Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79. This document may contain material from IETF Documents or IETF Contributions published or made publicly available before November 10, 2008. The person(s) controlling the copyright in some of this material may not have granted the IETF Trust the right to allow modifications of such material outside the IETF Standards Process. Without obtaining an adequate license from the person(s) controlling the copyright in such materials, this document may not be modified outside the IETF Standards Process, and derivative works of it may not be created outside the IETF Standards Process, except to format it for publication as an RFC or to translate it into languages other than English.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on January 4, 2010.

Copyright Notice

Copyright (c) 2009 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 in effect on the date of publication of this document (http://trustee.ietf.org/license-info). Please review these documents carefully, as they describe your rights and restrictions with respect to this document.
Abstract

The IP Router Alert Option is an IP option that alerts transit routers to more closely examine the contents of an IP packet. RSVP, PGM, IGMP/MLD and MRD are some of the protocols which make use of the IP Router Alert option. This document discusses security aspects, common practices and usage guidelines around the use of the current IP Router Alert option. Specifically, it provides recommendations on the use of Router Alert by new protocols, discusses controlled environments where existing protocols depending on Router Alert can be used effectively and discusses protection approaches for Service Providers. Finally it provides brief guidelines for Router Alert implementation on routers.

Table of Contents

1. Terminology .................................. 4
   1.1. Conventions Used in This Document ............. 4
2. Introduction .................................. 5
3. Guidelines for use of Router Alert .................. 7
   3.1. Use of Router Alert by New Protocols .......... 7
   3.2. Use of Router Alert by Existing Protocols in Controlled Environments .................. 8
   3.3. Router Alert Protection Approaches for Service Providers .......................... 8
4. Guidelines for Router Alert Implementation ........... 11
5. Security Considerations .......................... 12
6. IANA Considerations ............................. 13
7. Contributors .................................. 14
8. Acknowledgments ............................... 15
9. References ..................................... 16
   9.1. Normative References .......................... 16
   9.2. Informative References ........................ 16
Author's Address ................................. 18
1. Terminology

For readability, this document uses the following loosely defined terms:

- **Slow path**: Software processing path for packets
- **Fast path**: ASIC/Hardware processing path for packets

1.1. Conventions Used in This Document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].
2. Introduction

[RFC2113] and [RFC2711] respectively define the IPv4 and IPv6 Router Alert Option. In this document, we collectively refer to those as the IP Router Alert. RSVP ([RFC2205], [RFC3175], [RFC3209]), PGM ([RFC3208]), IGMP ([RFC3376]), MLD ([RFC2710], [RFC3810]) and MRD ([RFC4286]) are some of the protocols which make use of the IP Router Alert. Those protocols are used in different ways, possibly even in multiple ways simultaneously: For example, they are used to support critical elements of the Internet infrastructure (e.g. RSVP-TE for traffic engineering within a service provider network) and as such they need to be protected; As another example, they are also used end to end, say inside a company’s private network, often transiting over the Internet infrastructure.

IP datagrams carrying the IP Router Alert are usually examined in a router’s slow path and an excess of such datagrams can cause performance degradation or packet drops in a router’s slow path.

[RFC4081] and [RFC2711] mention the security risks associated with the use of the IP Router Alert: flooding a router with bogus IP datagrams which contain the IP Router Alert would cause a performance degradation of the router’s slow path and can also lead to packet drops in the slow path.

[RFC2113] specifies no mechanism for identifying different users of IP Router Alert. As a result, many fast switching implementations of IP Router Alert punt most/all packets marked with IP Router Alert into the slow path. Some IP Router Alert implementations may be able to take into account the IP PID [RFC0791] as a discriminator for the punting decision for different protocols using IP Router Alert. However, this still only allows very coarse triage among various protocols using IP Router Alert for two reasons. First, the IP PID is the same when IP Router Alert is used for different applications of the same protocol (e.g., RSVP vs. RSVP-TE), or when IP Router Alert is used for different contexts of the same application (e.g., different levels of RSVP aggregation [RFC3175]). Thus, it is not possible to achieve the necessary triage in the fast path across IP Router Alert packets from different applications or from different contexts of an application. Secondly, some protocols requiring punting may be carried over a transport protocol (e.g., TCP or UDP) possibly because they require the services of that transport protocol or perhaps because the protocol does not justify allocation of a scarce IP PID value. Thus, considering the PID does not allow triage in the fast path of IP Router Alert packets from different protocols sharing the same transport protocol. Therefore, it is generally not possible to ensure that only the IP Router Alert packets of interest are punted to the slow path while other IP Router Alert packets are
efficiently forwarded (i.e., in fast path).

[RFC2711] mentions that limiting, by rate or some other means, the use of IP Router Alert option is a way of protecting against a potential attack. However, if rate limiting is used as a protection mechanism but if the granularity of the rate limiting is not fine enough to distinguish among IP Router Alert packet of interest from unwanted IP Router Alert packet, a IP Router Alert attack could still severely degrade operation of protocols of interest that depend on the use of IP Router Alert.

