NIST National Institute of Standards and Technology

iTL INFORMATION TECHNOLOGY LABORATORY

Enhanced Feasible-Path Unicast Reverse Path Filtering

draft-sriram-opsec-urpf-improvements-00

K. Sriram and D. Montgomery

GROW Working Group Meeting, IETF-97
November 2016

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

Difficulties with Adoption of uRPF Solutions

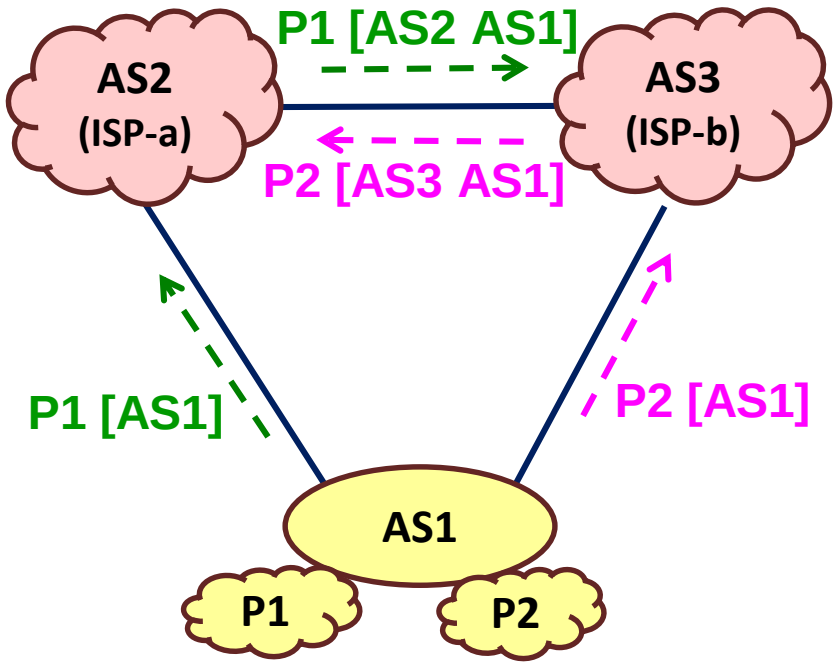
- Strict uRPF is usable in very limited scenarios
- Loose uRPF is not very effective for denying traffic with IPv4 address spoofing (except bogons, Martian)
- Feasible path uRPF is a refinement but ISPs apprehensive that they might deny traffic with legitimate customer source IP addresses
  - When faced 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

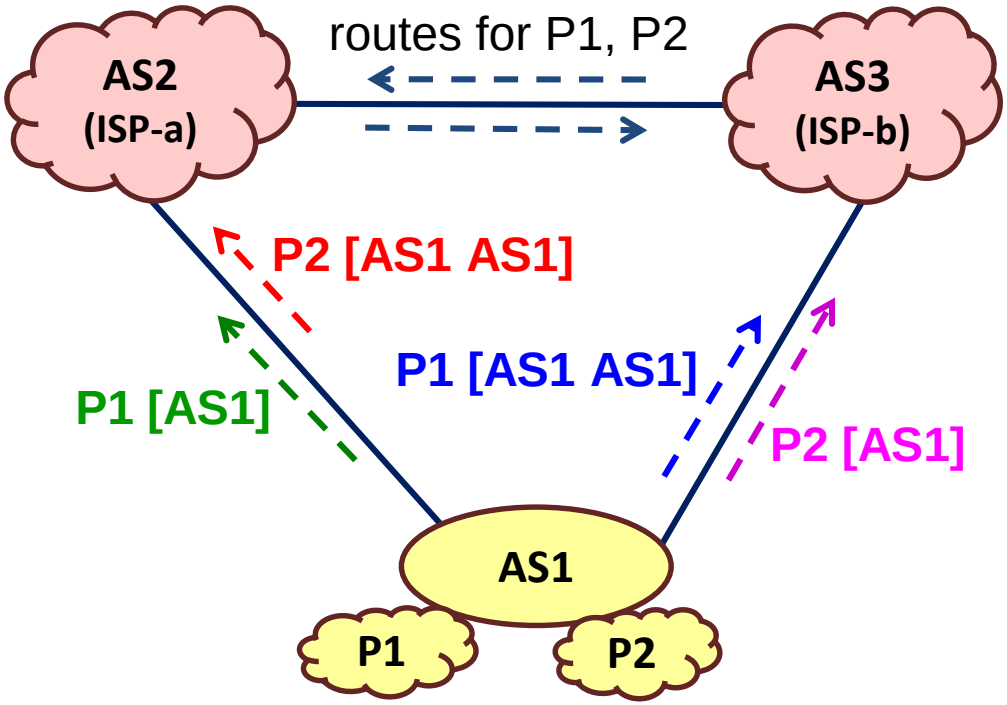
Scenario 1



Consider data packet received at AS2 via AS1 or AS3 that originated from AS1 with source address in P1:

