                        IP Router Alert Option

Status of this Memo

Abstract

   This memo describes a new IP Option type that alerts transit routers
   to more closely examine the contents of an IP packet. This is useful
   for, but not limited to, new protocols that are addressed to a
   destination but require relatively complex processing in routers
   along the path.

1.0 Introduction

   A recent trend in routing protocols is to loosely couple new routing
   functionality to existing unicast routing. The motivation for this
   is simple and elegant -- it allows deployment of new routing
   functionality without having to reinvent all of the basic routing
   protocol functions, greatly reducing specification and implementation
   complexity.

   The downside of this is that the new functionality can only depend on
   the least common denominator in unicast routing, the next hop toward
   the destination. No assumptions can be made about the existence of
   more richly detailed information (such as a link state database).

   It is also desirable to be able to gradually deploy the new
   technology, specifically to avoid having to upgrade all routers in
   the path between source and destination. This goal is somewhat at
   odds with the least common denominator information available, since a
   router that is not immediately adjacent to another router supporting
   the new protocol has no way of determining the location or identity
   of other such routers (unless something like a flooding algorithm is
   implemented over unicast forwarding, which conflicts with the
   simplicity goal).

One obvious approach to leveraging unicast routing is to do hop-by-
hop forwarding of the new protocol packets along the path toward the
ultimate destination. Each system that implements the new protocol
would be responsible for addressing the packet to the next system in
the path that understood it. As noted above, however, it is
difficult to know the next system implementing the protocol. The
simple, degenerate case is to assume that every system along the path
implements the protocol. This is a barrier to phased deployment of
the new protocol, however.

RSVP [1] finesses the problem by instead putting the address of the
ultimate destination in the IP Destination Address field, and then
asking that every RSVP router make a "small change in its ...
forwarding path" to look for the specific RSVP packet type and pull
such packets out of the mainline forwarding path, performing local
processing on the packets before forwarding them on. This has the
decided advantage of allowing automatic tunneling through routers
that don't understand RSVP, since the packets will naturally flow
toward the ultimate destination. However, the performance cost of
making this Small Change may be unacceptable, since the mainline
forwarding path of routers tends to be highly tuned--even the
addition of a single instruction may incur penalties of hundreds of
packets per second in performance.

2.0 Router Alert Option

The goal, then, is to provide a mechanism whereby routers can
intercept packets not addressed to them directly, without incurring
any significant performance penalty. This document defines a new IP
option type, Router Alert, for this purpose.

The Router Alert option has the semantic "routers should examine this
packet more closely". By including the Router Alert option in the IP
header of its protocol message, RSVP can cause the message to be
intercepted while causing little or no performance penalty on the
forwarding of normal data packets.

Routers that support option processing in the fast path already
demultiplex processing based on the option type field. If all option
types are supported in the fast path, then the addition of another
option type to process is unlikely to impact performance. If some
option types are not supported in the fast path, this new option type
will be unrecognized and cause packets carrying it to be kicked out
into the slow path, so no change to the fast path is necessary, and
no performance penalty will be incurred for regular data packets.

Routers that do not support option processing in the fast path will
cause packets carrying this new option to be forwarded through the
slow path, so no change to the fast path is necessary and no
performance penalty will be incurred for regular data packets.

2.1 Syntax

The Router Alert option has the following format:

```
          +--------+--------+--------+--------+
          |10010100|00000100|  2 octet value  |
          +--------+--------+--------+--------+
```

Type:
  Copied flag: 1 (all fragments must carry the option)
  Option class: 0 (control)
  Option number: 20 (decimal)

Length: 4

Value: A two octet code with the following values:
  0 - Router shall examine packet
  1-65535 - Reserved

2.2 Semantics

Hosts shall ignore this option. Routers that do not recognize this
option shall ignore it. Routers that recognize this option shall
examine packets carrying it more closely (check the IP Protocol
field, for example) to determine whether or not further processing is
necessary. Unrecognized value fields shall be silently ignored.

The semantics of other values in the Value field are for further
study.

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
packets not directly addressed to them. Currently such protocols
include RSVP [1] and IGMP [2].

4.0 Security Considerations

If the Router Alert option is not set and should be set, the behavior
of the protocol using the Router Alert, e.g., RSVP or IGMPv2, will be
adversely affected since the protocol relies on the use of the Router
Alert option.

If the Router Alert option is set when it should not be set, it is likely that the flow will experience a performance penalty, as a packet whose Router Alert option is set will not go through the router's fastpath and will be processed in the router more slowly than if the option were not set.

5.0 References

   [1] Braden, B. (ed.), L. Zhang, D. Estrin, S. Herzog, S. Jamin,
       "Resource ReSerVation Protocol (RSVP)," work in progress, March
       1996.

   [2] Fenner, W., "Internet Group Management Protocol, Version 2
       (IGMPv2)," work in progress, October 1996.

Author's Address

     Dave Katz
     cisco Systems
     170 W. Tasman Dr.
     San Jose, CA 95134-1706 USA

     Phone: +1 408 526 8284
     Email: dkatz@cisco.com