Network Working Group
Internet-Draft
Updates: 5175 (if approved)
Intended status: Standards Track
Expires: February 15, 2019

R. Hinden
Check Point Software
B. Carpenter
Univ. of Auckland

August 14, 2018

IPv6 Router Advertisement IPv6-Only Flag
draft-ietf-6man-ipv6only-flag-02

Abstract

This document specifies a Router Advertisement Flag to indicate to hosts that the administrator has configured the router to advertise that the link is IPv6-Only. This document updates RFC5175.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on February 15, 2019.

Table of Contents

1. Introduction

This document specifies a Router Advertisement Flag to indicate to hosts that the administrator has configured the router to advertise that the link is IPv6-Only. The flag does not apply to non-default IPv6 routers.

Hosts that support IPv4 and IPv6, usually called dual stack hosts, need to also work efficiently on IPv6 only links. That is, a link where there are no IPv4 routers and/or IPv4 services. Dual stack is the default configuration for most current host operating systems such as Windows 10, IOS, Android, Linux, and BSD, as well as devices such as printers. Monitoring of IPv6-only link, for example at the IETF 100 meeting in Singapore, shows that current dual stack hosts will create local auto-configured IPv4 addresses and attempt to reach IPv4 services. This may be a problem for several reasons:

- It may result in an undesirable level of Layer 2 broadcast traffic, especially on large wireless networks.

- In particular, this may overload switches in multi-segment wireless networks because it will create IPv4 state for every dual stack host.

- Such traffic may drain battery power on wireless hosts that have no interest in link-local IPv4 traffic. [RFC7772] indicates how this risk might be quantified.

- Similarly, hosts may waste battery power on futile attempts to access IPv4 services.

- On an IPv6-only link, IPv4 might be used for malicious purposes and pass unnoticed by IPv6-only monitoring mechanisms.

This document defines a mechanism that a router administrator can use to inform hosts that this is an IPv6-Only link on their default routers such that they can disable IPv4 on this link, mitigating all of the above problems.

In managed networks whose equipment allows it, these problems could be mitigated by configuring the Layer 2 infrastructure to drop IPv4 and ARP traffic by filtering Ethertypes 0x0800 and 0x806 [IANA-Ethertype]. IPv6 uses a different Ethertype 0x86DD so this filtering will not interfere with IPv6 traffic. Depending on the equipment details, this would limit the traffic to the link to the switch, and would drop all IPv4 and ARP broadcast packets. However, hosts transmitting IPv4 packets would still do so, consuming their own battery power and some radio bandwidth. The intent of this specification is to provide a mechanism that works on networks without the ability to filter L2 traffic, or where there are portions of a network without the ability to filter L2 traffic. It may also be valuable on unmanaged networks using routers pre-configured for IPv6-only operations and where Layer 2 filtering is unavailable.

Because there is no IPv4 support on IPv6-only routers, the only way to notify the dual stack hosts that this link is IPv6-Only is to use an IPv6 mechanism. An active notification will be much more precise than attempting to deduce this fact by the lack of IPv4 responses or traffic.

IPv4-only hosts, and dual-stack hosts that do not recognize the new flag, will continue to attempt IPv4 operations, in particular IPv4 discovery protocols typically sent as link-layer broadcasts. This legacy traffic cannot be prevented by any IPv6 mechanism. The value of the new flag is limited to hosts that recognize it.

This document specifies a new flag for Router Advertisement Flag [RFC5175]. It updates [RFC5175] to add this flag.

2. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Applicability Statements

The mechanism is designed to allow administrators to notify hosts that the link is IPv6-Only. It SHOULD be only used in IPv6-Only links.

Dual stack hosts that have a good reason to use IPv4, for example for a specific IPv4 link-local service, can continue to do so. This is consistent with the SHOULD language in this document.

Administrators SHOULD only use this mechanism if they are certain that the link is IPv6-Only. For example, in cases where there is a need to continue to use IPv4 or there are IPv4 only routers, setting this flag to 1 is a configuration error.

