National Institute of Standards and Technology

INFORMATION TECHNOLOGY LABORATORY

Enhanced Feasible-Path Unicast Reverse Path Filtering

draft-sriram-opsec-urpf-improvements-01

K. Sriram and D. Montgomery

OPSEC Working Group Meeting, IETF-99
July 2017

Acknowledgements: The authors are grateful to many folks who offered feedback on the GROW WG mailing list.

Difficulties with Adoption of uRPF Solutions

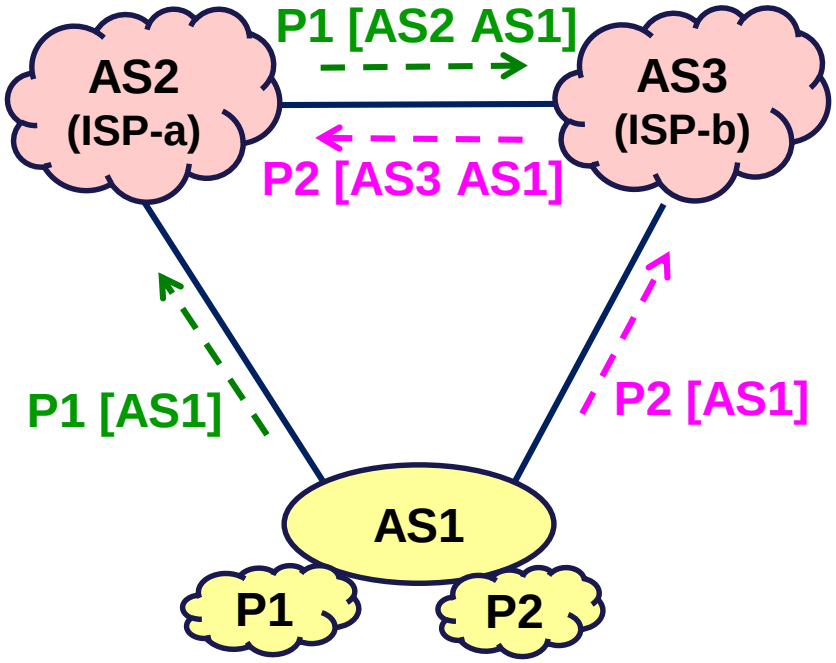
- Strict uRPF is usable in very limited scenarios
- Loose uRPF is not very effective for denying traffic with IPv4 address spoofing (except bogons, etc.)
- Feasible path uRPF is a refinement but ISPs apprehensive that they might deny traffic with legitimate customer source IP addresses
  - When faced with multi-homing and asymmetric routing
- Is there a way to make feasible-path more generalized and accurate?
- Goal: Encourage wider deployment of uRPF

Key Principles of Enhanced Feasible Path uRPF

The Algorithm

1. ISP eBGP router creates a union of all announced prefixes that have a common origin AS
2. Those announcements have potentially been received on different customer/ peer/ provider interfaces
3. Take that union of prefixes and include it in Reverse Path Filter (RPF) tables on all interfaces on which one or more of the prefixes in the union were announced
4. ISP might choose to apply Step #3 across customer interfaces only

