Internet Engineering Task Force (IETF)
Request for Comments: 9805
Updates: 2711
Category: Standards Track
ISSN: 2070-1721

R. Bonica
Juniper Networks

June 2025

Deprecation of the IPv6 Router Alert Option for New Protocols

Abstract

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

This document updates RFC 2711.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9805.

Table of Contents

1. Introduction

In IPv6 [RFC8200], optional internet-layer information is encoded in separate headers that may be placed between the IPv6 header and the upper-layer header in a packet. There is a small number of such extension headers, each one identified by a distinct Next Header value.

One of these extension headers is called the Hop-by-Hop Options header. The Hop-by-Hop Options header is used to carry optional information that may be examined and processed by every node along a packet's delivery path.

The Hop-by-Hop Options header can carry one or more options. Among these is the IPv6 Router Alert option [RFC2711].

The IPv6 Router Alert option provides a mechanism whereby routers can know when to intercept datagrams not addressed to them without having to extensively examine every datagram. The semantic of the IPv6 Router Alert option is that "routers should examine this datagram more closely". Excluding this option tells the router that there is no need to examine this datagram more closely.

As explained below, the IPv6 Router Alert option introduces many issues.

This document updates [RFC2711]. Implementers of protocols that continue to use the IPv6 Router Alert option can continue to reference [RFC2711] for IPv6 Router Alert option details.

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. Issues Associated with the IPv6 Router Alert Option

[RFC6398] identifies security considerations associated with the IPv6 Router Alert option. In a nutshell, the IP Router Alert Option does not provide a universal mechanism to accurately and reliably distinguish between IP Router Alert packets of interest and unwanted IP Router Alerts. This creates a security concern because, short of appropriate router-implementation-specific mechanisms, the router's control plane is at risk of being flooded by unwanted traffic.

> | NOTE: Many routers maintain separation between forwarding and control plane hardware. The forwarding plane is implemented on high-performance Application-Specific Integrated Circuits (ASICs) and Network Processors (NPs), while the control plane is implemented on general-purpose processors. Given this difference, the control plane is more susceptible to a Denial-of-Service (DoS) attack than the forwarding plane.

[RFC6192] demonstrates how a network operator can deploy Access Control Lists (ACLs) that protect the control plane from DoS attacks. These ACLs are effective and efficient when they select packets based upon information that can be found in a fixed position. However, they become less effective and less efficient when they must parse a Hop-by-Hop Options header, searching for the IPv6 Router Alert option.

Network operators can address the security considerations raised in

[RFC6398] by:

* Deploying the operationally complex and computationally expensive ACLs described in [RFC6192].

* Configuring their routers to ignore the IPv6 Router Alert option.

* Dropping or severely rate limiting packets that contain the Hop-by-Hop Options header at the network edge.

These options become less viable as protocol designers continue to design protocols that use the IPv6 Router Alert option.

[RFC9673] seeks to eliminate hop-by-hop processing on the control plane. However, because of its unique function, the IPv6 Router Alert option is granted an exception to this rule. One approach would be to deprecate the IPv6 Router Alert option, because current usage beyond the local network appears to be limited and packets containing Hop-by-Hop options are frequently dropped. Deprecation would allow current implementations to continue using it, but its use could be phased out over time.

4. Deprecation of the IPv6 Router Alert Option

This document deprecates the IPv6 Router Alert option. Protocols that use the IPv6 Router Alert option MAY continue to do so, even in future versions. However, new protocols that are standardized in the future MUST NOT use the IPv6 Router Alert option. Appendix A contains an exhaustive list of protocols that MAY continue to use the IPv6 Router Alert option.

This document updates [RFC2711].

5. Future Work

A number of protocols use the IPv6 Router Alert option; these are listed in Appendix A. The only protocols in Appendix A that have widespread deployment are Multicast Listener Discovery Version 2 (MLDv2) [RFC9777] and Multicast Router Discovery (MRD) [RFC4286]. The other protocols either have limited deployment, are experimental, or have no known implementation.

It is left for future work to develop new versions of MLDv2 and MRD that do not rely on the IPv6 Router Alert option. That task is out of scope for this document.