4. IPv6-Only Definition

IPv6-Only is defined to mean that no other versions of internet protocol than IPv6 are running directly on the link. Today this effectively simply means that IPv4 is not running on the link, and it includes:

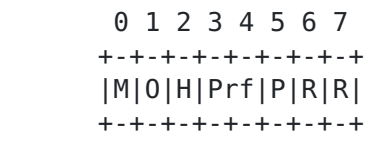
* No IPv4 traffic on the Link
* No IPv4 routers on the Link
* No DHCPv4 servers on the Link
* No IPv4 accessible services on the Link
* All IPv4 and ARP traffic may be blocked at Layer 2 by the administrator

It is expected that on IPv6-Only networks it will be common for access to IPv4 external services to be reached by techniques such as NAT64 [RFC6146] and DNS64 [RFC6147] at the edge of the network. This is beyond the scope of this document.

Note that IPv6-Only provides no information about other network protocols than IP running directly over the link layer. It is out of scope of this specification whether any such protocol is running on the link or whether any protocol is tunneled over IPv6.

5. IPv6-Only Flag

RFC5175 currently defines the flags in the NDP Router Advertisement message and these flags are registered in the IANA IPv6 ND Router Advertisement flags Registry [IANA-RF]. This currently contains the following one-bit flags defined in published RFCs:



M Managed Address Configuration Flag [RFC4861]
O Other Configuration Flag [RFC4861]
H Mobile IPv6 Home Agent Flag [RFC3775]
Prf Router Selection Preferences [RFC4191]
P Neighbor Discovery Proxy Flag [RFC4389]
R Reserved

This document defines bit 6 to be the IPv6-Only Flag:

6 IPv6-Only Flag

This flag has two values. These are:

0 This is not an IPv6-Only link
1 This is an IPv6-Only link

RFC 5175 requires that unused flag bits be set to zero. Therefore, a router that does not support the new flag will not appear to assert that this is an IPv6-Only link.

Hosts receiving the Router Advertisement SHOULD only process this flag if the advertising router is a Default Router. Specifically, if the Lifetime field in the Router Advertisement is not zero, otherwise it SHOUD be ignored. This is done to allow some IPv6 routers to advertise information without being a Default Router and providing IPv6 connectivity.

6. Router and Operational Considerations

Default IPv6 routers that are on an IPv6-Only link SHOULD be configured to set the IPv6-Only flag to 1 on interfaces on this link. In all other cases the flag SHOULD NOT be set to 1.

The intent is that the administrator of the router configures the router to set the IPv6-Only flag if she/he wants to tell the hosts on the link that the link is IPv6-Only. This is a configuration flag, it is not something that the router decides on it's own. Routers MAY

log a configuration error if the flag is set and IPv4 is still active on the router.

Operators of large IPv6-only wireless links are advised to also use Layer 2 techniques to drop IPv4 and ARP packets (Ethertypes 0x0800 and 0x806) at all switches, and to ensure that IPv4 and ARP features are disabled in all switches.

7. Host Behavior Considerations

If there are multiple IPv6 default routers on a link, they might send different values of the flag. If at least one IPv6 default router sends the flag with value 0, a dual stack host SHOULD NOT assume that the link is IPv6-Only. If all IPv6 default routers send the flag with value 1, a dual stack host SHOULD assume that this is an IPv6-Only link.

A host that receives only RAs with the flag set to 1 SHOULD NOT attempt any IPv4 operations, unless it subsequently receives at least one RA with the flag set to zero. As soon as such an RA is received, IPv4 operations SHOULD be started.

A host MAY choose to delay all IPv4 operations at start-up until a reasonable time has elapsed for RA messages to arrive. If all RAs received have the flag set, a host SHOULD also choose to not attempt IPv4 operations until an application asks it to, specifically delay performing DHCPV4 until it gets a request from an application to use IPv4. This would avoid attempting to obtain IPv4 addresses if there are no applications trying to use IPv4.

