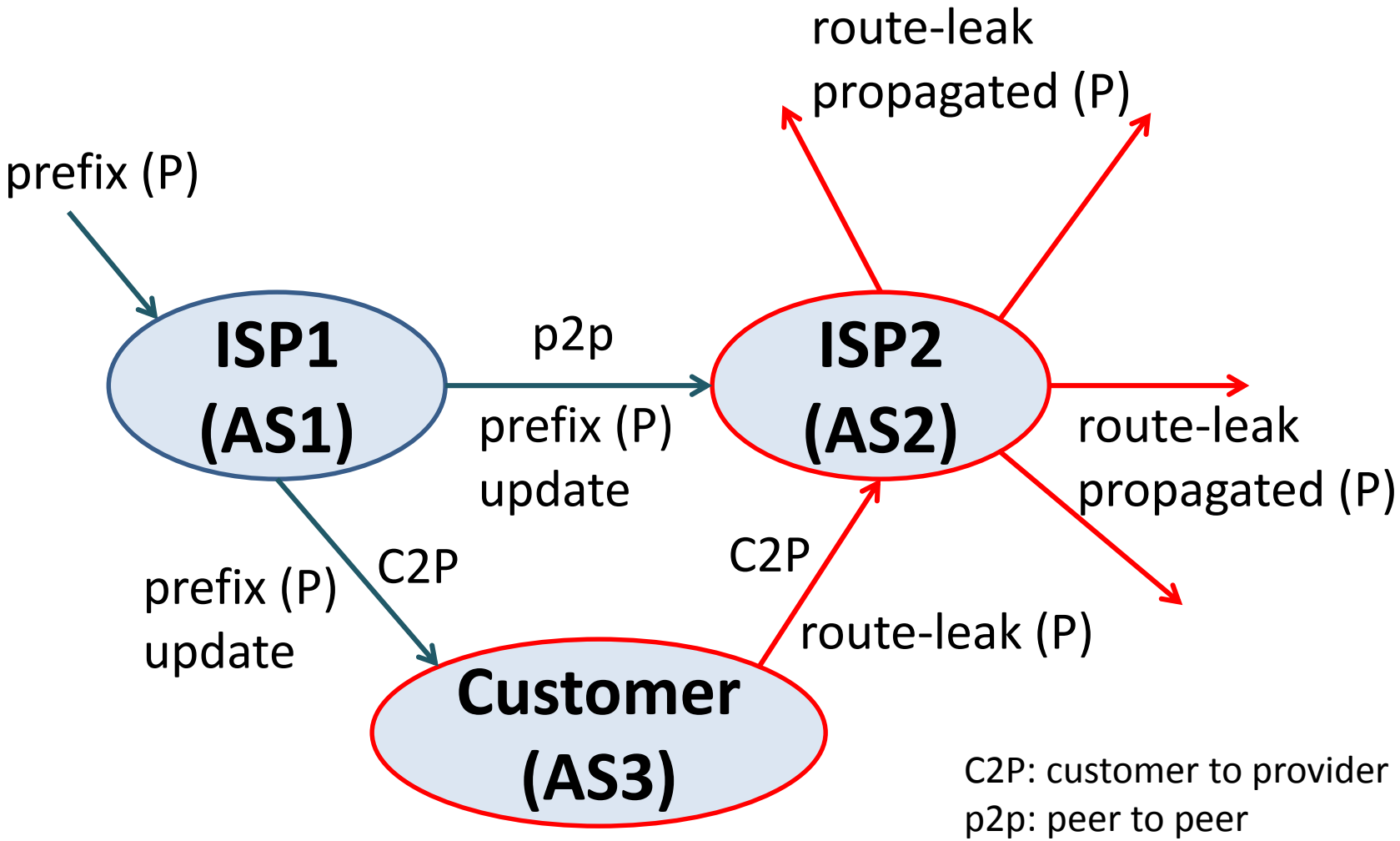
# Changes in -08 compared to the -07 version

