

Internet Draft  
October 19, 2006  
Expires April 2007

D. Thaler  
Microsoft

A Comparison of IP Mobility-Related Protocols  
<[draft-thaler-mobility-comparison-02.txt](#)>

## Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with [Section 6 of 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/lid-abstracts.html>

The list of Internet-Draft Shadow Directories can be accessed at  
<http://www.ietf.org/shadow.html>.

## Copyright Notice

Copyright (C) The Internet Society (2006). All Rights Reserved.

## Abstract

Mobile IPv6 (MIPv6), the Level 3 Multihoming Shim Protocol (SHIM6), and the Host Identity Protocol (HIP) all address various aspects of mobility and multi-homing in similar ways. This document gives a brief comparison of their features.

## 1. Introduction

This document describes a number of commonalities and differences between Mobile IPv6 [[MIPv6](#)], the Level 3 Multihoming Shim Protocol [[SHIM6](#)], and the Host Identity Protocol [[HIP](#)]. Each of them addresses different aspects of the overall mobility and multi-homing problems. The set of features compared herein was constructed based on taking the union of the problem statements for each protocol. As we will see, significant overlap exists, but each has unique aspects

that the others do not address.

Thaler  
Draft

Expires April 2007  
IP Mobility Comparison

1  
October 2006

This comparison shows a snapshot in time, and there may be additional work not mentioned here which adds capabilities to one or more of the protocols discussed herein. Only work currently within the IETF has been considered in the tables below. Finally, only IPv6 is considered within this document, although some protocols may work for IPv4 as well.

In this document, three types of identifiers are referred to:

Name: A DNS fully-qualified domain name.

Upper-layer Identifier (ULID): An address used by protocols and applications above the mobility/multi-homing sub-layer. In MIP6, this is a Home Address (HoA). SHIM6 uses normal IPv6 addresses as upper-layer identifiers, and calls them ULIDs when used as such. In HIP, this is a Host Identity Tag (HIT).

Locator: An address used for routing below the mobility/multi-homing sub-layer. In MIP6, this is a Care-of Address. SHIM6 and HIP use normal IPv6 addresses and simply call them Locators.

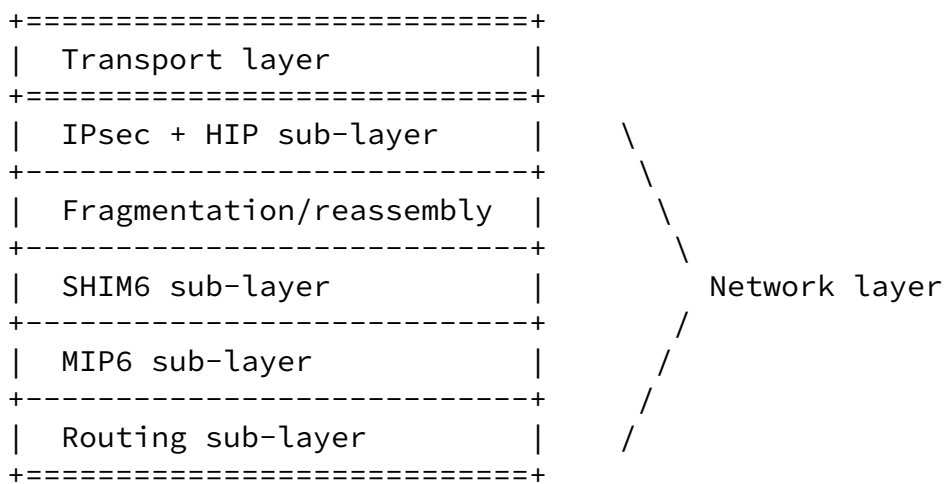
## 2. Layering

MIP6, SHIM6, and HIP all insert a conceptual sub-layer between the routing portion of the network layer, and the transport layer. Each of them does some processing in the data path for specific headers.

