Workgroup: 6man
Internet-Draft:
draft-bonica-6man-deprecate-router-alert-00
Updates: RFC 2711 (if approved)
Published: 30 December 2021
Intended Status: Standards Track
Expires: 3 July 2022
Authors: R. Bonica
Juniper Networks

Deprecation Of The IPv6 Router Alert Option

Abstract

This document deprecates the IPv6 Router Alert Option. Protocols that use the Router Alert Option may continue to do so. However, protocols standardized in the future must not use the Router Alert Option.

Status of This Memo

This Internet-Draft will expire on 3 July 2022.

Copyright Notice

Table of Contents

1. Introduction

Figure 1 models an Internet router. The router has a forwarding plane and a control plane.

```
          ---------------------------------------------------
          |                                                  |
          |                  CONTROL PLANE                   |
          |               (OSPF, ISIS, BGP)                  |
          |                                                  |
          |                 (FIB Read-Write)                 |
          ---------------------------------------------------
                |                   / \
                | FIB updates and    |  Messages addressed
                | routing protocol   |  to the router and
                | messages to        |  messages that contain
                | other nodes        |  the Router Alert Option
               \ /                   |
          ---------------------------------------------------
          |                                                  |
          |                FORWARDING PLANE                  |
          |                    (IPv6)                        |
          |                                                  |
          |                (FIB Read-Only)                   |
          ---------------------------------------------------
```

Figure 1: An Internet Router

IPv6 [RFC8200] operates on the forwarding plane. It:

*Accepts a packet.

*Determines the packet's next hop.

*Forwards the packet to its next hop.

IPv6 determines a packet's next hop by searching the Forwarding Information Base (FIB) for an entry that best matches the packet's destination address. Therefore, IPv6 requires read-only access to the FIB.

Routing protocols (e.g., OSPF, IS-IS, BGP) operate on a router's control plane. They create and maintain the FIB by exchanging routing protocol messages with other nodes. Therefore, the control plane requires read-write access to the FIB.

The forwarding and control planes communicate with one another as follows:

- The control plane sends FIB updates to the forwarding plane so it can maintain a read-only FIB copy.
- The control plane sends routing protocol messages through the forwarding plane to other nodes.
- The forwarding plane sends routing protocol messages received from other nodes and addressed to the router to the control plane.
- The forwarding plane sends messages that are not addressed to the router but include the IPv6 Router Alert Option [RFC2711] to the control plane. The control plane inspects these messages and returns them to the forwarding plane so that they can continue on to their ultimate destination.

Many routers maintain separation between forwarding and control plane hardware. The forwarding plain is implemented on high-performance Application Specific Integrated Circuits (ASIC) and Network Processors (NP), while the control plane is implemented on general-purpose processors. Therefore, the forwarding plane can process many more packets per second than the control plane. Given this difference in packet-handling capabilities, a router's control plane is more susceptible to a Denial-of-Service (DoS) attack than the router's forwarding plane.

[RFC6192] demonstrates how a network operator can deploy Access Control Lists (ACL) that protect the control plane from DoS attack. These ACLs are effective and efficient when they select packets based upon information that can be found in a fixed position in the packet header. However, they become less effective and less efficient when they must parse an IPv6 Hop-by-hop Options extension header, searching for the Router Alert Option. Therefore, many network operators drop or severely rate limit packets that contain the IPv6 Hop-by-hop Options extension header.

[RFC6398] identifies security considerations associated with the Router Alert Option. It provides the following recommendations:

- "Network operators SHOULD actively protect themselves against externally generated IP Router Alert packets."
- "Applications and protocols SHOULD NOT be deployed with a dependency on processing of the Router Alert Option (as currently specified) across independent administrative domains in the Internet."
- "Router implementations of the IP Router Alert Option SHOULD offer the configuration option to simply ignore the presence of "IP Router Alert" in IPv4 and IPv6 packets."
- "A router implementation SHOULD forward within the "fast path" (subject to all normal policies and forwarding rules) a packet carrying the IP Router Alert Option containing a next level protocol that is not a protocol of interest to that router."

NOTE: In RFC 6398, the terms "fast path" and "control plane components" are used synonymously.

Network operators can address all of the security considerations raised in RFC 6398 by configuring their routers to ignore the Router Alert Option. However, such configuration may not be possible if protocol designers continue to design protocols that use the Router Alert Option. Alternatively, network operators will be required to deploy the operationally complex and computationally expensive ACLs described in RFC 6192. Therefore, this document deprecates the IPv6 Router Alert Option.

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. Updates To RFC 2711

This document deprecates the IPv6 Router Alert Option. Protocols that use the Router Alert Option MAY continue to do so. However, protocols standardized in the future MUST NOT use the Router Alert Option.

Table 1 contains a list of protocols that use the IPv6 Router Alert Option. There are no known IPv6 implementations of MPLS PING.

Neither INTSERV nor NSIS are widely deployed. All NSIS protocols are EXPERIMENTAL.