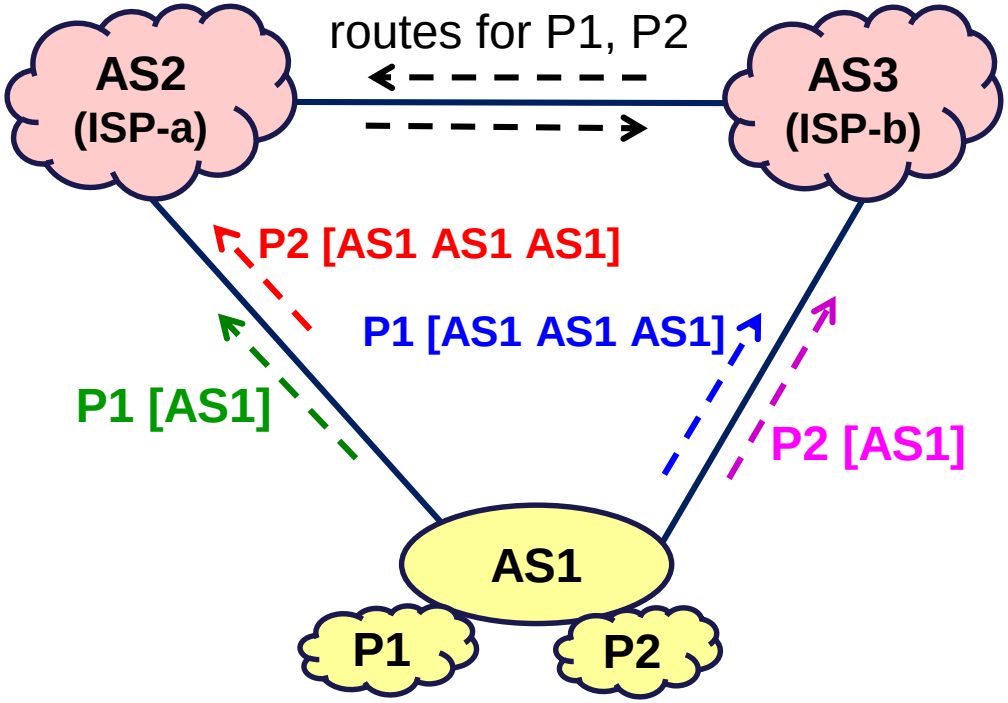
Scenario 1



Consider data packets received at AS2 with source address in P1 or P2:

- X Strict uRPF fails
- X Feasible-path uRPF fails (since routes for P1, P2 are selectively announced to different upstream ISPs)
- ✔ Loose uRPF works (but not desirable)
- ✔ Enhanced Feasible-path uRPF works best

