

HIP Working Group
Internet-Draft
Intended status: Experimental
Expires: September 9, 2010

G. Camarillo
A. Keranen
Ericsson
March 8, 2010

Host Identity Protocol (HIP) Multi-hop Routing Extension
draft-ietf-hip-via-01.txt

Abstract

This document specifies two extensions to HIP to implement multi-hop routing. The first extension allows implementing source routing in HIP. That is, a host sending a HIP packet can define a set of hosts that the HIP packet should traverse. The second extension allows a HIP packet to carry and record the list of hosts that forwarded it.

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

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 September 9, 2010.

Copyright Notice

Copyright (c) 2010 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 (<http://trustee.ietf.org/license-info>) in effect on the date of

publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the BSD License.

Table of Contents

1.	Introduction	3
2.	Terminology	3
2.1.	Requirements Language	3
2.2.	Definitions	3
3.	Protocol Definitions	4
3.1.	Creating and Processing Via Lists	4
3.2.	Creating Destination Lists	4
3.3.	Processing Destination Lists	5
4.	Packet Formats	5
4.1.	Source and Destination Route List Parameters	6
5.	IANA Considerations	7
6.	Security Considerations	7
7.	Acknowledgments	8
8.	References	8
8.1.	Normative References	8
8.2.	Informative References	8
	Authors' Addresses	8

1. Introduction

When HIP [[RFC5201](#)] is used in certain contexts, hosts need the ability to perform source routing. That is, a host needs the ability to send a HIP packet that will traverse a set of hosts before reaching its destination. Such features are needed, e.g., in HIP BONE [[I-D.ietf-hip-bone](#)] overlay networks or if two hosts wish to keep a third, or more, HIP hosts on the signaling path. This document defines an extension that provides HIP with this functionality.

Additionally, when HIP packets are routed through multiple hosts, some of these hosts (e.g., the destination host) need the ability to know the hosts a particular packet traversed. This document defines another extension that provides HIP with this functionality.

These two extensions enable multi-hop routing in HIP. Before these extensions were specified, there were standardized ways for supporting only a single intermediate host (e.g., a rendezvous server [[RFC5204](#)]) between the source of a HIP packet and its destination.

2. Terminology

2.1. 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](#)].

2.2. Definitions

The following terms used in this document are similar to those defined by RELOAD [[I-D.ietf-p2psip-base](#)] but used here in context of HIP.

Destination list: A list of HITs of the hosts that a HIP packet should traverse.

Via list: A list of HITs of the hosts that a HIP packet has traversed.

Symmetric routing: A response to a message is routed back using the same set of intermediary nodes as the original message used, except in reversed order. Also known as symmetric recursive routing.

3. Protocol Definitions

The multi-hop routing extensions may be used in different contexts and whether a new HIP packet should, for example, include a Via list or have different options enabled, can depend on the particular use case, local policies, and different protocols using the extension. This section defines how the new parameters are handled, but when to use these extensions is out of scope for this document.

3.1. Creating and Processing Via Lists

When a host sending a HIP packet needs to record the hosts that are on the path that the HIP packet traverses, it includes an empty ROUTE_VIA parameter to the packet.

A host that receives a packet with a ROUTE_VIA parameter SHOULD add its own HIT to the end of the ROUTE_VIA parameter, unless it is the receiver of the packet. If the host uses a different HIT on the HIP association it used for receiving the packet than for sending it forward, it SHOULD also add the receiving HIT to the route list before the sending HIT.

If the host is the receiver of the packet, and the received packet generates a response HIP packet, the host checks the SYMMETRIC flag from the ROUTE_VIA parameter. If the SYMMETRIC flag is set, the host MUST create a ROUTE_DST parameter from the ROUTE_VIA parameter, as described in [Section 3.2](#), and include it in the response packet. Also, if an intermediary host generates a new HIP packet (e.g., an error NOTIFY packet) due to a HIP packet that had a ROUTE_VIA parameter with SYMMETRIC flag set, and the new packet is intended for the sender of the original HIP packet, the host SHOULD construct and add a ROUTE_DST parameter into the new packet as in the previous case.

3.2. Creating Destination Lists

A host that needs to define the other hosts that should be on the path a HIP packet traverses adds a ROUTE_DST parameter to the HIP packet. The host may either decide the path independently, or it may create the path based on a ROUTE_VIA parameter. Only the originator of a signed HIP packet can add a ROUTE_DST parameter to the HIP packet since the parameter is covered by the signature.

