Network Working Group
Internet-Draft
Expires: August 14, 2005

T. Henderson
The Boeing Company
February 13, 2005

# Generalizing the HIP base protocol
# draft-henderson-hip-generalize-00

## Status of this Memo



## Copyright Notice



## Abstract

The Host Identity Protocol and architecture (HIP) proposes to add a cryptographic name space for network stack names. This draft observes that HIP can be viewed as an instance of a more general migration towards decoupling identity from location in the Internet architecture, and shows how other proposals (mobile IP, multi6, mobike, and i3) fit into this framework. We argue that if the HIP base protocol were to be slightly generalized, it might be useful to

other related efforts and might allow more experimental flexibility. Specifically, an extensible identifier TLV, the ability to define usage profiles for the HIP handshake, and a relaxation of the requirements that specific HIP messages carry specific parameters are the three changes suggested.

Table of Contents

## 1. Introduction

The Host Identity Protocol (HIP) [1] is an experimental effort in the IETF and IRTF to study a new public-key-based name space for use as host identifiers in Internet protocols. Taking a step back, HIP can be viewed as one instance of a large number of proposals for decoupling (network) name or identity from (network) location in the Internet architecture, managing more than one IP address for active communications flows, or providing an additional layer of indirection in the protocol stack, located at or slightly above the network layer.

The topic of whether a new name space is needed for the Internet is controversial. The Name Space Research Group (NSRG) at the IRTF was not able to reach consensus on the issue, nor even to publish a final report. The IRTF HIP research group is tasked to evaluate the impact of deployment of a HIP or related name space in the Internet. Yet, there seems to be little disagreement that, for many scenarios, some level of indirection from network name to network location is essential or highly desirable to provide adequate service. Mobile IP [2] is one example (the first such Standards Track proposal), with particular deployment and security properties, that reuses an existing name space for host naming. Since mobile IP was finalized (and in a few cases, even around or before the time it was initially proposed [3]), many new variants to providing this indirection have been suggested.

Most recently, there has been standardization and development efforts in the IETF and IRTF on multi6 protocols and HIP. In the research community, several related proposals have been explored, such as the Internet Indirection Infrastructure (i3) [4], IPNL [5], DataRouter [6], Network Pointers [7], FARA [8], and TRIAD [9]. The purpose of this draft is to outline the broad framework into which most of these examples fit, provide a way of categorizing the various proposals, and how they might be coherently combined, and discuss how the HIP base protocol [1] could be generalized to better support this broader framework.

## 2. Motivation

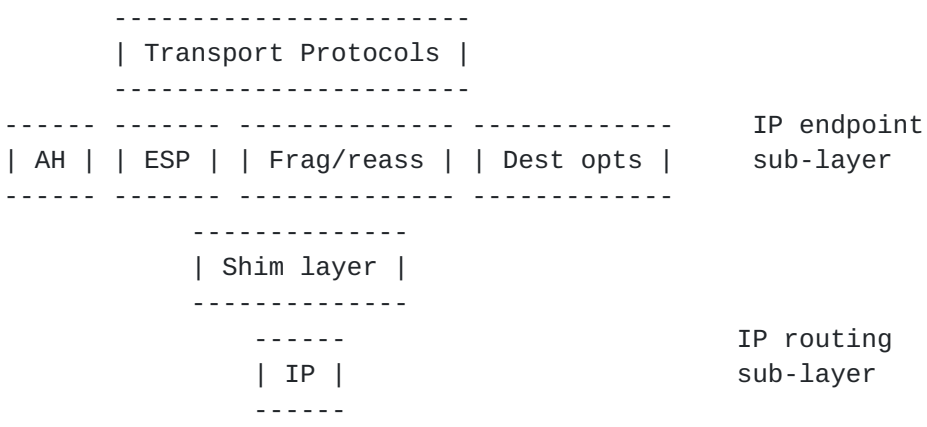
It is beyond the scope of this draft to discuss whether a network layer identifier is needed or preferred to identifiers at other layers, but some of the main reasons that are frequently cited in support of identifiers at this layer include generality, security, mobility, multihoming (both site and local multihoming), traversal of multiple addressing realms, and the enabling of network overlays. For more insight into the motivations of various proposals, see, e.g., [4], [10], [11], [12], and [8].