Protocol	References	Application
Multicast Listener Discovery Version 2 (MLDv2)	[RFC3810]	IPv6 Multicast
Multicast Router Discovery (MRD)	[RFC4286]	IPv6 Multicast
MPLS PING	[RFC8029]	MPLS OAM
Resource Reservation Protocol (RSVP)	[RFC3175] [RFC5946] [RFC6016] [RFC6401]	Integrated Services (INTSERV) [RFC1633] (Not Traffic engineering or MPLS signaling)
Next Steps In Signaling (NSIS)	[RFC5979] [RFC5971]	NSIS [RFC4080]

Table 1: Protocols That Use The IPv6 Router Alert Option

4. Security Considerations

This document extends the security considerations provided in RFC 2711, RFC 6192 and RFC 6398.

5. IANA Considerations

IANA is requested to mark the Router Alert Option as Deprecated in the Destination Options and Hop-by-hop Options Registry (https://www.iana.org/assignments/ipv6-parameters/ipv6-parameters.xhtml#ipv6-parameters-2) and add a pointer to this document.

6. Acknowledgements

Thanks to Bob Hinden for his review of this document.

7. References

7.1. Normative References

[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>.

[RFC2711] Partridge, C. and A. Jackson, "IPv6 Router Alert Option", RFC 2711, DOI 10.17487/RFC2711, October 1999, <https://www.rfc-editor.org/info/rfc2711>.

[RFC6398] Le Faucheur, F., Ed., "IP Router Alert Considerations and Usage", BCP 168, RFC 6398, DOI 10.17487/RFC6398, October 2011, <https://www.rfc-editor.org/info/rfc6398>.

[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>.

[RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017, <https://www.rfc-editor.org/info/rfc8200>.

7.2. Informative References

[RFC1633] Braden, R., Clark, D., and S. Shenker, "Integrated Services in the Internet Architecture: an Overview", RFC 1633, DOI 10.17487/RFC1633, June 1994, <https://www.rfc-editor.org/info/rfc1633>.

[RFC3175] Baker, F., Iturralde, C., Le Faucheur, F., and B. Davie, "Aggregation of RSVP for IPv4 and IPv6 Reservations", RFC 3175, DOI 10.17487/RFC3175, September 2001, <https://www.rfc-editor.org/info/rfc3175>.

[RFC3810] Vida, R., Ed. and L. Costa, Ed., "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC 3810, DOI 10.17487/RFC3810, June 2004, <https://www.rfc-editor.org/info/rfc3810>.

[RFC4080] Hancock, R., Karagiannis, G., Loughney, J., and S. Van den Bosch, "Next Steps in Signaling (NSIS): Framework", RFC 4080, DOI 10.17487/RFC4080, June 2005, <https://www.rfc-editor.org/info/rfc4080>.

[RFC4286] Haberman, B. and J. Martin, "Multicast Router Discovery", RFC 4286, DOI 10.17487/RFC4286, December 2005, <https://www.rfc-editor.org/info/rfc4286>.

[RFC5946] Le Faucheur, F., Manner, J., Narayanan, A., Guillou, A., and H. Malik, "Resource Reservation Protocol (RSVP) Extensions for Path-Triggered RSVP Receiver Proxy", RFC

5946, DOI 10.17487/RFC5946, October 2010, <https://www.rfc-editor.org/info/rfc5946>.

[RFC5971] Schulzrinne, H. and R. Hancock, "GIST: General Internet Signalling Transport", RFC 5971, DOI 10.17487/RFC5971, October 2010, <https://www.rfc-editor.org/info/rfc5971>.

[RFC5979] Shen, C., Schulzrinne, H., Lee, S., and J. Bang, "NSIS Operation over IP Tunnels", RFC 5979, DOI 10.17487/RFC5979, March 2011, <https://www.rfc-editor.org/info/rfc5979>.

[RFC6016] Davie, B., Le Faucheur, F., and A. Narayanan, "Support for the Resource Reservation Protocol (RSVP) in Layer 3 VPNs", RFC 6016, DOI 10.17487/RFC6016, October 2010, <https://www.rfc-editor.org/info/rfc6016>.

[RFC6192] Dugal, D., Pignataro, C., and R. Dunn, "Protecting the Router Control Plane", RFC 6192, DOI 10.17487/RFC6192, March 2011, <https://www.rfc-editor.org/info/rfc6192>.

[RFC6401] Le Faucheur, F., Polk, J., and K. Carlberg, "RSVP Extensions for Admission Priority", RFC 6401, DOI 10.17487/RFC6401, October 2011, <https://www.rfc-editor.org/info/rfc6401>.

[RFC8029] Kompella, K., Swallow, G., Pignataro, C., Ed., Kumar, N., Aldrin, S., and M. Chen, "Detecting Multiprotocol Label Switched (MPLS) Data-Plane Failures", RFC 8029, DOI 10.17487/RFC8029, March 2017, <https://www.rfc-editor.org/info/rfc8029>.

Author's Address

Ron Bonica
Juniper Networks
2251 Corporate Park Drive
Herndon, Virginia 20171
United States of America

Email: rbonica@juniper.net