

HIP Working Group  
Internet-Draft  
Intended status: Experimental  
Expires: April 30, 2012

A. Keranen  
G. Camarillo  
J. Maenpaa  
Ericsson  
October 28, 2011

**Host Identity Protocol-Based Overlay Networking Environment (HIP BONE)  
Instance Specification for REsource LOcation And Discovery (RELOAD)  
draft-ietf-hip-reload-instance-04.txt**

**Abstract**

This document is the Host Identity Protocol-Based Overlay Networking Environment (HIP BONE) instance specification for the REsource LOcation And Discovery (RELOAD) protocol. The document provides the details needed to build a RELOAD-based overlay that uses HIP.

**Status of this Memo**

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

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

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."

This Internet-Draft will expire on April 30, 2012.

**Copyright Notice**

Copyright (c) 2011 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 Simplified BSD License.

## Table of Contents

<a href="#">1.</a>	Introduction . . . . .	<a href="#">3</a>
<a href="#">2.</a>	Terminology . . . . .	<a href="#">3</a>
<a href="#">3.</a>	Peer Protocol . . . . .	<a href="#">3</a>
<a href="#">4.</a>	Node ID Generation . . . . .	<a href="#">3</a>
<a href="#">5.</a>	Mapping between Protocol Primitives and HIP Messages . . . . .	<a href="#">4</a>
<a href="#">5.1.</a>	Forwarding Header . . . . .	<a href="#">4</a>
<a href="#">5.2.</a>	Security Block . . . . .	<a href="#">5</a>
<a href="#">5.3.</a>	Replaced RELOAD Messages . . . . .	<a href="#">5</a>
<a href="#">6.</a>	Securing Communication . . . . .	<a href="#">5</a>
<a href="#">7.</a>	Routing HIP Messages via the Overlay . . . . .	<a href="#">6</a>
<a href="#">8.</a>	Enrollment and Bootstrapping . . . . .	<a href="#">7</a>
<a href="#">9.</a>	NAT Traversal . . . . .	<a href="#">7</a>
<a href="#">10.</a>	RELOAD Overlay Configuration Document Extension . . . . .	<a href="#">7</a>
<a href="#">11.</a>	Security Considerations . . . . .	<a href="#">8</a>
<a href="#">12.</a>	IANA Considerations . . . . .	<a href="#">8</a>
<a href="#">13.</a>	Acknowledgements . . . . .	<a href="#">9</a>
<a href="#">14.</a>	References . . . . .	<a href="#">9</a>
<a href="#">14.1.</a>	Normative References . . . . .	<a href="#">9</a>
<a href="#">14.2.</a>	Informational References . . . . .	<a href="#">10</a>
	Authors' Addresses . . . . .	<a href="#">10</a>



## **1. Introduction**

The HIP BONE (Host Identify Protocol-Based Overlay Networking Environment) specification [[RFC6079](#)] provides a high-level framework for building HIP-based [[RFC5201](#)] overlays. The HIP BONE framework leaves the specification of the details on how to combine a particular peer protocol with HIP to build an overlay up to documents referred to as HIP BONE instance specifications. As discussed in [[RFC6079](#)], a HIP BONE instance specification needs to define, minimally:

- o the peer protocol to be used.
- o what kind of Node IDs are used and how they are derived.
- o which peer protocol primitives trigger HIP messages.
- o how the overlay identifier is generated.

This document addresses all the previous items and provides additional details needed to built RELOAD-based HIP BONES. The details on how different RELOAD modules would be integrated to a HIP implementation and what kind of APIs are used between them are left as implementation details or to be defined by other documents.

## **2. Terminology**

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](#)]. In addition, this document uses the terms defined in [[RFC5201](#)], [[RFC6079](#)], [[RFC6028](#)], and [[I-D.ietf-p2psip-base](#)].

## **3. Peer Protocol**

The peer protocol to be used is RELOAD, which is specified in [[I-D.ietf-p2psip-base](#)]. When used with RELOAD, HIP replaces the RELOAD's Forwarding and Link Management Layer (described in [Section 5.5.](#) of [[I-D.ietf-p2psip-base](#)]).

## **4. Node ID Generation**

This document specifies two modes for generating Node IDs. Which mode is used in an actual overlay is defined by the overlay configuration.