In all of the above, the flag's value is considered valid for the lifetime of the default router concerned, unless a subsequent RA delivers a different flag value. If a default router expires (i.e., no RA is received that refreshes its lifetime), the host must remove this router's flag value from consideration. If the result is that all surviving default routers have the flag set to 1, the host SHOULD assume that the link is IPv6-Only. In other words, at any given time, the state of the flag as seen by the host is the logical AND of the flags sent by all unexpired default IPv6 routers.

This also means that if all default routers have set the flag, the flag for the host is thereby set. If the lifetimes of all the routers subsequently expire, then the state of the flag for the host becomes cleared.

8. IANA Considerations

IANA is requested to assign the new Router Advertisement flag defined in Section 5 of this document. Bit 6 is the next available bit in this registry, IANA is requested to use this bit unless there is a reason to use another bit in this registry.

IANA is also requested to register this new flag bit in the IANA IPv6 ND Router Advertisement flags Registry [IANA-RF].

9. Security Considerations

This document shares the security issues with other parts of IPv6 Neighbor Discovery. General techniques to protect Router Advertisement traffic such as Router Guard [RFC6105] are useful in protecting these vulnerabilities.

A bad actor could use this mechanism to attempt turn off IPv4 service on a link that is using IPv4, by sending Router Advertisements with the IPv6-Only Flag set to 1. In that case, as long as there are routers sending Router Advertisements with this Flag set to 0, they would override this attack given the mechanism in Section 5. Specifically a host would only turn off IPv4 service if it wasn't hearing any Router Advertisement with the Flag set to 0. If the advice in Section 6 is followed, this attack will fail.

Conversely, a bad actor could use this mechanism to turn on, or pretend to turn on, IPv4 service on an IPv6-only link, by sending Router Advertisements with the Flag set to 0. However, this is really no different than what such a bad actor can do anyway, if they have the ability to configure a bogus router in the first place. The advice in Section 6 will minimize such an attack by limiting it to a single link.

Note that manipulating the Router Preference [RFC4191] will not affect either of these attacks: any IPv6-Only Flag of 0 will always override all Flags set to 1.

The new flag is neutral from an IPv6 privacy viewpoint, since it does not affect IPv6 operations in any way. From an IPv4 privacy viewpoint, it has the potential benefit of suppressing unnecessary traffic that might reveal the existence of a host and the correlation between its hardware and IPv4 addresses. It should be noted that hosts that don't support this flag are not protected from IPv4-based attacks.

10. Acknowledgments

A closely related proposal was published earlier as [I-D.ietf-sunset4-noipv4].

Helpful comments were received from Lorenzo Colitti, David Farmer, Fernando Gont, Nick Hilliard, Erik Kline, Jen Linkova, Veronika McKillop, Michael Richardson, Mark Smith, Barbara Stark, Tatuya Jinmei, Ole Troan, James Woodyatt, and other members of the 6MAN working group.

Bjoern Zeeb has also produced a variant of this proposal and proposed an IPv6 transition plan in [I-D.bz-v4goawayflag].

11. Change log [RFC Editor: Please remove]

draft-ietf-6man-ipv6only-flag-02, 2018-August-14:

* Added text about logging configuration errors to Section 6
* 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-01, 2018-June-29:

* Added text to section that defines what IPv6-Only includes to clarify that only other version of the Internet protocol are in scope.
* Added clarification if the lifetime of all routers expire.
* Editorial changes.

draft-ietf-6man-ipv6only-flag-00, 2018-May-21:

* Changed the file name to draft-ietf-6man-ipv6only-flag to match the current tile and that it is a w.g. draft.
* Added new section that defines what IPv6-Only includes.
* Expanded description of using Layer 2 filter to block IPv4 and ARP traffic.
* Editorial changes.

draft-hinden-ipv4flag-04, 2018-April-16:

* Changed the name of the document and flag to be the IPv6-Only flag.

