NSIS
Internet-Draft
Intended status: Experimental
Expires: May 21, 2009

R. Hancock
Roke Manor Research

November 17, 2008

Using the Router Alert Option for Packet Interception in GIST
draft-hancock-nsis-gist-rao-00

Status of this Memo

Abstract

The Generic Internet Signalling Transport (GIST) protocol depends on packet interception to identify the nodes that should participate in signalling sessions. The base protocol assumes n-tuple analysis of the packet header as the interception algorithm. This document describes an experimental extension to GIST to use the Router Alert Option (RAO) to enhance interception efficiency. It describes the tradeoffs in using such an approach including the impact on legacy equipment and protocol deployability, and also the considerations to be taken into account in selecting values for the RAO value field.

Table of Contents

1. Introduction

The Generic Internet Signalling Transport (GIST) protocol [I-D.ietf-nsis-ntlp] is designed to provide a general-purpose messaging layer to carry signalling between end systems and forwarding nodes (routers, middleboxes, etc.) in the Internet. GIST supports multiple signalling applications, each of which is implemented by an NSIS Signalling Layer Protocol (NSLP). GIST defines a number of different message routing methods to support different types of signalling: for example, routing signalling messages along the path taken by a data flow, or routing signalling messages to an egress gateway of a stub network. These message routing methods require GIST operation to be aware of the topology of the underlying infrastructure.

Rather than depending on the availability of global network topology information, GIST uses packet interception to identify the nodes that should participate in signalling sessions. Query packets are injected into the network, encapsulated so they should follow a path consistent with what is required for the signalling; GIST unaware nodes are supposed to forward these Query packets as normal data traffic, while GIST-aware nodes can extract them from the data path and begin signalling with the Query sender.

The GIST protocol as defined in [I-D.ietf-nsis-ntlp] assumes n-tuple analysis of the packet header as the interception algorithm. This document describes an experimental extension to GIST to use the Router Alert Option (RAO) to enhance interception efficiency. It describes the tradeoffs in using such an approach, including the impact on legacy equipment and protocol deployability, and also the considerations to be taken into account in selecting values for the RAO value field.

The structure of this document as follows. Section 2 describes the requirements that GIST has for packet interception in general, and Section 3 discusses the major alternative approaches and theoretical tradeoffs. Section 4 describes the issues that arise in practice with existing equipment and deployment practices, which render the RAO difficult to use in some networks. The modifications to GIST operation are given in Section 5, and corresponding IANA considerations in Section 6. Finally, security considerations are given in Section 7.

1.1. Requirements Language

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 [RFC2119].

2. Q-Mode Encapsulation Requirements

The requirements on encapsulation of GIST Q-mode messages can be considered from two perspectives: functionally, and from the point of view of the different types of node that have to handle the message. These requirements apply essentially identically to IPv4 and IPv6.

	Requirement on non-GIST nodes	Requirement on GIST nodes
Routing	Must be forwarded in a way compatible with the message routing requirements, based only on the IP header	Special processing; forwarding could take into account the contents of GIST payloads
Transparency	Packets must be forwarded (and not dropped) unchanged	Only packets that are genuine signalling packets must be intercepted
Interception	No interception, and no or minimal overhead on passing through the node	Efficiently intercept those packets related to NSLPs implemented on the node, but forward others transparently

Table 1: Q-Mode Encapsulation Requirements

Note that, to retain some possibility of running GIST through NATs, the GIST Q-mode encapsulation is fixed as being UDP; this means that correct routing through non-GIST nodes depends on the assumption that forwarding is on the basis of the IP header only. There are additional features of the payload encapsulation that prevent GIST nodes incorrectly processing non-GIST packets that happen to use the same port number as GIST. GIST nodes are required to re-inject such packets onto the forwarding path transparently. All these requirements are handled by the Q-mode encapsulation rules defined in the base GIST specification.

One particular requirement that distinguishes GIST from (for example) RSVP is the requirement to support multiple NSLPs. A GIST node might implement a single NSLP or it might implement several; it is extremely unlikely to support all of them (because the set is extensible). Therefore, the interception requirement for any specific GIST node is to extract Q-mode messages for a strict subset of NSLPs, and to forward the other Q-mode messages transparently. This can be achieved by intercepting all Q-mode messages, and re-

injecting irrelevant ones back on to the forwarding path after some additional GIST processing, which is the behaviour implemented in the current GIST specification.

3. Design Space Discussion

In this section, we compare two interception approaches:

- Using header n-tuple analysis, namely the use of a specific UDP destination port. This is the approach of the current GIST specification.

- Using the Router Alert Option (RAO), defined for IPv4 in [RFC2113] and IPv6 in [RFC2711]. This is the approach defined experimentally in this document.

The RAO analysis here makes the assumption that the value field in the RAO can be assigned non-zero values, and that these values can be used to filter subclasses of messages. This has long been the case for IPv6. For IPv4, there are two issues:

- The existence of the necessary IANA registries. These are established in [RFC5350].

- Whether the router alert is a feasible mechanism for use in the current Internet, taking into the account the contraints imposed by existing implementations. Some aspects of this are discussed in [I-D.rahman-rtg-router-alert-dangerous].