RELOAD uses 128-bit Node IDs. Since HIP uses 128-bit ORCHIDs [[RFC4843](#)], a peer's ORCHID can be used as such as a RELOAD Node ID



(the "ORCHID" mode). In this mode, also all the RELOAD Resource IDs are prefixed with the ORCHID prefix and the lower 100 bits of the IDs, as defined by RELOAD usage documents, are used after the prefix.

In the other Node ID mode, namely "RELOAD", all 128 bits are generated as defined in [[I-D.ietf-p2psip-base](#)] resulting in a larger usable address space.

## 5. Mapping between Protocol Primitives and HIP Messages

RELOAD HIP BONE replaces the RELOAD protocol primitives taking care of connection establishment with the HIP base exchange, whereas the rest of the RELOAD messages are conveyed within HIP messages. The Forwarding and Link Management Layer functionality of RELOAD defined in Section 5.5. of [[I-D.ietf-p2psip-base](#)], including all the NAT traversal functionality, is replaced by HIP and the extensions defined in this document.

The standard RELOAD messages consist of three parts: Forwarding Header, Message Contents and the Security Block. When RELOAD messages are sent in a RELOAD HIP BONE overlay, the RELOAD Message Contents are used as such within HIP DATA [[RFC6078](#)] messages, but the functionality of the Forwarding Header and Security Block are replaced with HIP header, HIP Destination and Via lists [[RFC6028](#)], and CERT [[RFC6253](#)], TRANSACTION\_ID [[RFC6078](#)], OVERLAY\_ID and OVERLAY\_TTL [[RFC6079](#)] parameters.

### 5.1. Forwarding Header

The RELOAD Forwarding Header is used for forwarding messages between peers and to their final destination. The Forwarding Header's overlay field's value MUST be used as such in an OVERLAY\_ID parameter and the transaction\_id field in a TRANSACTION\_ID parameter. That is, all RELOAD HIP BONE messages MUST contain these parameters and the length of the OVERLAY\_ID parameter's identifier field is 4 and the length of the TRANSACTION\_ID's identifier 8 octets. HIP Destination and Via lists are used for the same purpose as the destination\_list and via\_list in the Forwarding Header, with the exception that all Resource IDs MUST be of the same length as Node IDs and compressed IDs MUST NOT be used. The TTL value in the OVERLAY\_TTL parameter is used like the ttl field in the Forwarding Header.

The functionality of the fragment and length fields are provided by the HIP headers. The relo\_token, version, and max\_res\_len are not needed with HIP and options field, if needed eventually for some extensions, can be replaced with additional HIP parameters.



## 5.2. Security Block

The RELOAD Security Block contains certificates and digital signatures of the message. All the HIP DATA messages are digitally signed by the originator of the message and contain the HOST\_ID parameter with the identifier that can be used for verifying the signature. Certificates are delivered in a HIP CERT parameter as defined in [\[RFC6253\]](#) or stored to the overlay using the RELOAD Certificate Storage Usage.

Note that when the RELOAD mode for Node ID generation is used, the certificate certifying that a host is allowed to use a certain Node ID MUST contain host's Node ID instead of HIT in the "Subject Alternative Name" of the certificate as described in Section 10.3 of [\[I-D.ietf-p2psip-base\]](#) while the "Subject" field contains the HIT calculated from the Host Identity.

## 5.3. Replaced RELOAD Messages

The Attach procedure in RELOAD establishes a connection between two peers. This procedure is performed using the AttachReq and AttachAns messages. When HIP is used, the Attach procedure is performed by using a HIP base exchange. That is, peers send HIP I1 messages instead of RELOAD AttachReq messages. This behavior replaces the one described in Section 5.5. of [\[I-D.ietf-p2psip-base\]](#).

The AppAttach procedure in RELOAD is used for creating a connection for other applications than RELOAD. Also the AppAttach procedure is replaced with HIP base exchange and after the base exchange peers can exchange any application layer data using the normal transport layer ports over the NAT traversing IPsec connection.

This specification does not support flooding of configuration files, so Config\_Update requests and responses (Section 5.5.6. of [\[I-D.ietf-p2psip-base\]](#)) MUST NOT be sent in the overlay. RELOAD Ping messages (Section 5.5.5 of [\[I-D.ietf-p2psip-base\]](#)) MAY be used.