- The draft now focuses on the RLP solution which is inter-AS (multi-hop)
  - Note: The intra-AS (local AS) solution with iOTC Attribute is provided in ietf-idr-bgp-open-policy draft
- The main body is now concise since several sections have moved into the Appendices

# Changes in -08 compared to the -07 version

- The Appendices now contain:
  - Related prior-work review
  - Design rationale and discussion
    - Questions raised in IDR/GROW and the discussions captured here
  - Stopgap solution
  - Intra-AS route leak prevention with Community (includes inputs from NANOG list)

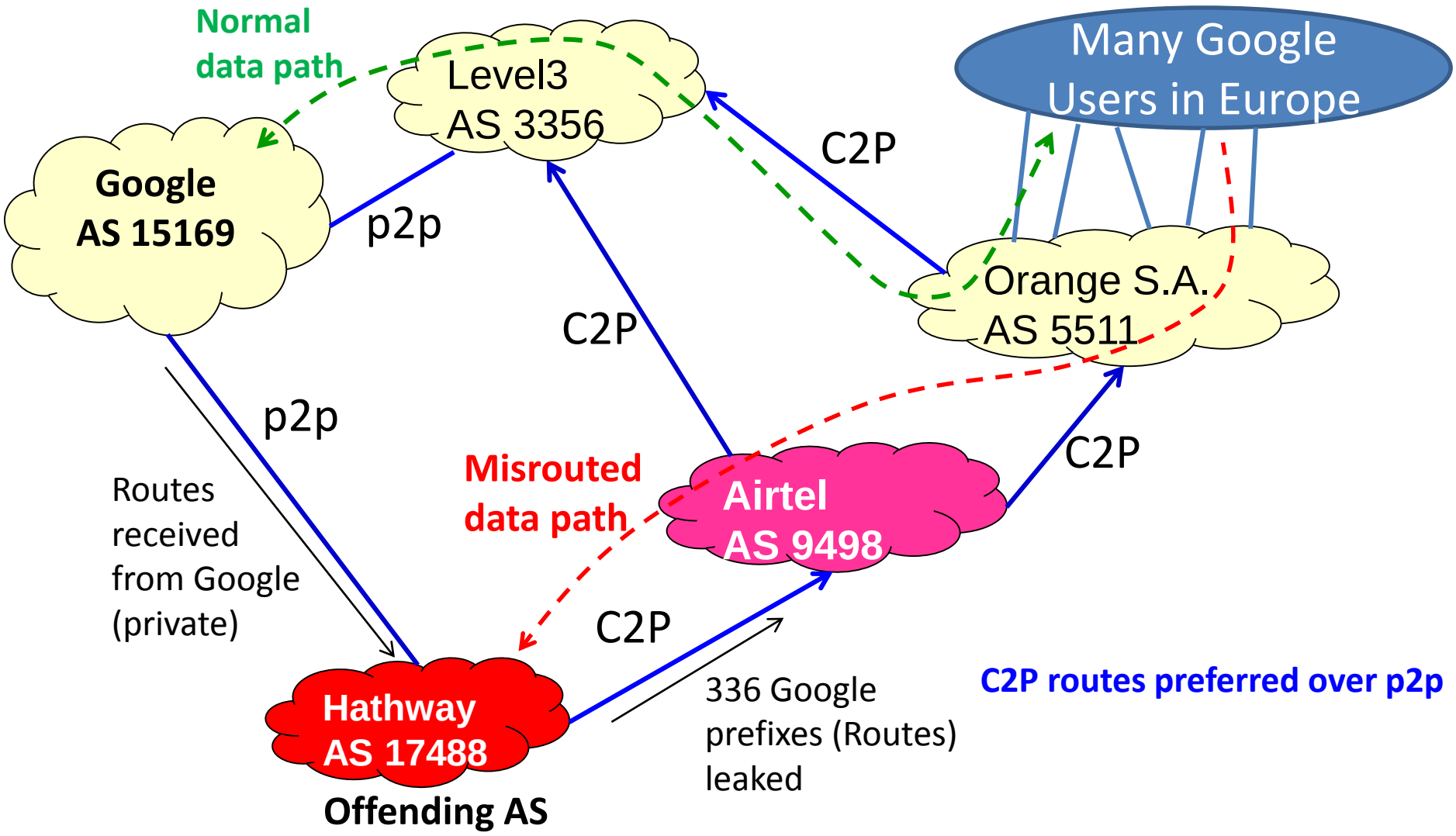
# Route Leak: The Tale of Two Culprits




- Intra-AS and Inter-AS solutions are necessary.