MIP6 uses a Destination Options Header with a Home Address Option in data packets sent from a home address, and a Type 2 Routing Header in packets sent to a home address. SHIM6 defines a Payload Extension Header. HIP uses the Encapsulating Security Payload header itself. A theoretical packet with all of the above present, plus other extension headers, would thus look like this:

```
+-----+-----+-----+-----+-----+-----+-----+-----+
| IPv6 | HbH  | Type2 | DstOpts | SHIM6 | Frag | ESP  | Payload
| Hdr  | Opts | RtHdr | (HoA)   | PEH   | Hdr  | (HIP) |
+-----+-----+-----+-----+-----+-----+-----+-----+
```

As can be seen from this, MIP6 headers appear first, followed by SHIM6, followed by HIP. As such, a natural organization in an implementation would be (ignoring other destination options):



### 3. Feature Comparison

The following table summarizes the features compared in this section. Each line has a corresponding section below with a more detailed explanation.

	MIP6	SHIM6	HIP
Preserve established connections	Yes	Yes	Yes
Support both ends moving simultan.	Yes	Only w/in known set	Yes
Span path outages	No	Yes	No
Resolve name to locators immed. after move	Yes	No	Yes

Support referrals	Yes	Yes	Only by name	
Stable addresses	Yes	Assumed	Non-routable	
Support load spreading	Yes (monami6)	Yes	Yes	
Multicast support	Yes	Not mobile	No	

### [3.1.](#) Preserve established connections

All three protocols are able to preserve established connections across a locator change, including by both sides simultaneously.

Thaler  
Draft

Expires August 2006  
IP Mobility Comparison

3  
October 2006

### [3.2.](#) Support both ends moving simultan.

MIP6 and HIP both are able to preserve established connections even if both ends move simultaneously. SHIM6 is only able to do so if at least one end only moves to a new locator which has previously been communicated to the other prior to the move.

### [3.3.](#) Span path outages

A "path outage" here refers to a case where both ends of a connection believe they have network connectivity and their locator is valid, but the path between the locator pair is broken somewhere in the middle of the network.

MIP6 is not able to preserve connections across such outages between the correspondent node and the home address. HIP would be capable of preserving connections across such outages, but has no mechanisms for detecting failures end-to-end and testing alternate paths. SHIM6 was designed for this scenario and is able to preserve connections across such outages.

### [3.4.](#) Resolve name to locators immed. after move

If the TTL in the DNS AAAA records is (say) 30 seconds, or if DNS resolvers do not respect a TTL less than 30 seconds, then normally new connections to a device would not be able to be established for up to 30 seconds after the device moves to a new network location. MIP6 and HIP are both able to accept new connections without waiting for name resolution, since DNS records need not be updated when

moving.

SHIM6 does not attempt to address this problem.

### [3.5.](#) Support referrals

In some applications and protocols, one device redirects another device to a third device. Such a redirection may be by giving it the name or the upper-layer identifier of the third party. Another similar variation occurs when one device wants to connect back to another device which previously connected to it.

MIP6 and SHIM6 both support such referrals by either name or upper-layer identifier.

HIP, on the other hand, currently only supports referrals by name, not upper-layer identifier. This is because there is currently no way to get the locator corresponding to a HIT, without knowing the name. As a result, applications and protocols that use address-based referrals do not work with HIP. The IRTF is currently investigating addressing this problem via a Distributed Hash Table.

Thaler  
Draft

Expires August 2006  
IP Mobility Comparison

4  
October 2006

### [3.6.](#) Stable addresses

Many applications and higher-layer protocols today cache addresses for a significant length of time. Because of this, there is often a desire for stable (i.e., long-lived) upper-layer identifiers. Typically this is desired to be able to accept new connections immediately ([section 3.2](#)) and to support referrals ([section 3.5](#)). It is also useful for management purposes.

MIP6 provides this by providing a stable Home Address. SHIM6 does not attempt to address this problem, nor does it make the problem any worse. HIP provides a stable upper-layer identifier, but it is not a routable address.

### [3.7.](#) Support load spreading

When multiple locators are advertised to another device, that other device can do load spreading of different connections to the first device by using different locators.

SHIM6 supports the ability to advertise multiple locators, whereas MIP6 itself only advertises a single one, but there is work in

progress [[MCOA](#)] on extending MIP6 to advertise multiple locators. HIP also supports the ability to advertise multiple locators, but its ability to use them is not as mature as SHIM6.

### [3.8](#). Multicast support

MIP6 supports sourcing multicast from home addresses by tunneling it through the home agent. In SHIM6, multicast can be sourced from any address, but it does not support moving such sessions with SHIM6. HIP, on the other hand, does not support sourcing multicast from HITs.