For all other RELOAD messages the Message Contents are used as such within HIP DATA messages.

## 6. Securing Communication

RELOAD uses TLS [\[RFC5246\]](#) connections for securing the hop-by-hop messaging and certificates and signatures for providing integrity protection for the overlay messages and for the data stored in the overlay.





With a RELOAD HIP BONE, instead of using TLS connections as defined in [[I-D.ietf-p2psip-base](#)], all HIP overlay messages SHOULD be either sent using encrypted connections (such as IPsec ESP tunnel between two peers [[RFC6261](#)]) or the contents of the messages SHOULD be in an ENCRYPTED parameter (see [Section 5.2.15 of \[RFC5201\]](#)). Use of encrypted connections is RECOMMENDED since that provides confidentiality also for the HIP headers.

The data objects stored in the RELOAD HIP BONE overlay are signed and the signatures are stored as defined in [[I-D.ietf-p2psip-base](#)] with the exception that SignerIdentity is carried in the HIP DATA message's HOST\_ID parameter instead of using the RELOAD SecurityBlock. If certificates are needed, they are sent using the CERT parameter.

## **7. Routing HIP Messages via the Overlay**

If a host has no valid locator for the receiver of a new HIP packet, and the receiver is part of a RELOAD HIP BONE overlay the host is participating in, the host can send the HIP packet to the receiver using the overlay routing.

When sending a HIP packet via the overlay, the host MUST add an empty ROUTE\_VIA parameter [[RFC6028](#)] to the packet with the SYMMETRIC and MUST\_FOLLOW flags set and an OVERLAY\_ID parameter containing the identifier of the right overlay network. The host consults the RELOAD Topology Plugin for the next hop and sends the HIP packet to that host.

An intermediate host receiving a HIP packet with the OVERLAY\_ID parameter checks if it is participating in that overlay, and SHOULD drop packets sent to unknown overlays. If the host is not the final destination of the packet (i.e., the HIP header's receiver's HIT does not match to any of its HITs), it checks if the packet contains a ROUTE\_DST parameter. Such packets are forwarded to the next hop as specified in [[RFC6028](#)]. If the packet does not contain a ROUTE\_DST parameter, the host finds the next hop from the RELOAD Topology Plugin and forwards the packet there. As specified in [[RFC6028](#)], the host adds the HIT it uses on the HIP association with the next hop host to the end of the ROUTE\_VIA parameter, if present.

When the final destination host receives the HIP packet, the host processes it as specified in [[RFC5201](#)] and in case of HIP DATA packet, the contents are processed as specified in [[I-D.ietf-p2psip-base](#)]. If the HIP packet generates a response, the response is routed back on the same path using the ROUTE\_DST parameter as specified in [[RFC6028](#)].



## **8. Enrollment and Bootstrapping**

The RELOAD HIP BONE instance uses the enrollment and bootstrap procedure defined by RELOAD [[I-D.ietf-p2psip-base](#)] with the exceptions listed below.

- o In RELOAD, a node wishing to enroll in an overlay starts with obtaining a configuration document as explained in [[I-D.ietf-p2psip-base](#)]. This specification extends the RELOAD overlay configuration document as defined in [Section 10](#).
- o The X.509 certificates used by the RELOAD HIP BONE instance are similar to those of RELOAD except that they contain HITs instead of RELOAD URIs. The HITs are included in the SubjectAltName field of the certificate as described in [[RFC6253](#)].
- o When contacting a bootstrap node, instead of forming a DTLS or TLS connection, the host MUST perform a HIP base exchange with the bootstrap node. The base exchange MAY be performed using a HIP rendezvous or relay server.

## **9. NAT Traversal**

RELOAD relies on the Forwarding and Link Management Layer providing NAT traversal capabilities. Thus, the RELOAD HIP BONE instance implementations MUST implement some reliable NAT traversal mechanism. To maximize interoperability, all implementations SHOULD implement at least [[RFC5770](#)].

HIP relay servers are not necessarily needed with this HIP BONE instance since the overlay network can be used for relaying the Base Exchange and further HIP signaling can be done directly between the peers. However, if it is possible that a bootstrap peer is behind a NAT, it MUST register with a HIP relay so that there is a reliable way to connect to it.

