                          IPv6 Router Alert Option

Status of this Memo

Copyright Notice

Abstract

   This memo describes a new IPv6 Hop-by-Hop Option type that alerts
   transit routers to more closely examine the contents of an IP
   datagram. This option is useful for situations where a datagram
   addressed to a particular destination contains information that may
   require special processing by routers along the path.

1.0 Introduction

   New protocols, such as RSVP, use control datagrams which, while
   addressed to a particular destination, contain information that needs
   to be examined, and in some case updated, by routers along the path
   between the source and destination. It is desirable to forward
   regular datagrams as rapidly as possible, while ensuring that the
   router processes these special control datagrams appropriately.
   Currently, however, the only way for a router to determine if it
   needs to examine a datagram is to at least partially parse upper
   layer data in all datagrams. This parsing is expensive and slow.
   This situation is undesirable.

   This document defines a new option within the IPv6 Hop-by-Hop Header.
   The presence of this option in an IPv6 datagram informs the router
   that the contents of this datagram is of interest to the router and
   to handle any control data accordingly. The absence of this option
   in an IPv6 datagram informs the router that the datagram does not
   contain information needed by the router and hence can be safely

routed without further datagram parsing. Hosts originating IPv6
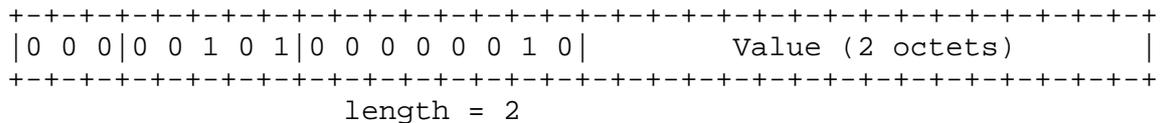datagrams are required to include this option in certain
circumstances.

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 [RFC-2119].

2.0 Approach

The goal is to provide an efficient mechanism whereby routers can
know when to intercept datagrams not addressed to them without having
to extensively examine every datagram. The described solution is to
define a new IPv6 Hop-by-Hop Header option having the semantic
"routers should examine this datagram more closely" and require
protocols such as RSVP to use this option. This approach incurs
little or no performance penalty on the forwarding of normal
datagrams. Not including this option tells the router that there is
no need to closely examine the contents of the datagram.

2.1 Syntax

The router alert option has the following format:

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|0 0 0|0 0 1 0 1|0 0 0 0 0 0 1 0|          Value (2 octets)      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
             length = 2
```

The first three bits of the first byte are zero and the value 5 in
the remaining five bits is the Hop-by-Hop Option Type number.
[RFC-2460] specifies the meaning of the first three bits. By
zeroing all three, this specification requires that nodes not
recognizing this option type should skip over this option and
continue processing the header and that the option must not change
en route.

There MUST only be one option of this type, regardless of value,
per Hop-by-Hop header.

Value: A 2 octet code in network byte order with the following
values:

0	Datagram contains a Multicast Listener Discovery message [RFC-2710].
1	Datagram contains RSVP message.
2	Datagram contains an Active Networks message.
3-65535	Reserved to IANA for future use.

Alignment requirement: 2n+0

Values are registered and maintained by the IANA. See section 5.0
for more details.

2.2 Semantics

The option indicates that the contents of the datagram may be
interesting to the router. The router's interest and the actions
taken by employing Router Alert MUST be specified in the RFC of the
protocol that mandates or allows the use of Router Alert.

The final destination of the IPv6 datagram MUST ignore this option
upon receipt to prevent multiple evaluations of the datagram.
Unrecognized value fields MUST be silently ignored and the processing
of the header continued.

Routers that recognize the option will examine datagrams carrying it
more closely to determine whether or not further processing is
necessary. The router only needs to parse the packet in sufficient
detail to decide whether the packet contains something of interest.
The value field can be used by an implementation to speed processing
of the datagram within the transit router.

Observe that further processing can involve protocol layers above
IPv6. E.g., for RSVP messages, the datagram will have to undergo UDP
and RSVP protocol processing. Once the datagram leaves the IPv6
layer, there is considerable ambiguity about whether the router is
acting as an IPv6 host or an IPv6 router. Precisely how the router
handles the contents is value-field specific. However, if the
processing required for the datagram involves examining the payload
of the IPv6 datagram, then the interim router is performing a host
function and SHOULD interpret the data as a host.

3.0 Impact on Other Protocols

   For this option to be effective, its use MUST be mandated in
   protocols that expect routers to perform significant processing on
   datagrams not directly addressed to them. Routers are not required
   to examine the datagrams not addressed to them unless the datagrams
   include the router alert option.

   All IPv6 datagrams containing an RSVP message MUST contain this
   option within the IPv6 Hop-by-Hop Options Header of such datagrams.

4.0 Security Considerations

   Gratuitous use of this option can cause performance problems in
   routers. A more severe attack is possible in which the router is
   flooded by bogus datagrams containing router alert options.

   The use of the option, if supported in a router, MAY therefore be
   limited by rate or other means by the transit router.

5.0 IANA Considerations

   The value field described in Section 2.1 is registered and maintained
   by IANA. New values are to be assigned via IETF Consensus as defined
   in RFC 2434 [RFC-2434].

6.0 Notice on Intellectual Property

   The IETF takes no position regarding the validity or scope of any
   intellectual property or other rights that might be claimed to
   pertain to the implementation or use of the technology described in
   this document or the extent to which any license under such rights
   might or might not be available; neither does it represent that it
   has made any effort to identify any such rights. Information on the
   IETF's procedures with respect to rights in standards-track and
   standards-related documentation can be found in BCP-11. Copies of
   claims of rights made available for publication and any assurances of
   licenses to be made available, or the result of an attempt made to
   obtain a general license or permission for the use of such
   proprietary rights by implementors or users of this specification can
   be obtained from the IETF Secretariat.

   The IETF invites any interested party to bring to its attention any
   copyrights, patents or patent applications, or other proprietary
   rights which may cover technology that may be required to practice
   this standard. Please address the information to the IETF Executive
   Director.

7.0 References

   [RFC-2119] Bradner, S., "Key words for use in RFC's to Indicate
              Requirement Levels", BCP 14, RFC 2119, March 1977.

   [RFC-2205] Braden, B. (ed.), Zhang, L., Berson, S., Herzog, S. and S.
              Jamin, "Resource ReSerVation Protocol (RSVP)", RFC 2205,
              September 1997.

   [RFC-2434] Narten, T. and H. Alvestrand, "Guidelines for Writing an
              IANA Considerations Section in RFCs", BCP 26, RFC 2434,
              October 1998.

   [RFC-2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6
              (IPv6) Specification", RFC 2460, December 1998.

   [RFC-2710] Deering, S., Fenner, W. and B. Haberman, "Multicast
              Listener Discovery (MLD) for IPv6", RFC 2710, October
              1999.

6.0 Authors' Addresses

   Craig Partridge
   BBN Technologies
   10 Moulton Street
   Cambridge, MA 02138
   USA

   Phone: +1 (617) 873-3000
   EMail: craig@bbn.com

   Alden Jackson
   BBN Technologies
   10 Moulton Street
   Cambridge, MA 02138
   USA

   Phone: +1 (617) 873-3000
   EMail: awjacks@bbn.com

7.0 Full Copyright Statement

Acknowledgement