* Rewrote text to make it affirmative that this is used by an administrator to tell the hosts that the link is IPv6-Only.
* Added an Applicability Statements section to scope the intend use.
* Changed requirement language to upper case, added Requirements Language section with references to [RFC2119] and [RFC8174].
* Editorial changes.

draft-hinden-ipv4flag-03, 2018-Feb-15:

* Changed terminology to use "link" instead of "network".
* Improved text in Section 4. "Host Behavior Considerations" and added suggestion to only perform IPv4 if an application requests it.
* Added clarification that the bit is set because an administrator configured the router to send it.
* Editorial changes.

draft-hinden-ipv4flag-02, 2018-Feb-15:

* Improved text in introduction.
* Added reference to current IANA registry in Section 2.
* Editorial changes.

draft-hinden-ipv4flag-01, 2017-Dec-12

* Inverted name of flag from "Available" to "Unavailable".
* Added problem description and clarified scope.
* Added router and operational considerations.
* Added host behavior considerations.
* Extended security considerations.
* Added Acknowledgment section, including reference to prior sunset4 draft.

draft-hinden-ipv4flag-00, 2017-Nov-17:

* Original version.

12. References

12.1. Normative References

[IANA-Ethertype]
"Ether Types", <https://www.iana.org/assignments/ieee-802-numbers/ieee-802-numbers.xhtml#ieee-802-numbers-1>.

[IANA-RF] "IPv6 ND Router Advertisement flags", <https://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xhtml#icmpv6-parameters-11>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC4191] Draves, R. and D. Thaler, "Default Router Preferences and More-Specific Routes", RFC 4191, DOI 10.17487/RFC4191, November 2005, <https://www.rfc-editor.org/info/rfc4191>.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, DOI 10.17487/RFC4861, September 2007, <https://www.rfc-editor.org/info/rfc4861>.

[RFC5175] Haberman, B., Ed. and R. Hinden, "IPv6 Router Advertisement Flags Option", RFC 5175, DOI 10.17487/RFC5175, March 2008, <https://www.rfc-editor.org/info/rfc5175>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

12.2. Informative References

[I-D.bz-v4goawayflag]
Zeeb, B., "IPv6 Router Advertisement IPv4 GoAway Flag", draft-bz-v4goawayflag-00 (work in progress), March 2018.

[I-D.ietf-sunset4-noipv4]
Perreault, S., George, W., Tsou, T., Yang, T., and J. Tremblay, "Turning off IPv4 Using DHCPv6 or Router Advertisements", draft-ietf-sunset4-noipv4-01 (work in progress), December 2014.

[RFC6105] Levy-Abegnoli, E., Van de Velde, G., Popoviciu, C., and J. Mohacsi, "IPv6 Router Advertisement Guard", RFC 6105, DOI 10.17487/RFC6105, February 2011, <https://www.rfc-editor.org/info/rfc6105>.

[RFC6146] Bagnulo, M., Matthews, P., and I. van Beijnum, "Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers", RFC 6146, DOI 10.17487/RFC6146, April 2011, <https://www.rfc-editor.org/info/rfc6146>.

[RFC6147] Bagnulo, M., Sullivan, A., Matthews, P., and I. van Beijnum, "DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers", RFC 6147, DOI 10.17487/RFC6147, April 2011, <https://www.rfc-editor.org/info/rfc6147>.

[RFC7772] Yourtchenko, A. and L. Colitti, "Reducing Energy Consumption of Router Advertisements", BCP 202, RFC 7772, DOI 10.17487/RFC7772, February 2016, <https://www.rfc-editor.org/info/rfc7772>.

Authors' Addresses

Robert M. Hinden
Check Point Software
959 Skyway Road
San Carlos, CA 94070
USA

Email: bob.hinden@gmail.com

Brian Carpenter
Department of Computer Science
University of Auckland
PB 92019
Auckland 1142
New Zealand

Email: brian.e.carpenter@gmail.com