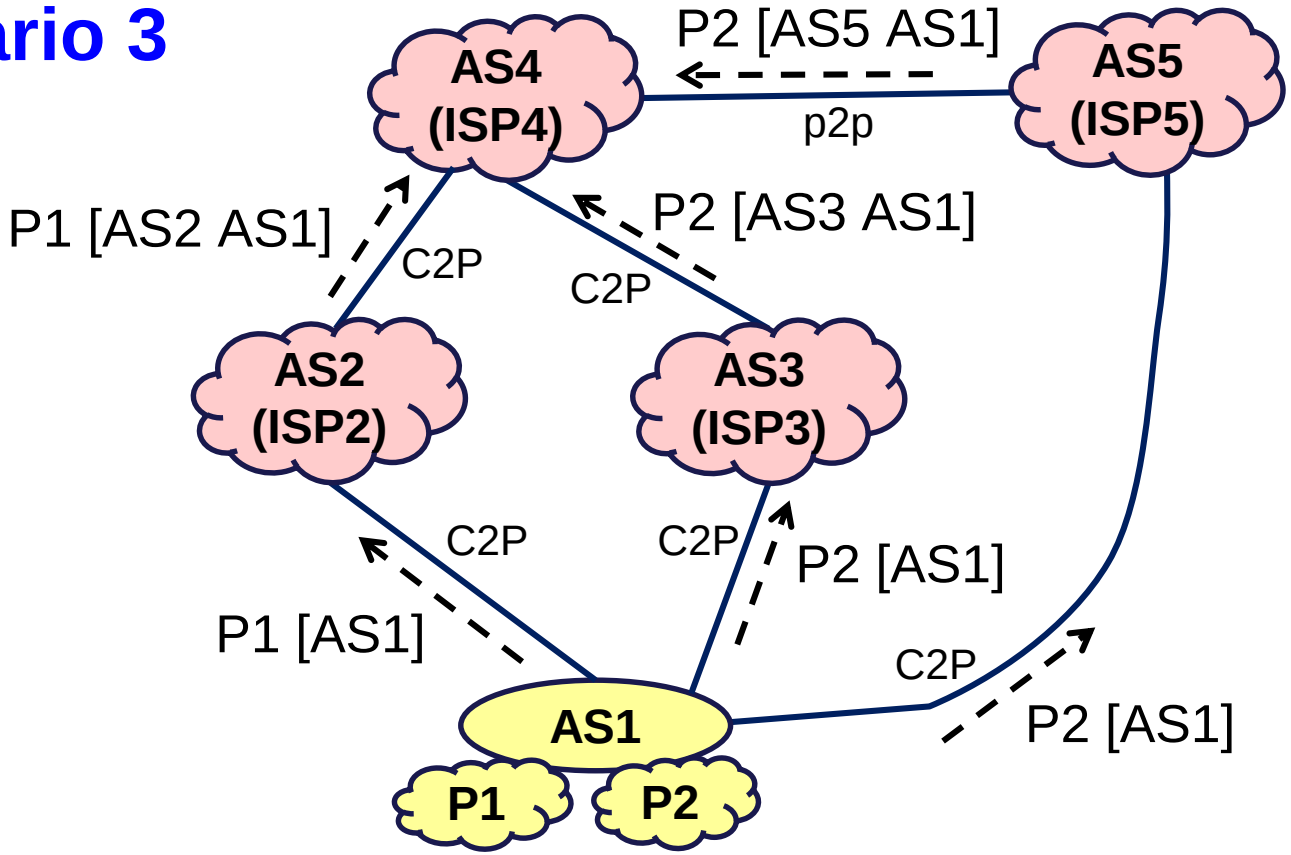
Scenario 2



Consider data packets received at AS2 with source address in P1 or P2:

- ✔ Feasible-path uRPF works (if customer route preferred at AS3 over shorter path)
- X Feasible-path uRPF fails (if shorter path preferred at AS3 over customer route)
- ✔ Loose uRPF works (but not desirable)
- ✔ Enhanced Feasible-path uRPF works best