## [4](#). Efficiency Considerations

The following table summarizes the efficiency metrics compared in this section. Each line has a corresponding section below with a more detailed explanation.

	MIP6	SHIM6	HIP
Per-packet overhead (bytes)	0 if both home / 20/40 if src away + 24 if dest away	0 normally/ 8 if moved	0 (beyond IPsec transport mode)
Connect overhead (messages)	0	0	0 + 4 for IPsec key negotiation
Locator change overhead (messages)	2 to update HA + 6 / 4 (cga) / 0 if local (hmip6)	4 to update peer	3 to update RVS + 3 to update peer

	to update peer		
--	----------------	--	--

#### 4.1. Per-packet overhead (bytes)

MIP6 uses a Destination Options Header with a Home Address Option (20 bytes) in data packets sent from a home address. If packets are reverse tunneled to a home agent, then there is instead an overhead of at least 40 bytes (the size of an IPv6 Header), plus any other extension headers used by the tunnel, if any, on packets between the mobile node and the home agent

MIP6 uses a Type 2 Routing Header (24 bytes) in packets sent to a home address. When both ends use home addresses, the overhead is thus 44 bytes (or if reverse tunneling is used instead, 64 bytes between the mobile node and the home agent).

If a packet is fragmented, the above overhead is added to every fragment.

SHIM6 uses an 8-byte Payload Extension Header with data packets. If a packet is fragment, this overhead is added to every fragment. This overhead is only present after a locator change occurs.

HIP uses the IP Encapsulating Security Payload (ESP) within data packets. As such, the overhead is equal to the size of the ESP header, or 0 if IPsec transport mode would be used anyway. Furthermore, its processing is per reassembled packet, not per fragment.

#### 4.2. Connect overhead

At the time data is first exchanged between a mobile node and a correspondent node (e.g., a TCP connect), MIP6 generates no additional messages prior to a switch to use route optimization. At the time a mobile node is away from home and decides to use route optimization, it generates 6 additional messages (Binding Update,

Thaler  
Draft

Expires August 2006  
IP Mobility Comparison

6  
October 2006

Binding Acknowledgement, Home Test Init, Home Test, Care-of Test Init, and Care-of Test).

SHIM6 assumes the node is always at home and generates no messages prior to a locator change.

In HIP, a node is always "away from home" in the sense that its locator is never equal to the ULID (which is non-routable), and

hence it uses a 4-way handshake to negotiate IPsec state prior to being able to send data. If IPsec would be used anyway, HIP requires no additional messages (although whether this is the same, more, or less overhead than typical IPsec overhead depends on the key management protocol it is compared to).

### [4.3. Locator change overhead](#)

To change a locator for existing communication, MIP6 generates 2 messages to update the Home Agent, and 6 (or 4 if the optimization in [\[CGA\]](#) is used) to update the correspondent node. If the mobile node is communicating with multiple correspondent nodes, the 2 to update the Home Agent only applies once, not per correspondent node. Hierarchical Mobile IPv6 [\[HMIP6\]](#) specifies an optimization which avoids any messages to correspondent nodes in the case where the mobile node moves within the same domain; it does so, however, at the expense of requiring that a Mobility Anchor Point (MAP) is deployed within that domain and routers are configured to advertise it.

SHIM6 generates 4 messages to update the peer. HIP generates 3 messages to update the Rendezvous Server (RVS), and a 3 message handshake to update each peer.

## [5. Deployment Considerations](#)

The following table summarizes the deployment considerations compared in this section. Each line has a corresponding section below with a more detailed explanation.

	MIP6	SHIM6	HIP
One-end benefit	Yes	No	No
Typical deployment dependencies	Home agent, if hmip used: MAP + config routers	None	Rendezvous Svr, New RR, IPsec

### [5.1. One-end benefit](#)

Protocols that allow some partial benefit when only one end of a connection supports the protocol have a deployment advantage over

those that require support from both ends. This is because the



former allows a new device to gain immediate benefit, whereas the latter only gives significant benefit once the majority of devices it talks to are upgraded.

MIP6 provides benefit for a mobile node even without support in correspondent nodes; traffic is simply less efficient since traffic must be routed via the home agent rather than using route optimization.

SHIM6 and HIP both require support in both ends before their benefits can be realized.

## [5.2](#). Typical deployment dependencies

To gain the full benefits of a protocol, often additional deployment dependencies exist on other protocols or servers.