## **10. RELOAD Overlay Configuration Document Extension**

This document modifies the bootstrap-node element of the RELOAD overlay configuration document. The modified bootstrap-node element contains the following attributes:

address: The locator of the bootstrap node.  
port: The HIP port of the bootstrap node.



hit: The HIT of the bootstrap node.

If the bootstrap-node element does not contain a HIT, opportunistic mode SHOULD be used for contacting the bootstrap node. If the element does not contain a port number, the bootstrap node SHOULD be contacted by starting the base exchange as defined in [\[RFC5201\]](#). Otherwise, the base exchange MUST be started UDP-encapsulated as defined in [\[RFC5770\]](#) using the given port as the destination port number.

A RELOAD HIP BONE overlay MUST use Overlay Link Protocol type "HIP" in the configuration document's overlay-link-protocol element. The enrolling node MUST check the overlay-link-protocol element and proceed with procedures defined in this document only if "HIP" link type is found.

This document also adds a new element inside the configuration element that defines which mode (see [Section 4](#)) is used for generating the Node and Resource IDs. The name of the element is "hipbone-id-mode" and the content is the identifier of the mode: "ORCHID" for the ORCHID prefixed IDs and "RELOAD" for the IDs that use the whole 128 bits as defined by the RELOAD specification.

## **[11.](#) Security Considerations**

The security considerations of RELOAD (Section 12 of [\[I-D.ietf-p2psip-base\]](#)), with the exception of TLS specific features, apply also to RELOAD HIP BONE instances.

The option to send overlay messages unencrypted makes it possible for hosts that are not part of the overlay to inspect the contents of the messages and thus should be avoided when possible. If the ENCRYPTED parameter is used instead of encrypted connections, the HIP header remains visible but the contents are protected.

Limiting the Node ID and Resource ID space into 128 bits (or 100 bits with ORCHID prefixes) results in a higher probability for ID collisions, both unintentional and intentional, than using larger address spaces.

## **[12.](#) IANA Considerations**

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

IANA is requested to update the "Overlay Link Protocol" registry [\[I-D.ietf-p2psip-base\]](#) by assigning new Overlay Link Protocol type



"HIP" (see [Section 10](#)).

### **13. Acknowledgements**

Tom Henderson provided valuable comments on the draft.

### **14. References**

#### **14.1. Normative References**

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [RFC4843] Nikander, P., Laganier, J., and F. Dupont, "An IPv6 Prefix for Overlay Routable Cryptographic Hash Identifiers (ORCHID)", [RFC 4843](#), April 2007.
- [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.
- [RFC6079] Camarillo, G., Nikander, P., Hautakorpi, J., Keranen, A., and A. Johnston, "HIP BONE: Host Identity Protocol (HIP) Based Overlay Networking Environment (BONE)", [RFC 6079](#), January 2011.
- [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-18](#) (work in progress), August 2011.
- [RFC5770] Komu, M., Henderson, T., Tschofenig, H., Melen, J., and A. Keranen, "Basic Host Identity Protocol (HIP) Extensions for Traversal of Network Address Translators", [RFC 5770](#), April 2010.
- [RFC6028] Camarillo, G. and A. Keranen, "Host Identity Protocol (HIP) Multi-Hop Routing Extension", [RFC 6028](#), October 2010.
- [RFC6078] Camarillo, G. and J. Melen, "Host Identity Protocol (HIP) Immediate Carriage and Conveyance of Upper-Layer Protocol





Signaling (HICCUPS)", [RFC 6078](#), January 2011.

[RFC6253] Heer, T. and S. Varjonen, "Host Identity Protocol Certificates", [RFC 6253](#), May 2011.

[RFC6261] Keranen, A., "Encrypted Signaling Transport Modes for the Host Identity Protocol", [RFC 6261](#), May 2011.

#### **[14.2.](#) Informational References**

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", [RFC 5246](#), August 2008.

#### Authors' Addresses

Ari Keranen  
Ericsson  
Hirsalantie 11  
02420 Jorvas  
Finland

Email: Ari.Keranen@ericsson.com

Gonzalo Camarillo  
Ericsson  
Hirsalantie 11  
Jorvas 02420  
Finland

Email: Gonzalo.Camarillo@ericsson.com

Jouni Maenpaa  
Ericsson  
Hirsalantie 11  
Jorvas 02420  
Finland

Email: Jouni.Maenpaa@ericsson.com