This comparison is obviously not exhaustive. For example, there could be approaches based on using a new IP protocol number (like RSVP); however, these are ruled out a priori for NAT traversal issues. We also ignore non-interception approaches, where a candidate forwarding node is discovered by some other means (e.g. a topology database, or traceroute) and addressed directly. (The latter is considered further in Section 4.)

Consider the handling of various packet/node-type combinations: a data (non-signalling packet); a non-GIST node handling a signalling packet; a GIST node handling a signalling packet where it does not host the NSLP; and a GIST node handling a signalling packet where it does host the NSLP. The two interception approaches are compared in the following table:

	Interception on n-tuple analysis	Interception on RAO analysis
Data packet (non-GIST node)	Zero cost (n-tuple analysis not performed)	Zero cost (RAO not present)
Signalling packet (non-GIST node)	Zero cost (n-tuple analysis not performed)	Cost to handle and forward RAO; possibly on slow path
Data packet (GIST node)	Cost to process header n-tuple	Zero cost (RAO not present)
Signalling packet (GIST node not hosting NSLP)	Cost to process header n-tuple, extract GIST header and read NSLPID, re-inject packet	Cost to read RAO value and determine not relevant to local signalling
Signalling packet (GIST node hosting NSLP)	Irrelevant (dominated by other signalling costs)	Irrelevant (dominated by other signalling costs)

Table 2: Q-Mode Encapsulation Requirements

Clearly, n-tuple analysis is the most favourable for non-GIST nodes; the impact of using RAO depends on the quality of the RAO implementation (in particular, whether they are able to filter on unknown RAO values). The GIST nodes the situation is the opposite: the n-tuple analysis must be carried out for every packet (not just signalling ones), and if there is GIST traffic not relevant to the node then it requires analysis of the GIST payload to detect this. Note that in theory, the latter step would require UDP checksum validation; however, ignoring checksum validation for the initial NSLPID check does not lead to any new error cases. On the other hand, the mere IP/transport header analysis itself may be expensive, and this is particularly the case for IPv6 (where getting to the transport header might require traversing IP destination options).

4. Compatibility Constraints

GIST depends on the transmission of Q-mode packets through the network, and their interception at GIST-aware nodes. The requirements for GIST-aware nodes are easy to ensure whichever design approach is selected, and the issues are of load and extensibility (see Section 3 above).

However, GIST packets will also encounter non-GIST nodes, for which the requirement of transparent forwarding might not be satisfied. If non-GIST nodes block Q-mode packets, GIST will not function. It is always possible for middleboxes to block specific traffic types; by using a normal UDP encapsulation for Q-mode traffic, GIST allows NATs at least to pass these messages, and firewalls can be configured with standard policies. However, for any Q-mode encapsulation using RAO, this can lead to additional problems. The situation is different for IPv4 and IPv6.

The IPv4 RAO is defined by [RFC2113], which defines the RAO format with a 2-byte value field; however, only one value (zero) was defined, and the IANA registry for further allocations was only established in [RFC5350]. [RFC2113] states that unknown values should be ignored (i.e. the packets forwarded as normal IP traffic); however, it has also been reported that some existing implementations simply ignore the RAO value completely (i.e. process any packet with an RAO as though the option value was zero). Therefore, a Q-mode encapsulation using non-zero RAO values cannot be relied on to make Q-mode traffic transparent to existing implementations. (Note that it may still be valuable to be able to allocate non-zero RAO values for IPv4: this makes the interception process more efficient for nodes which do examine the value field, and makes no difference to nodes which - incorrectly - ignore it. Whether or not non-zero RAO values are used does not change the GIST protocol operation, but needs to be decided when new NSLPs are registered.)

The second stage of the analysis is therefore what happens when a non-GIST node which implements RAO handling sees a Q-mode packet. The RAO specification simply states that "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." There are two possible basic behaviours for GIST traffic:

1. The "closer examination" of the packet is sufficiently intelligent to realise that the node does not need to process it and should forward it. This could either be by virtue of the fact that the node has not been configured to match IP-Protocol=UDP for RAO packets at all, or that even if UDP traffic is intercepted the port numbers do not match anything locally configured.

2. The "closer examination" of the packet identifies it as UDP, and delivers it to the UDP stack on the node. In this case, it can no longer be guaranteed to be processed appropriately. Most likely it will simply be dropped or rejected with an ICMP error (because there is no GIST process on the destination port to

deliver it to).

Analysis of open-source operating system source code shows the first type of behaviour, and this has also been seen in direct GIST experiments with commercial routers, including the case when they process other uses of the RAO (i.e. RSVP). However, it has also been reported that other RAO implementations may exhibit the second type of behaviour. The consequence of this would be that Q-mode packets are blocked in the network and GIST could not be used. Note that although this caused by some subtle details in the RAO processing rules, the end result is the same as if the packet was simply blocked for other reasons (for example, many IPv4 firewalls drop packets with options by default). Because of these issues, even where a GIST extension is defined for using RAO for Q-mode, it will be necessary to handle cases where signalling paths encounter nodes which block Q-mode traffic in IPv4. There are essentially two options. Which of these options to use would be a matter of implementation and configuration choice.

