IPv6 RA IPv6-Only Flag
<draft-ietf-6man-ipv6only-flag-04>

Bob Hinden
Brian Carpenter

IETF103 Bangkok
Working Group Last Call

● Started on 6 September 2018
  ● Many emails
  ● Requests for implementations
● Thanks to Lee Howard for detailed review and everyone else's comments.
● Three new versions of draft published since IETF 102 intended to resolve issues raised in discussion and last call
Changes Since IETF102

- draft-ietf-6man-ipv6only-flag-02 (2018-August-14)
  - Added text to Section 9 to clarify that hosts not supporting this flag are not protected from IPv4-based attacks.
  - Editorial changes.

- draft-ietf-6man-ipv6only-flag-03 (2018-October-16)
  - Reorganized text about problem statement and applicability
  - Added note about shortage of flag bits
  - Clarified text about logging configuration error in Section 6
  - Editorial changes
Changes Since IETF102 (cont)

- draft-ietf-6man-ipv6only-flag-04 (5 Nov 2018)
  - Added text to Section 1 explaining why the mechanism is based on Router Advertisements.
  - Added text to Section 3 that for a VLAN, the IPv6-Only flag only applies to the specific VLAN on which it was received.
  - Changed Section 3 that administrators MUST only use this mechanism if they are certain that the link is IPv6-Only, instead of SHOULD.
  - Added ARP to Section 4 for protocols that the IPv6-Only flag applies to.
  - Renamed the IPv6-Only flag label from "6" to "S".
  - Added pointers to Section 7.2.7 of RFC4861 in Section 6.
  - Added that RFC4861 is also updated by Section 6 for routers implementing this flag.
  - Changed Section 7 from SHOULD NOT to MUST NOT.
  - Added Appendix A on implementations and testing.
  - Many small clarifications based on IPv6 list discussion and editorial changes.
Implementation and Testing

- FreeBSD Implementation by Bjoern Zeeb
  - ~100 lines of code
  - Tested with two FreeBSD IPv6 routers, a FreeBSD laptop on Ethernet and WiFi, and with Win10 and OSX clients

- Test using Scapy
  - Verified that setting this flag did not cause any adverse effects on Windows 10 and Android.
Issues Raised (1 of 2)

- Not needed because layer 2 filters sufficient
  - L2 filters may not existing on all links.
  - This is to inform hosts not to even try sending IPv4, so there is an incremental benefit

- Not needed because hosts can discover the lack of IPv4 services anyway
  - Hard to make discovery reliable, discovery process might cause other hosts to think there was IPv4 when it was just discovery traffic.
  - This is signal from Administrator that the link is IPv6-Only

- Could be done by DHCPv4 mechanism
  - Not if routers are IPv6 only; or if layer 2 blocks IPv4, or if no IPv4 services on link.
Issues Raised (2 of 2)

- Could be done by management protocol or DHCPv6
  - Management protocols not universal (BYOD devices, unmanged links, etc.)
  - RA is the only universal mechanism
- Host behavior suggested, not mandatory
  - Requirement is SHOULD, do this unless you have a good reason to not do it.
  - Administrator is saying the link in IPv6-Only
- Might cause interop issues among IPv4 hosts
  - Not an issue, the network admin has decided not to support IPv4!
Next Steps

- Authors think it is ready to advance

- Implementation experience shows it is feasible and doesn’t disrupt legacy IPv6 implementations

- Next steps?
QUESTIONS / COMMENTS?