

Network Working Group  
Internet-Draft  
Updates: [5175](#) (if approved)  
Intended status: Standards Track  
Expires: September 3, 2018

R. Hinden  
Check Point Software  
B. Carpenter  
Univ. of Auckland  
March 2, 2018

**IPv6 Router Advertisement IPv4 Unavailable Flag  
draft-hinden-ipv4flag-03**

Abstract

This document specifies a Router Advertisement Flag to indicate to hosts that there is no IPv4 service on the advertising default IPv6 router. 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 September 3, 2018.

Copyright Notice

Copyright (c) 2018 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

<a href="#">1.</a>	Introduction . . . . .	<a href="#">2</a>
<a href="#">2.</a>	IPv4 Unavailable Flag . . . . .	<a href="#">3</a>
<a href="#">3.</a>	Router and Operational Considerations . . . . .	<a href="#">4</a>
<a href="#">4.</a>	Host Behavior Considerations . . . . .	<a href="#">5</a>
<a href="#">5.</a>	IANA Considerations . . . . .	<a href="#">6</a>
<a href="#">6.</a>	Security Considerations . . . . .	<a href="#">6</a>
<a href="#">7.</a>	Acknowledgments . . . . .	<a href="#">7</a>
<a href="#">8.</a>	Change log [RFC Editor: Please remove] . . . . .	<a href="#">7</a>
<a href="#">9.</a>	References . . . . .	<a href="#">8</a>
<a href="#">9.1.</a>	Normative References . . . . .	<a href="#">8</a>
<a href="#">9.2.</a>	Informative References . . . . .	<a href="#">8</a>
	Authors' Addresses . . . . .	<a href="#">9</a>

## [1.](#) Introduction

This document specifies a Router Advertisement Flag to indicate to hosts that there is no IPv4 service on the advertising default IPv6 router. 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:

- o It may result in an undesirable level of Layer 2 broadcast traffic, especially on large wireless networks.
- o In particular, this may overload switches in multi-segment wireless networks because it will create IPv4 state for every dual stack host.
- o 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.
- o Similarly, hosts may waste battery power on futile attempts to access IPv4 services.
- o On an IPv6-only link, IPv4 might be used for malicious purposes and pass unnoticed by IPv6-only monitoring mechanisms.



Some of these problems could be mitigated by configuring the Layer 2 infrastructure to drop IPv4 and DHCPv4 traffic by filtering Ethertypes 0x0800 and 0x806. However although this would limit the traffic to a single segment, it would not eliminate it.

This document defines a mechanism that a router administrator can use to inform hosts that there is no IPv4 support on their default routers so that they may choose to turn off IPv4, mitigating all of the above problems. Each TCP/IP host implementation will differ in the way it handles the absence of IPv4 support, so the usefulness of this mechanism will vary. In any case, it is only a hint.

Because there is no IPv4 support on IPv6-only routers, the only way to notify the dual stack hosts on the link 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 dual-stack hosts that recognize it.

Additionally, dual-stack hosts that support any form of link-local service may choose to support such a service over IPv4 regardless of the new mechanism. Similarly, it is possible that a link could be configured with both IPv6-only routers and IPv4-only routers. For that reason, the new mechanism is advisory in nature. Host behaviors are discussed in more detail in [Section 4](#).

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

## 2. IPv4 Unavailable 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-RE](#)]. This currently contains the following one-bit flags defined in published RFCs:

```

0 1 2 3 4 5 6 7
+--+--+--+--+--+
|M|O|H|Prf|P|R|R|
+--+--+--+--+--+
```



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 IPv4 Unavailable Flag:

#### 4    IPv4 Unavailable Flag

This flag has two values. These are:

0    IPv4 is Available on this default Router  
1    IPv4 is Not Available on this default Router

[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 IPv4 is unsupported.

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 should be ignored. This is done to allow some IPv6 routers to advertise information without being a Default Router and providing IPv6 connectivity.

### 3. Router and Operational Considerations

Default IPv6 routers that do not support IPv4 should be configured to set the IPv4 Unavailable flag to 1, unless the operator is aware that IPv4 support is available from another router. Default IPv6 routers that also support IPv4 must be configured to clear the IPv4 Unavailable flag.

The intent is that the administrator of the router configures the router to set the IPv4 Unavailable flag if she/he wants to tell the hosts on the link that IPv4 is unavailable. This is intended to be a configuration flag, not something that the router decides on it's own.

Operators of large IPv6-only wireless links are advised to also use Layer 2 techniques to drop IPv4 and DHCPv4 packets (Ethertypes 0x0800



and 0x806) at all switches, and to ensure that IPv4 and DHCPv4 Layer 3 features are disabled in all switches.

#### **4. Host Behavior Considerations**

As noted above, the IPv4 Unavailable flag is advisory. Hosts may vary in their treatment of it.

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 could 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.

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 assume that IPv4 is available. If all IPv6 default routers send the flag with value 1, a dual stack host may take this as an indication that IPv4 is probably not available. It is however possible that there is an IPv4-only router on the link.

A host that receives only RAs with the flag set to 1 may choose not to 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.

Alternatively, a host that receives only RAs with the flag set to 1 may choose to attempt IPv4 operations but at significantly lower frequency than normal. For example, it may choose to lengthen the interval between DHCPv4 discovery messages to much longer than the 64 seconds defined by [\[RFC2131\]](#).

A host that receives only RAs with the flag set to 1 may choose not to form an IPv4 link-local address. However, as noted above, if it contains link-local applications that can use IPv4, it may instead choose to form an IPv4 link-local address in the normal way [\[RFC3927\]](#), and then send the discovery traffic for such applications.

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 may now assume that IPv4 is not available. 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.

## 5. IANA Considerations

IANA is requested to assign the new Router Advertisement flag defined in [Section 2](#) 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 should also register this new flag bit in the IANA IPv6 ND Router Advertisement flags Registry [[IANA-RF](#)].

## 6. 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 IPv4 Unavailable 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 2](#). 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 3](#) 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 3](#) 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 IPv4 Unavailable 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.



## **7. 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, Erik Kline, Jen Linkova, Michael Richardson, Mark Smith, James Woodyatt, and other members of the 6MAN working group.

## **8. Change log [RFC Editor: Please remove]**

[draft-hinden-ipv4flag-02](#), 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.

## 9. References

### 9.1. Normative References

- [IANA-RF] "IPv6 ND Router Advertisement flags",  
<<https://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xhtml#icmpv6-parameters-11>>.
- [RFC2131] Droms, R., "Dynamic Host Configuration Protocol", [RFC 2131](#), DOI 10.17487/RFC2131, March 1997, <<https://www.rfc-editor.org/info/rfc2131>>.
- [RFC3927] Cheshire, S., Aboba, B., and E. Guttman, "Dynamic Configuration of IPv4 Link-Local Addresses", [RFC 3927](#), DOI 10.17487/RFC3927, May 2005, <<https://www.rfc-editor.org/info/rfc3927>>.
- [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>>.

### 9.2. Informative References

- [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>>.



[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