In some environments where it is not possible to accurately and reliably distinguish between IP Router Alert packets of interest and unwanted IP Router Alert packets, operators have resorted to actively protecting themselves against externally generated IP Router Alert packets in ways that result in end to end IP Router Alert packets being (occasionally or systematically) dropped and/or ignored on a segment. The consequences of such practises on the use of IP Router Alert by new applications and protocols are discussed in Section 3.1 of the present document.

Section 3.2 discusses environments where existing applications/protocols relying on IP Router Alert can be deployed effectively and safely.

Section 3.3 provides recommendations on protection approaches to be used by Service Providers in order to protect their network from Router Alert based attacks.

Finally, Section 4 provides generic recommendations for router implementation of Router Alert aiming at increasing protection against attacks.

The present document discusses considerations and practises based on the current specification of IP Router Alert ([RFC2113], [RFC2711]). Possible future enhancements to the specification of IP Router Alert (in view of reducing the security risks associated with the use of IP Router Alert) are outside the scope of this document. A proposal for such enhancements can be found in [I-D.narayanan-rtg-router-alert-extension].
3. Guidelines for use of Router Alert

3.1. Use of Router Alert by New Protocols

First, as mentioned earlier, some networks actively protect themselves against externally generated IP Router Alert packets. This may be by tunneling IP Router Alert packets [I-D.dasmith-mpls-ip-options] so that the IP Router Alert option is hidden through that network or it may be via mechanisms resulting in occasional (e.g., rate limiting) or systematic drop of IP Router Alert packets.

Secondly, application protocols are often not carried directly on top of IP but rather are carried by a transport protocol such as UDP, TCP, or SCTP that in turns runs over IP. In these cases, the application protocol is not visible in the IP header (that only contains information about the transport protocol) and could not be determined without further "deep packet" inspection. In the event of the IP Router Alert option being used for an application protocol carried in a transport protocol, the intercepted IP packet would be delivered to the transport protocol for processing in accordance with [RFC2113] (as opposed to being delivered directly to the application protocol). However, the behavior of the transport protocol in these circumstances is not defined, and may cause rejection of the packet for various reasons.

As a consequence, in the general case of open networks, applications can not safely rely on IP Router Alert packets being visible to all nodes on the path today, and more importantly can not even rely on IP Router Alert packets being transported end to end.

[RFC2113] implies that the router may examine other fields of a received packet that contains the IP Router Alert option to decide whether that packet needs further processing, but no further advice is given. Examination of other fields of the received IP packet that carries the IP Router Alert to help determine what to do with the packet would result in implementation-specific behavior that is unpredictable to the sender of the packet. Therefore applications cannot depend on IP Router Alert interception involving inspection of fields in the packet outside the IP header.

Thus, creating a new application or end-to-end protocol that depends on use of the current IP Router Alert ([RFC2113], [RFC2711]) is considered harmful and it is RECOMMENDED that new application or protocol be developed without using IP Router Alert. A different mechanism SHOULD be used in order to increase likelihood of operation of that application/protocol end-to-end and to decrease the risk of impacting existing protocols that use the IP Router Alert option.
3.2. Use of Router Alert by Existing Protocols in Controlled Environments

In some controlled environments, the network administrator can determine that IP Router Alert packets will only be received from trusted well-behaved devices or can establish that the protection mechanisms discussed in the present document against the plausible RAO-based DoS attacks (e.g., RAO filtering and rate-limiting) are sufficient. In that case, an application relying on exchange and handling of RAO packets (e.g., RSVP) may be safely deployed within the controlled network. A private enterprise network firewall from the Internet and using RSVP for voice and video reservation and admission control may be an example of such controlled environment.

In some environments, the network administrator can reliably ensure that router alert packets from any untrusted device (e.g., from external routers) are prevented from entering a trusted area (e.g., the internal routers). For example, this may be achieved by ensuring that routers straddling the trust boundary (e.g., edge routers) always encapsulate those packets (without setting IP Router Alert -or equivalent- in the encapsulating header) through the trusted area (as discussed in [I-D.dasmith-mpls-ip-options]). In such environments, the risks of DOS attacks through the IP Router Alert vector is removed in the trusted area (or greatly reduced) even if IP Router Alert is used inside the trusted area (say for RSVP-TE). Thus an application relying on IP Router Alert may be safely deployed within the trusted area. A Service Provider running RSVP-TE within his network may be an example of such protected environment.

When a controlled environment requires RAO packet exchange across his routers for some application (e.g., RSVP) and transits via a Service Provider network (that is not part of the controlled environment), the administrator of the controlled environment needs to ensure with the Service Provider that the Service Provider network protects itself from IP Router Alert messages without dropping those when they transit over the Service Provider network (for example using mechanisms discussed in [I-D.dasmith-mpls-ip-options]). In this case, an application relying on IP Router Alert (e.g. RSVP) may be deployed within the controlled environment and effectively transparently over the Service Provider network without affecting the security of the Service Provider network.