The purpose of this draft is to explore the common ground of a number of proposals to use location-independent identifiers as part of the network layer (or logically or explicitly wedged between the network and transport layer protocols), and to describe how a more general HIP protocol might be of more general use.

## 3. Taxonomy of Proposals

In this section, we attempt to categorize a number of proposals and show the overall commonality of the approach. As examples, we will describe how the multi6 shim [13], mobile IP [2], HIP [1], and i3 [4] map into this framework.

The following figure, adapted from [13], depicts the architecture under consideration (although not all proposals map exactly to this architecture, the diagram is conceptual). It illustrates a placement of a (logical or real) shim below the IP endpoint sublayer and the IP routing sublayer.




The following details are relevant to such an architecture and are different from traditional systems:

Upper layer identifier: The 32- or 128-bit datum used by transport protocol or above (that may be different from the IP address or locator used at the IP routing sub-layer). Examples include special IP addresses (e.g., mobile IP home address, the identifier-address discussed in [13], and unique-local addresses [14]), and host identity tags (HITs) [1], which are non-routable by the existing IP infrastructure. A further distinction may be made between transport, session, and application-layer identifiers.

Identifier resolution: If the upper layer identifier is not routable or is not the same as the outer IP addresses that will appear on the packet, it must be resolved to a routable locator. Proposals in this space are sometimes categorized as being "early binding" (e.g., HIT resolution on the end hosts, mobile IP with route optimization) or "late binding" (e.g., trigger resolution within the i3 infrastructure, mobile IP without route optimization).

Context establishment: When upper layer identifiers are used that are different from the locators, some context establishment protocol is likely needed to signal the upper layer identifiers in use, and perhaps to establish context for flow demultiplexing and other purposes. The HIP base protocol is a clear example of this, serving to signal to the peer the upper layer HIT identifiers to use (and also to authenticate the host if needed), to derive keying material used within the protocol itself and for security associations, and, when ESP is used, to select SPIs. Other working groups (shim6 and mobike) are poised to define their own context establishment protocol.

Per-packet context tag: When identifiers and locators are different, some kind of context tag is needed for receivers to locate the right identity context for the received packet. In HIP with ESP, the SPI serves as a compressed representation of the HITs; other tags may also be possible with HIP. Mobile IP with route optimization uses Routing Headers or Destination Options for this purpose. Another example is the M6 shim protocol of SIM [15].

Locator management: The techniques by which multiple locators are associated with the identifier, using some security technique for binding, and by which locators are selected for source and destination addresses when there are more than one to choose from. Proposals in this space include MAST [16], CELP [17], multi6 failure detection and locator selection [18], hash-based addresses [19], and HIP multihoming extensions [20].

## 3.1 Examples

Below are some examples of how specific proposals map into the above framework.

### 3.1.1 Mobile IP with Route Optimization

Upper layer identifier: The home address serves as an upper layer identifier.

Identifier resolution: Resolution is done at the endpoints, when the Care-of Address (COA) is appended (early binding).

Context establishment: The Binding Update procedure is used to establish the tunneling context.

Per-packet context tag: The home address is carried in each packet, in either the Home Address Destination Option or the Type 2 Routing Header.

Locator management: New CoA locators are sent directly to the correspondent nodes via the Binding Update message. The Binding Update is authenticated via the key generated as part of the return routability procedure.

### 3.1.2 Host Identity Protocol

Upper layer identifier: The Host Identity Tag, a 128-bit hash of the public key, is used as the upper layer identifier in transport protocols.

Identifier resolution: Early-binding; either performed via DNS lookup, some to-be-developed resolution service, or opportunistically (when the Initiator does not know the Responder's identity, only the address).

Context establishment: A four-packet handshake performs a Diffie-Hellman key exchange and, when used with ESP, sets up the context for the SA.

Per-packet context tag: The SPI in the SA serves as a compressed representation of the HITs in every data packet.

Locator management: Mobility extensions to the base protocol allow IP addresses associated with an ESP tunnel to be added, changed, and authenticated.

### 3.1.3 Multihoming L3 Shim

Upper layer identifier: Some kind of IP address, although the exact semantics are still unsettled.

Identifier resolution: Performed at the end-hosts (early binding).