- 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

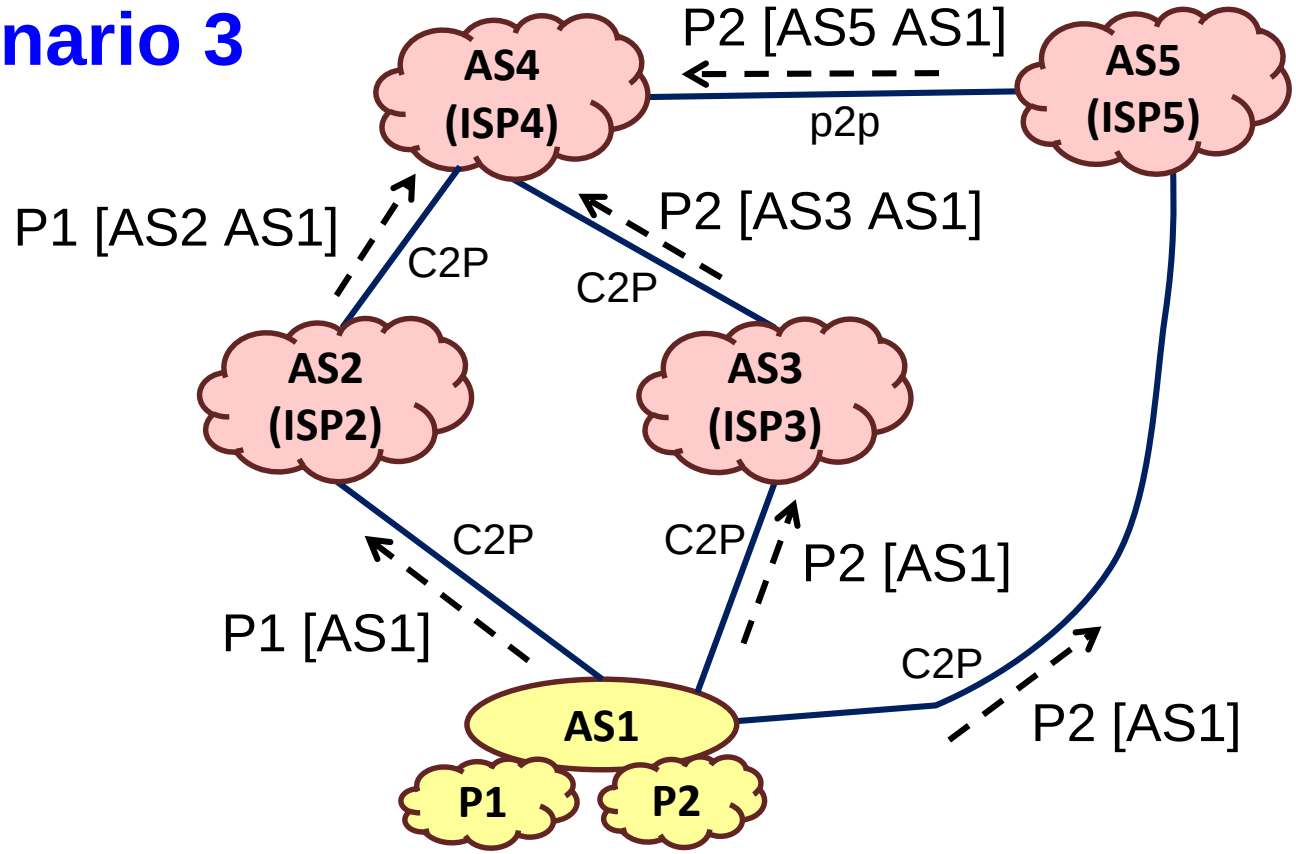
Scenario 2



Consider data packet received at AS2 via AS3 that originated from AS1 with source address in P1:

- ✔ 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 (source 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

Summary

- The proposal adds better logic to feasible path uRPF
- Might limit this kind of broader criterion for the feasible paths to customer interfaces only
- Implementation details are similar as for the current feasible path method
- This enhanced method certainly should help alleviate ISP’s customer service disruption concern
- Wherever feasible path method is used currently, the enhanced method would work more robustly