3.3. Router Alert Protection Approaches for Service Providers

Section 2 discusses the security risks associated with the use of the IP Router Alert and how it opens up a DOS vector in the router control plane. Opening up a hole in the control plane of Service Provider edge routers is commonly done for other applications such as
BGP peering. However, the resulting DOS attack vector is arguably more serious with Router Alert option than with BGP peering for a number of reasons including:

- with BGP, a DOS attack would only affect the edge router(s), while with Router Alert option, the attack could propagate to core routers
- with BGP, the BGP policy control would typically prevent re-injection of undesirable information out of the attacked device, while with Router-Alert option, the non-filtered attacking messages would typically be forwarded downstream.

Thus, it is RECOMMENDED that a Service Provider implements strong protection of his network against attacks based on IP Router Alert.

Since some existing applications would benefit from end-to-end transport of IP Router Alert packets (e.g. RSVP in a controlled environment), it is RECOMMENDED that a Service Provider protects his network from attacks based on IP Router Alert using mechanisms that avoid (or at least minimize) dropping of end to end IP Router Alert packets (other than those involved in the attack).

For example, if the Service Provider does not run any protocol depending on IP Router Alert within his network, he may elect to simply turn-off punting of IP Router Alert packet on his routers; this will ensure that end-to-end IP Router Alert packet transit transparently and safely through his network.

As another example, using protection mechanisms such selective filtering and rate-limiting (that Section 4 suggests be supported by IP Router Alert implementations) a Service Provider can protect the operation of a protocol depending on IP Router Alert within his network (e.g., RSVP-TE) while at the same time transporting IP Router Alert packets carrying another protocol that may be used end to end. Note that the Service Provider might additionally use protocol specific mechanisms that reduce the dependency on Router Alert for operation of this protocol inside the Service Provider environment; use of RSVP refresh reduction mechanisms ([RFC2961]) would be an example of such mechanisms in the case where the Service Provider is running RSVP-TE within his network since this allows refresh of existing Path and Resv states without use of the IP Router Alert option.

As yet another example, using mechanisms such as those discussed in [I-D.dasmith-mpls-ip-options] a Service Provider can safely protect the operation of a protocol depending on IP Router Alert within his network (e.g., RSVP-TE) while at the same time safely transporting IP
Router Alert packets carrying another protocol that may be used end to end (e.g., IPv4/IPv6 RSVP).

As a last resort, if the SP does not have any means to safely transport end to end IP Router Alert option packets over his network, the SP MAY drop those packets.
4. Guidelines for Router Alert Implementation

It is RECOMMENDED that router implementations of IP Router Alert option include protection mechanisms against Router Alert based DOS attacks appropriate for their targeted deployment environments. For example, this can include ability on an edge router to "tunnel" IP Router Alert option of received packets when forwarding those over the core as discussed in [I-D.dasmith-mpls-ip-options]. As another example, although not always available from current implementations, new implementations may include protection mechanisms such as selective (possibly dynamic) filtering and rate-limiting of IP Router Alert option packets.

If an IP packet contains the IP Router Alert option, but the payload protocol is not explicitly identified as a Payload of interest by the router examining the packet, the behavior is not explicitly defined by [RFC2113]. However, the behavior is implied and, for example, the definition of RSVP in [RFC2205] assumes that the packet will be forwarded using normal forwarding based on the destination IP address. Thus, 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 payload that is not a payload of interest to that router. The "not passing" behavior protects the router from DOS attacks using IP Router Alert packets of a protocol unknown to the router. The "forwarding" behavior contributes to transparent end to end transport of IP Router Alert packets (e.g., to facilitate their use by end to end application).
5. Security Considerations

This document discusses security risks associated with current usage of the IP Router Alert Option and associated practices.
6. IANA Considerations

None.
7. Contributors

The contributors to this document (in addition to the editors) are:

- Reshad Rahman:
  * Cisco Systems
  * rrahman@cisco.com

- David Ward:
  * Cisco Systems
  * wardd@cisco.com

- Ashok Narayanan:
  * Cisco Systems
  * ashokn@cisco.com

- Adrian Farrell:
  * OldDog Consulting
  * adrian@olddog.co.uk

- Tony Li:
  * tony.li@tony.li
8. Acknowledgments

We would like to thank Dave Oran, Magnus Westerlund, John Scudder, Ron Bonica, Ross Callon and Alfred Hines for their comments.
9. References

9.1. Normative References


9.2. Informative References


[RFC3208] Speakman, T., Crowcroft, J., Gemmell, J., Farinacci, D., Lin, S., Leshchiner, D., Luby, M., Montgomery, T., Rizzo,


Author’s Address

Francois Le Faucheur (editor)
Cisco Systems
Greenside, 400 Avenue de Roumanille
Sophia Antipolis  06410
France

Phone: +33 4 97 23 26 19
Email: flefauch@cisco.com