Context establishment: An as-yet unspecified protocol will be used to establish context when the upper layer identifiers in use start to diverge from the locators in use.

Per-packet context tag: Options include using predefined relationships between identifier addresses and locator addresses, use of the flow label, or use of a new extension header.

Locator management: Locators may be related to each other cryptographically, or may be authenticated via some as-yet unspecified protocol.

#### 3.1.4 i3 (Internet Indirection Infrastructure)

Upper layer identifier: The i3 tag.

Identifier resolution: Performed in the i3 forwarding infrastructure, since the act of sending and receiving packets is decoupled (late binding).

Context establishment: Directives for receiving packets sent to particular tags are explicitly inserted into the forwarding infrastructure by receiving hosts; no end-to-end context need be established.

Per-packet context tag: Explicitly inserted in the IP packet: [IP | UDP | trigger stack | transport data].

Locator management: Locator management is handled by receivers and their interactions with the forwarding infrastructure.

### 3.2 Combinations and Syntheses

Not surprisingly, a large number of variants and combinations of the above have been proposed, to aggregate the desirable properties of distinct proposals. For example, we have:

- HIP/i3: The Host Identity Indirection Infrastructure (Hi3), advocated as a means of securing i3 with the HIP protocol [21];
- HIP/IKE: Proposal to use IKEv2 as the control plane for HIP [22];
- HIP/mobile IP: As presently defined, Mobile IP with Route Optimization resembles HIP mobility. It has been suggested that HIP could be used to secure the route optimization of mobile IPv6;
- HIP/multi6: A lighter-weight variant of HIP was proposed, to address the concerns of HIP's requirement for public-key operations and the need to manage a new name space [23];
- MOBIKE: Working group defining mobility enhancements to IKEv2 that will allow SAs to persist across locator changes [24]; and
- HIP Rendezvous Server (RVS): The HIP RVS is evolving to resemble a combination of a mobile IP home agent and a STUN [25] server.

Our conjecture is that a generalized HIP protocol may make some of these combinations easier, as exemplified in Section 4.2 below.

## 4. Implications for HIP work

It seems wasteful to this author for so many experimental and early standardization efforts to be designing to similar goals yet arriving at slightly different protocol solutions. Given that HIP is an experimental effort, and that the overall acceptance of the architecture and its implications is still an open question, it is worth considering whether there are protocol or architectural elements of the above taxonomy that could be generalized in HIP, to allow a greater breadth of experimentation and future flexibility. If the HIP protocol elements were more modular, HIP-based protocols might be more useful to many of these efforts. In that sense, we should explore whether the currently proposed HIP protocol can be handled as a particular usage profile of a more general architecture. Note that recent decisions in the HIP working group to decouple ESP from the base protocol are an initial step in this direction.