When a host creates a ROUTE_DST parameter due to receiving a packet with a ROUTE_VIA parameter, it copies all the HITs in the ROUTE_VIA parameter to the ROUTE_DST parameter, but in reversed order. This results in HIP response packet being forwarded using the same set of hosts as the packet for which the response was generated for.

3.3. Processing Destination Lists

When a host receives a HIP packet that contains a ROUTE_DST parameter, it first looks up its own HIT from the route list. If host's own HIT is not in the list and the host is not the receiver of the packet, the packet was incorrectly forwarded and MUST be dropped. If the host's HIT is in the list more than once, the list is invalid and the packet MUST be dropped to avoid forwarding loops. Next hop for the packet is the HIT after host's own HIT in the list. If the host's HIT was the last HIT in the list, the next hop is the receiver's HIT in the HIP header.

If the MUST_FOLLOW flag in the ROUTE_DST parameter is not set, the host SHOULD check whether it has a valid locator for one of the hosts later in the list, or for the receiver of the packet, and it MAY select such a host as the next hop. If the MUST_FOLLOW flag is set, the host MUST NOT skip any hosts in the list.

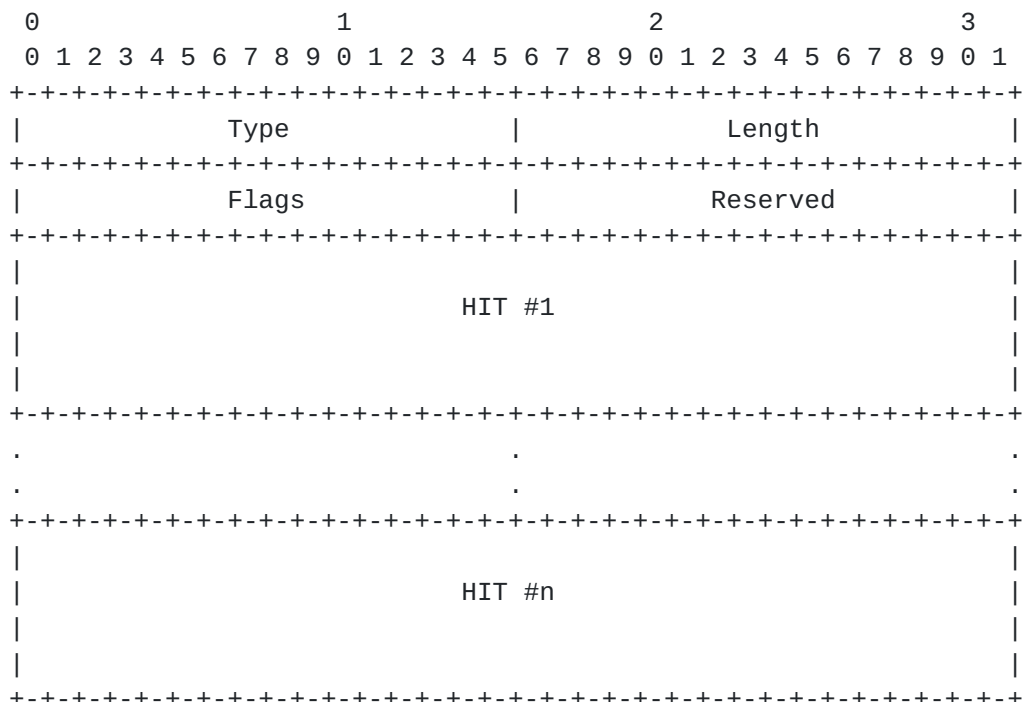
If the host has a valid locator for the next hop, it MUST forward the HIP packet to the next hop host. If the host can not determine a valid locator for the next hop host, it SHOULD drop the packet and SHOULD send back a NOTIFY error packet with type UNKNOWN_NEXT_HOP (value [TBD by IANA; 90]). The Notification Data field for the error notifications SHOULD contain the HIP header of the rejected packet and the ROUTE_DST parameter.

4. Packet Formats

This memo defines two new HIP parameters that are used for recording a route via multiple hosts (ROUTE_VIA) and for defining a route a packet should traverse by the sender of the packet (ROUTE_DST).