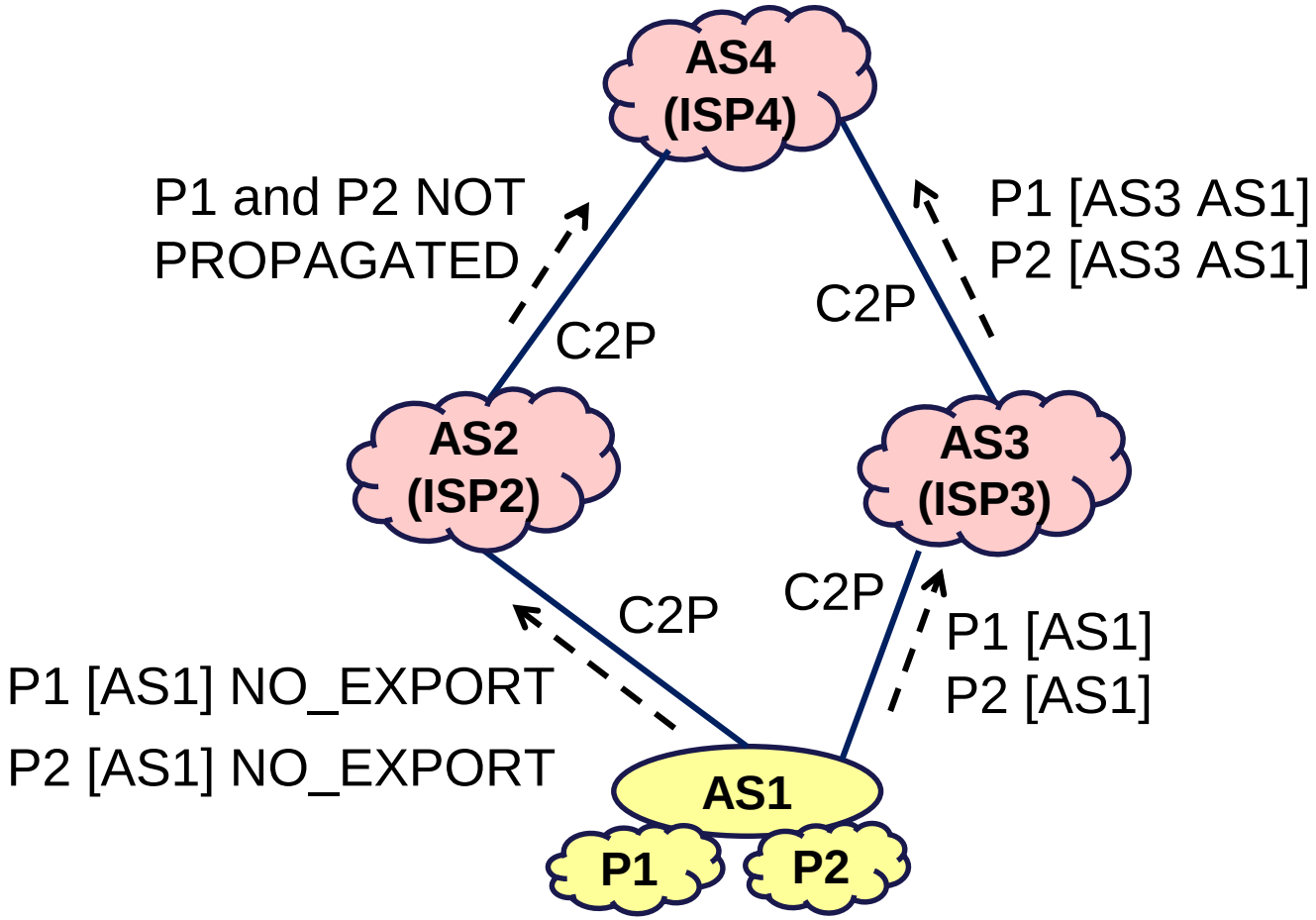
Scenario 3



Consider that data packets (sourced from AS1) may be received at AS4 with source address in P1 or P2 from any of the neighbors (AS2, AS3, AS5):

- **X** Feasible-Path uRPF fails (since routes for P1, P2 are selectively announced to different upstream ISPs)
- ✔ Loose uRPF works (but not desirable)
- ✔ Enhanced Feasible-Path uRPF works best

Example of a Challenging Scenario (from GROW discussion)



- Contradictory to the basic premise of feasible path uRPF (see BCP-84)

Operational Recommendations (BCP-84)

- The mechanism relies on consistent route advertisements (i.e., the same prefix(es), through all the paths) propagating to all the routers performing Feasible RPF checking.

More Relaxed Operational Recommendations (this draft)

For multi-homed stub AS:

- MUST announce at least one origination prefix (exportable) to each transit provider AS

For non-stub AS:

- The above recommendation applies
- Additionally, for the transit routes selected as best path, MUST announce at least one route for each unique {prefix, origin AS} pair to each transit provider

Implementation Considerations

- Existing RPF checks in edge routers take advantage of existing line card implementations to perform the RPF functions.

- For implementation of the proposed technique, the general necessary feature would be to extend the line cards to take arbitrary RPF lists that are not necessarily tied to the existing FIB contents.

- For example, in the proposed method, the RPF lists are constructed by applying a set of rules to all received BGP routes (not just those selected as best path and installed in FIB).

Thanks to Jeff Haas for offering suggestions about implementation.

Summary

- The proposal adds better logic to feasible path uRPF
- ISP might limit this kind of broader criterion for the feasible paths to customer interfaces only
- Implementation details are similar to those for the current feasible path method
- Proposed enhanced uRPF method should help alleviate ISP’s concern about customer service disruption