- A GIST node can be configured to fall back to the base Q-mode encapsulation, sending packets without the RAO at all. This should avoid the above problems, but should only be done if it is known that nodes on the path to the receiver are able to intercept such packets.

- If a GIST node can identify exactly where the packets are being blocked (e.g. from ICMP messages), or can discover some point on the path beyond the blockage (e.g. by use of traceroute or by routing table analysis), it can send the Q-mode messages to that point using IP-in-IP tunelling without any RAO. This bypasses the input side processing on the blocking node, but picks up normal GIST behaviour beyond it.

If in the light of deployment experience the problem of blocked Q-mode traffic turns out to be widespread and these techniques turn out to be insufficient, a further possibility is to define another alternative Q-mode encapsulation which does not use UDP. This would require another specification extension. Such an option would be restricted to network-internal use, since operation through NATs and firewalls would be much harder with it.

The situation with IPv6 is rather different, since in that case the use of non-zero RAO values is well established in the specification and an IANA registry exists. The main problem is that several implementations are still immature: for example, some treat any RAO-marked packet as though it was for local processing without further analysis. Since this prevents any RAO usage at all (including the existing standardised ones) in such a network, it seems reasonable to

assume that such implementations will be fixed as part of the general deployment of IPv6. Concerns about router load as discussed in [I-D.rahman-rtg-router-alert-dangerous] continue to apply.

5. RAO Usage for GIST

5.1. Packet Transmission

For the MRMs defined in [I-D.ietf-nsis-ntlp], this extension requires that a Router Alert Option be included in all Q-mode packets, as part of the IP header. The RAO requirements are the same for IPv4 and IPv6. The value in the RAO is derived from the interception class (see Section 6 below).

Implementations MUST provide a global option to enable or disable the use of RAO, and RAO use MUST be disabled by default. RAO use SHOULD be enabled in network environments where the use of RAO is considered safe and where Q-mode packets are not liable to be blocked by legacy equipment. Implementations MAY provide more fine-grained control, e.g. to enable/disable RAO use on Q-mode packets on a per-destination prefix basis, or if peer discovery fails.

5.2. Packet Reception

A node implementing this extension MUST use RAO inspection to make the initial interception decision, and MUST transparently forward IP packets containing unknown RAO values or RAO values not related to interception classes of locally hosted NSLPs. A node MUST also implement interception logic based based purely on IP-Protocol number and transport header analysis. A node SHOULD provide a per-interface option to enable/disable interception based on protocol number and transport header analysis, and if provided, this option MUST be enabled by default. The option SHOULD be disabled in network environments where it is known that other GIST nodes are using RAO on Q-mode packets.

6. IANA Considerations

Several different RAO values may be used by the NSIS protocol suite. This GIST extension itself does not allocate any RAO values (for either IPv4 or IPv6); an assignment is required for each NSLP interception class (see section 5.3.2 of [I-D.ietf-nsis-ntlp]). The assignment rationale for interception classes discussed in a separate document [I-D.nsis-ext].

The effect of this experimental extension for GIST is that IANA must

allocate an RAO value for each existing NSIS interception class. If interception classes are to be allocated by IANA (see [I-D.nsis-ext]), the IANA procedures must be extended so an RAO value is allocated whenever a new interception class is created.

For all assignments associated with NSIS, the RAO specific processing is the same and is as defined by this specification.

7. Security Considerations

A separate document has been prepared [I-D.rahman-rtg-router-alert-dangerous] with extensive discussion of security considerations on the general use of the RAO. There are no additional considerations raised by this specification.

8. Acknowledgements

With thanks to all the participants in NSIS activities. [I-D.ietf-nsis-ntlp] contains a fairly complete list.

9. Normative References

[I-D.ietf-nsis-ntlp]
Schulzrinne, H. and R. Hancock, "GIST: General Internet Signalling Transport", draft-ietf-nsis-ntlp-17 (work in progress), October 2008.

[I-D.nsis-ext]
Manner, J., Bless, R., Loughney, J., and E. Davies, "Using and Extending the NSIS Protocol Family", draft-nsis-ext-02 (work in progress), November 2008.

[I-D.rahman-rtg-router-alert-dangerous]
Rahman, R. and D. Ward, "Use of IP Router Alert Considered Dangerous", draft-rahman-rtg-router-alert-dangerous-00 (work in progress), October 2008.

[RFC2113] Katz, D., "IP Router Alert Option", RFC 2113, February 1997.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2711] Partridge, C. and A. Jackson, "IPv6 Router Alert Option", RFC 2711, October 1999.

[RFC5350] Manner, J. and A. McDonald, "IANA Considerations for the IPv4 and IPv6 Router Alert Options", RFC 5350, September 2008.

Author's Address

Robert Hancock
Roke Manor Research
Old Salisbury Lane
Romsy, Hampshire SO51 0ZN
UK

Email: robert.hancock@roke.co.uk

Full Copyright Statement

Intellectual Property