# Hathway / Airtel Route Leaks of Google Prefixes

**March 12, 2015**

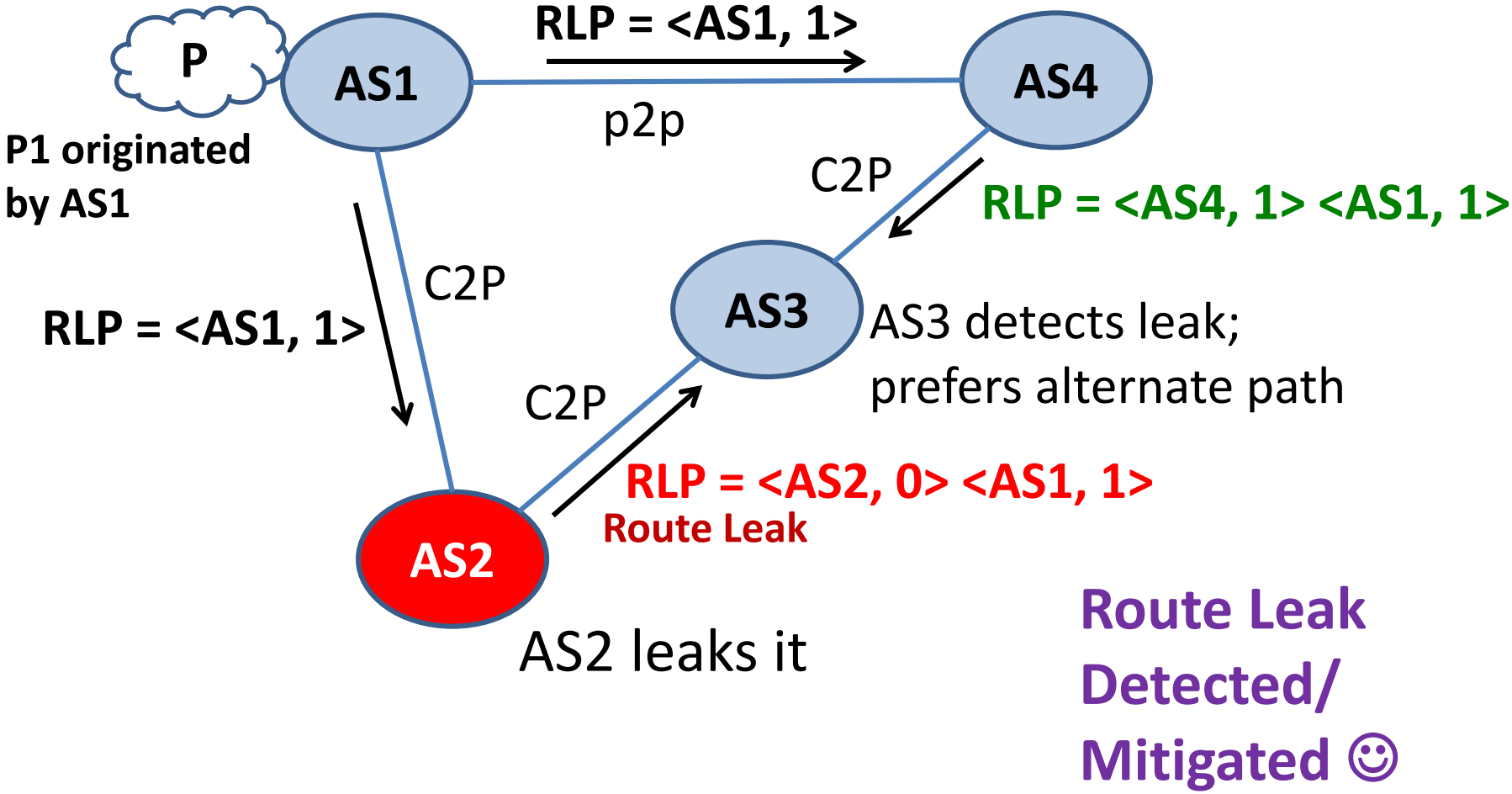



Incident analysis: http://research.dyn.com/2015/03/routing-leak-briefly-takes-google/

# Route Leak Protection (RLP) Field Encoding by Sending Router

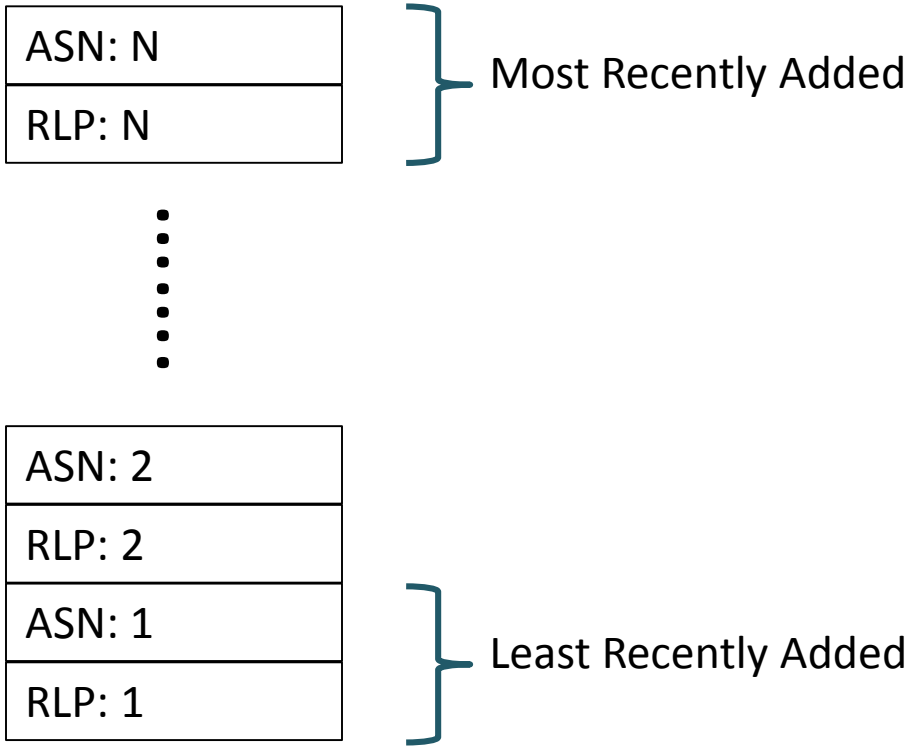
- RLP is a 2-bit field set by each AS along the path
- Can be carried as a transitive per hop attribute in BGP or in the existing Flags field in BGPsec
- The RLP field value MUST be set to one of two values as follows:
  - **00: Default value** (i.e. "nothing specified")
  - **01: 'Do not Propagate Up or Lateral'** indication
    - Sender indicates that the route SHOULD NOT be subsequently forwarded Up towards a transit-provider or to a lateral (non-transit) peer