6. Security Considerations

This document mitigates all security considerations associated with the IPv6 Router Alert option. These security considerations can be found in [RFC2711], [RFC6192], and [RFC6398].

7. IANA Considerations

IANA has marked the IPv6 Router Alert option as "DEPRECATED for New Protocols" in the "Destination Options and Hop-by-Hop Options" registry <https://www.iana.org/assignments/ipv6-parameters> and added this document as a reference.

IANA has also made a note in the "IPv6 Router Alert Option Values" registry <https://www.iana.org/assignments/ipv6-routeralert-values> stating that the registry is closed for allocations and added a reference to this document. The experimental codepoints in this registry have been changed to "Reserved" (i.e., they are no longer available for experimentation).

8. References

8.1. 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>.

[RFC9673] Hinden, R. and G. Fairhurst, "IPv6 Hop-by-Hop Options Processing Procedures", RFC 9673, DOI 10.17487/RFC9673, October 2024, <https://www.rfc-editor.org/info/rfc9673>.

8.2. 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>.

[RFC3031] Rosen, E., Viswanathan, A., and R. Callon, "Multiprotocol Label Switching Architecture", RFC 3031, DOI 10.17487/RFC3031, January 2001, <https://www.rfc-editor.org/info/rfc3031>.

[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>.

[RFC3208] Speakman, T., Crowcroft, J., Gemmell, J., Farinacci, D., Lin, S., Leshchiner, D., Luby, M., Montgomery, T., Rizzo, L., Tweedly, A., Bhaskar, N., Edmonstone, R., Sumanasekera, R., and L. Vicisano, "PGM Reliable Transport Protocol Specification", RFC 3208, DOI 10.17487/RFC3208, December 2001, <https://www.rfc-editor.org/info/rfc3208>.

[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>.

[RFC7506] Raza, K., Akiya, N., and C. Pignataro, "IPv6 Router Alert Option for MPLS Operations, Administration, and Maintenance (OAM)", RFC 7506, DOI 10.17487/RFC7506, April 2015, <https://www.rfc-editor.org/info/rfc7506>.

[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>.

[RFC9570] Kompella, K., Bonica, R., and G. Mirsky, Ed., "Deprecating the Use of Router Alert in LSP Ping", RFC 9570, DOI 10.17487/RFC9570, May 2024, <https://www.rfc-editor.org/info/rfc9570>.

[RFC9777] Haberman, B., Ed., "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", STD 101, RFC 9777, DOI 10.17487/RFC9777, March 2025, <https://www.rfc-editor.org/info/rfc9777>.

Appendix A. Protocols That Use the IPv6 Router Alert Option

Table 1 contains an exhaustive list of protocols that use the IPv6 Router Alert option. There are no known IPv6 implementations of MPLS Ping. Neither Integrated Services (Intserv) nor Next Steps in Signaling (NSIS) are widely deployed. All NSIS protocols are experimental. Pragmatic Generic Multicast (PGM) is experimental, and there are no known IPv6 implementations.

Protocol	References	Application
Multicast Listener Discovery Version 2 (MLDv2)	[RFC9777]	IPv6 Multicast
Multicast	[RFC4286]	IPv6 Multicast

Router Discovery (MRD)			
Pragmatic General Multicast (PGM)	[RFC3208]	IPv6 Multicast	
MPLS Ping (Use of the IPv6 Router Alert option is deprecated)	[RFC7506][RFC8029][RFC9570]	MPLS Operations, Administration, and Maintenance (OAM)	
Resource Reservation Protocol (RSVP): Both IPv4 and IPv6 implementations	[RFC3175] [RFC5946] [RFC6016] [RFC6401]	Integrated Services (Intserv) [RFC1633] and Multiprotocol Label Switching (MPLS) [RFC3031]	
Next Steps in Signaling (NSIS)	[RFC5979] [RFC5971]	NSIS [RFC4080]	

Table 1: Protocols That Use the IPv6 Router Alert Option

Acknowledgements

Thanks to Zafar Ali, Brian Carpenter, Toerless Eckert, David Farmer, Adrian Farrel, Bob Hinden, and Jen Linkova for their reviews of this document.

Author’s Address

Ron Bonica
Juniper Networks
United States of America
Email: rbonica@juniper.net