The ROUTE_DST parameter is integrity protected with the signature (where present) but ROUTE_VIA is not so that intermediary hosts can add their own HITs to the list. Both parameters have critical type (as defined in [Section 5.2.1 of \[RFC5201\]](#)) since the packet will not be properly routed unless all hosts on path recognize the parameters.

4.1. Source and Destination Route List Parameters



Type	[TBD by IANA ROUTE_DST: 971 ROUTE_VIA: 65525]
Length	length in octets, excluding Type and Length (i.e., number-of-HITs * 16 + 4)
Flags	bit flags that can be used for requesting special handling of the parameter
Reserved	reserved for future use
HIT	Host Identity Tag of one of the hosts on the path

Figure 1: Format of the ROUTE_VIA and ROUTE_DST Parameters

Figure 1 shows the format of both ROUTE_VIA and ROUTE_DST parameters. The ROUTE_DST parameter, if present, MUST have at least one HIT, but the ROUTE_VIA parameter can also have zero HITs. Both can contain at most 32 HITs. The Flags field is used for requesting special handling for via and destination lists. The flags defined in this document are shown in Table 1. The Reserved field can be used by future extensions; it MUST be zero when sending and ignored when receiving this parameter.

Pos	Name	Purpose
0	SYMMETRIC	The response packet MUST be sent with a ROUTE_DST list made from the ROUTE_VIA list containing this flag, i.e., using symmetric routing.
1	MUST_FOLLOW	All the hosts in a ROUTE_DST list MUST be traversed, i.e., even if a host would have a valid locator for a host beyond the next hop, it MUST NOT forward the packet there but to the next hop host.

Table 1: Bit Flags in ROUTE_VIA and ROUTE_DST Parameters

The "Pos" column in Table 1 shows the bit position of the flag (as in Figure 1) in the Flags field, "Name" gives the name of the flag used in this document, and "Purpose" gives brief description of the meaning of that flag.

The flags apply to both ROUTE_VIA and ROUTE_DST parameters and when a ROUTE_DST parameter is added to a packet because of a ROUTE_VIA parameter, the same flags MUST be copied to the ROUTE_DST parameter.

5. IANA Considerations

This section is to be interpreted according to [\[RFC5226\]](#).

This document updates the IANA Registry for HIP Parameter Types [\[RFC5201\]](#) by assigning new HIP Parameter Type values for the new HIP Parameters: ROUTE_VIA and ROUTE_DST (defined in [Section 4](#)). This document also defines a new Notify Packet Type [\[RFC5201\]](#) UNKNOWN_NEXT_HOP in [Section 3.3](#).

6. Security Considerations

A malicious host could craft a destination route list that contains the same HIT more than once and thus create a forwarding loop. The check described in [Section 3.3](#) should break such loops but hosts MAY in addition utilize the OVERLAY_TTL [\[I-D.ietf-hip-bone\]](#) parameter for additional protection against forwarding loops.

7. Acknowledgments

Tom Henderson provided valuable comments and improvement suggestions for this document.

8. References

8.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [RFC5201] Moskowitz, R., Nikander, P., Jokela, P., and T. Henderson, "Host Identity Protocol", [RFC 5201](#), April 2008.

8.2. Informative References

- [RFC5204] Laganier, J. and L. Eggert, "Host Identity Protocol (HIP) Rendezvous Extension", [RFC 5204](#), April 2008.
- [RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", [BCP 26](#), [RFC 5226](#), May 2008.
- [I-D.ietf-hip-bone] Camarillo, G., Nikander, P., Hautakorpi, J., Keranen, A., and A. Johnston, "HIP BONE: Host Identity Protocol (HIP) Based Overlay Networking Environment", [draft-ietf-hip-bone-04](#) (work in progress), January 2010.
- [I-D.ietf-p2psip-base] Jennings, C., Lowekamp, B., Rescorla, E., Baset, S., and H. Schulzrinne, "REsource LOcation And Discovery (RELOAD) Base Protocol", [draft-ietf-p2psip-base-07](#) (work in progress), February 2010.

Authors' Addresses

Gonzalo Camarillo
Ericsson
Hirsalantie 11
02420 Jorvas
Finland

Email: Gonzalo.Camarillo@ericsson.com

Ari Keranen
Ericsson
Hirsalantie 11
02420 Jorvas
Finland

Email: Ari.Keranen@ericsson.com