

HIP Working Group
Internet-Draft
Intended status: Experimental
Expires: April 29, 2010

G. Camarillo
A. Keranen
Ericsson
October 26, 2009

Host Identity Protocol (HIP) Multi-hop Routing Extension
draft-ietf-hip-via-00.txt

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/lid-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 April 29, 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

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.

Table of Contents

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

1. Introduction

When HIP [[RFC5201](#)] is used in certain contexts (e.g., in a HIP BONE [[I-D.ietf-hip-bone](#)] overlay), 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. 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, HIP only supported a single intermediate host (i.e., 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

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.

[3.](#) Protocol Definitions

[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 SHOULD 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

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.

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](#)).

6. Security Considerations

6.1. Forwarding Loops

A malicious host could craft a destination route list that contains the same HIT more than once and thus create a forwarding loop. Since the IP layer TTL is decremented on each hop, the loop will be eventually broken, but hosts may additionally protect themselves against this attack by checking that their own HIT is in the destination list only once and drop invalid packets.

7. References

7.1. 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.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", [BCP 26](#), [RFC 5226](#), May 2008.

[7.2.](#) Informative References

[RFC5204] Laganier, J. and L. Eggert, "Host Identity Protocol (HIP) Rendezvous Extension", [RFC 5204](#), April 2008.

[I-D.ietf-hip-bone]
Camarillo, G., Nikander, P., Hautakorpi, J., and A. Johnston, "HIP BONE: Host Identity Protocol (HIP) Based Overlay Networking Environment", [draft-ietf-hip-bone-02](#) (work in progress), July 2009.

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