MIP6 depends on the existence of a MIP6 Home Agent to be deployed. As noted in [section 4.3](#), the HMIP6 optimization also requires that a Mobility Anchor Point be deployed within a domain desiring the optimization for local movement, and also that routers in that domain be configured to advertise it.

SHIM6 has no outside dependencies.

HIP depends on the IPsec [[IPSEC](#)] protocol for basic operation. It also depends on the existence of a HIP Rendezvous Server for its mobility mechanisms. Finally, it requires a new DNS resource record, and to gain the full security benefit, it depends on the DNSSec [[DNSSEC](#)] protocol. However, the dependency on DNSSec to secure the name-to-ULID-related information is the same as for the other protocols, which do not attempt to address the key negotiation problem.

## [6](#). Security Considerations

Security considerations for each protocol discussed herein are covered in the respective protocol documents. A brief comparison of their security aspects is listed below.

	MIP6	SHIM6	HIP
Control message auth check			
Minimum	On path	On path + same node	Cryptographic
Maximum	Crypto.	Crypto.	Crypto.
Maximum control msg auth check	Crypto.	Crypto.	Crypto.
Data security	Optional	Optional	Required

### [6.1.](#) Control message auth check

Control messages indicating a locator change must be authenticated. MIP6 and SHIM6 at minimum only verify that control messages were originated by someone on the path between the two ends. MIP6 at a minimum only verifies that control messages were originated by someone on the path between the two ends using a return routability test, but allows optional cryptographic checks (using what is known as Cryptographically Generated Addresses (CGAs) [[CGA](#)]) for more security. SHIM6 also uses a return routability test, plus at least a verification that the new locator is a locator of the same node (but does not verify that the control message was actually sent by that node) using a technique known as Hash-Based Addresses; it also optionally allows CGAs for more security.

HIP, on the other hand, requires strong cryptographic checks on all control messages.

### [6.2.](#) Data security

HIP requires that IPsec [[IPSEC](#)] be used for data, whereas IPsec is optional for MIP6 and SHIM6.

## [7.](#) IANA Considerations

This document has no actions for IANA.

## [8.](#) Acknowledgements

Marcelo Bagnulo, Tom Henderson, Vijay Devarapalli, and Hesham Soliman provided valuable feedback and technical information regarding this draft.

Thaler  
Draft

Expires August 2006  
IP Mobility Comparison

9  
October 2006

## 9. Informative References

- [CGA] Arkko, J., Vogt, C., and W. Haddad, "Applying Cryptographically Generated Addresses and Credit-Based Authorization to Mobile IPv6", Internet Draft, [draft-ietf-mipshop-cga-cba-01.txt](#), September 2006.
- [DNSSEC] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", [RFC 4033](#), March 2005.
- [HIP] Moskowitz, R. and P. Nikander, "Host Identity Protocol (HIP) Architecture", [RFC 4423](#), May 2006.
- [HMIPv6] Soliman, H., Castelluccia, C., El Malki, K., and L. Bellier, "Hierarchical Mobile IPv6 Mobility Management (HMIPv6)", [RFC 4140](#), August 2005.
- [IPSEC] Kent, S. And K. Seo, "Security Architecture for the Internet Protocol", [RFC 4301](#), December 2005.
- [MIPv6] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", [RFC 3775](#), June 2004.
- [MCOA] Wakikawa, R., Ernst, T., and K. Nagami, "Multiple Care-of Addresses Registration", Internet Draft, [draft-ietf-monami6-multiplecoa-00.txt](#), June 2006.
- [SHIM6] Nordmark, E. And M. Bagnulo, "Level 3 multihoming shim protocol", Internet Draft, [draft-ietf-shim6-proto-05.txt](#), May 2006.

## Authors' Addresses

Dave Thaler  
Microsoft  
One Microsoft Way  
Redmond, WA 98052

Phone: +1 425 703 8835  
Email: dthaler@microsoft.com

## Full Copyright Statement

Copyright (C) The Internet Society (2006).

This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR

Thaler  
Draft

Expires August 2006  
IP Mobility Comparison

10  
October 2006

IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

## Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in [BCP 78](#) and [BCP 79](#).

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at [ietf-ipr@ietf.org](mailto:ietf-ipr@ietf.org).

Thaler

Expires August 2006

11