# Inter-AS Solution – RLP Attribute

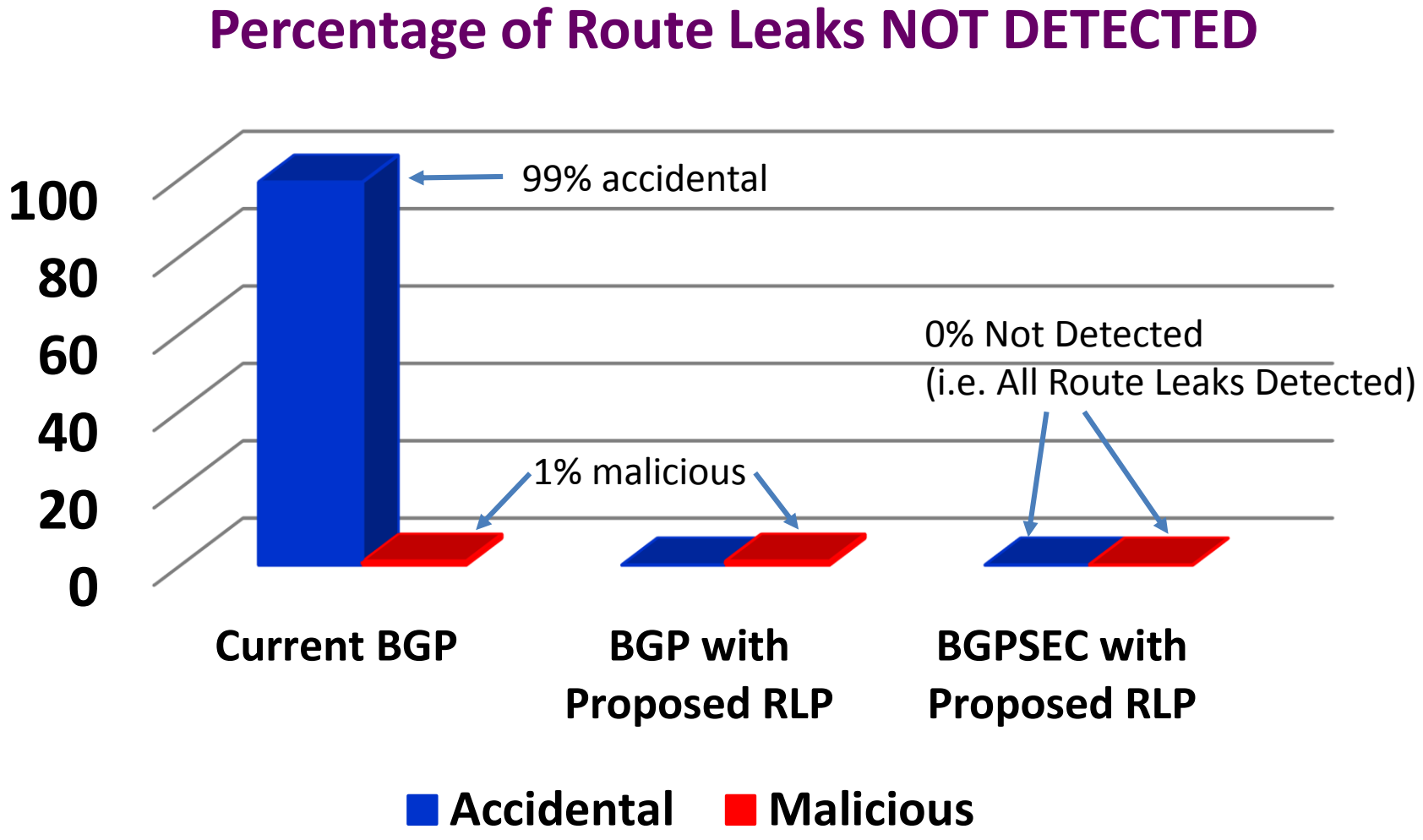


# Format of RLP Attribute

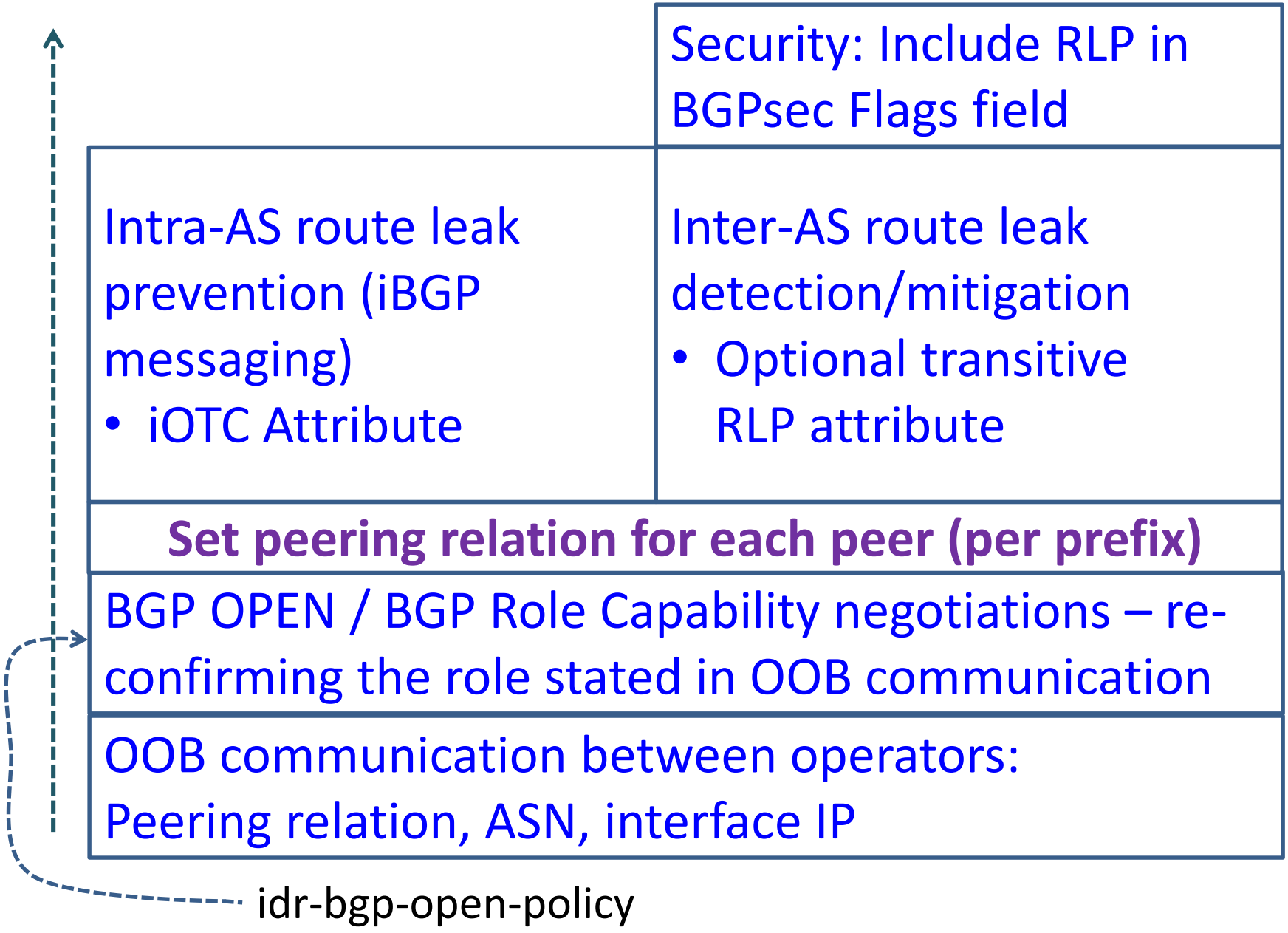
## Optional Transitive Attribute



# Effectiveness of the Proposed Solution



# Building Blocks



# No Single Point of Failure & Large ISPs' Ring of Security