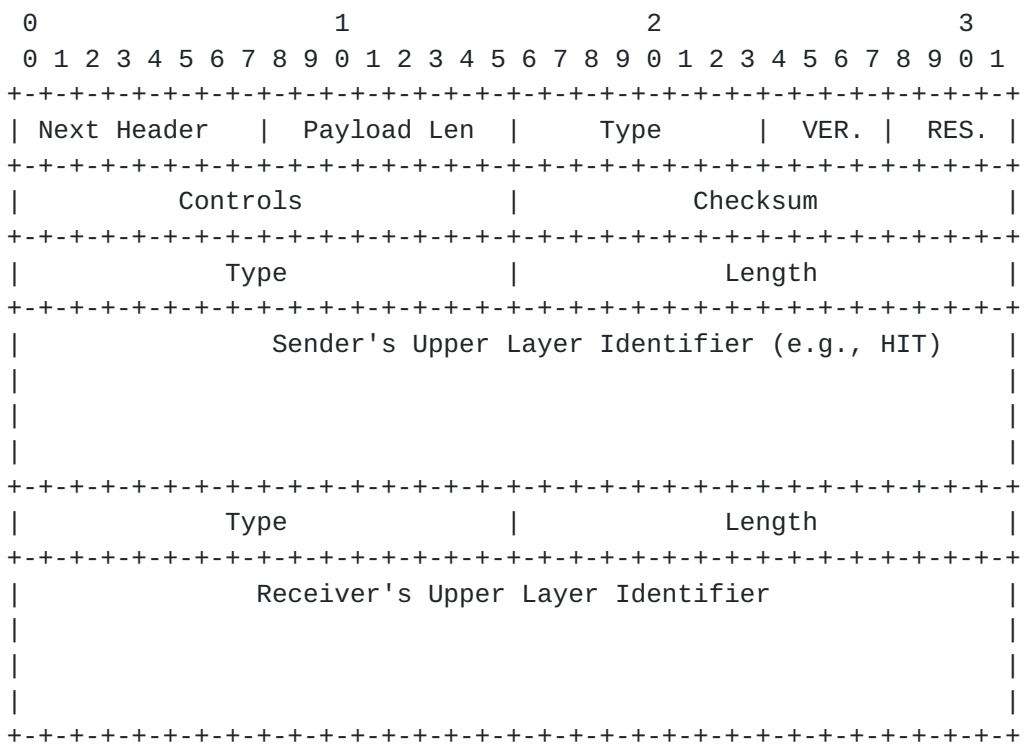
### 4.1 Proposed changes to HIP

The following changes would make HIP more flexible, at the expense of slightly more per-packet overhead in the protocol. The existing HIP could be mapped directly to the below as a specific usage profile.

#### 4.1.1 Identifiers

Allow the use of non-128-bit and non-HIT identifiers. For example, the initial locators might be used as the upper layer identifiers, or some other flat name (other than HIT). In addition, we should consider whether larger than 128-bit HITs may be needed in the future for HIP. If in the HIP header, a TLV were used instead of the bare 128-bit HITs, the context establishment protocol may be useful for other non-HIP uses.

Thus, the HIP header would look like:




### 4.1.2 Handshake

The existing HIP handshake (I1 through R2) is based on the SIGMA family of key-exchange protocols [26] and should continue to be the basis for the context handshake for the existing HIP usage profile, but there should also be other possibilities allowed, especially for impoverished devices that are willing to trade some security for less computation (public key signatures). The multi6 WIMP proposal based on hash chains [27] is one such alternative context-establishment handshake. One way to potentially support multiple protocol semantics would be to support a handshake-type parameter in the I1. The R1 could accept or reply with a list of handshake-types that it supports (i.e., similar to how the HIP- and ESP-TRANSFORM are negotiated today). An alternative to another TLV that saves bits but is less flexible is to use some of the HIP Control bits. The handshake could also potentially be delayed, such as in the multi6 shim proposals (in which one possible use case is to avoid performing any context handshake until a locator set has to change).

### 4.1.3 Mandatory parameters

There should be very few mandatory parameters for a given HIP packet type, in general. However, for a specific usage profile, there will be mandatory parameters. For example, when using the current HIP

profile, R1 MUST contain PUZZLE, but not necessarily when using another profile. The main mandatory parameters are the identifier TLVs discussed above in Section 4.1.1, which are always the first two parameters in the HIP header. The HIP base protocol specification should not include statements such as making ESP mandatory for a HIP implementation.

### 4.1.4 Per-packet context

This step (towards more flexibility) has already been agreed upon by the working group, allowing ESP to be one of potentially other per-packet contexts used with HIP (including possibly SRTP [29] or another shim header such as the M6 header proposed in SIM [15]).

## 4.2 Example Uses

Presently, the HIP drafts are being reworked and extended to cover NAT traversal and middlebox registration issues. The extensions will be based on established techniques including STUN [25], and MIDCOM and NSIS WG work. If a generalized HIP protocol were available and had solved all of these issues, they may apply more generally to other protocol efforts. For example, NAT traversal techniques could perhaps be common across multiple protocols.

Likewise, there are probably techniques in use in other protocols that could be leveraged in the generalized HIP. For example, micromobility extensions to mobile IP could be folded into a general framework and made to apply to non-mobile-IP mobility as well.

### 4.2.1 Securing MIPv6 Binding Update

One security aspect of Mobile IPv6 is that, while the mobile host can be assumed to have a security relationship (shared secret) with the home agent, it has no such assurance with an arbitrary correspondent node. This has made securing the mobile IPv6 route optimization mechanism more involved.

Presently, a mobile host using Mobile IPv6 can elect to send a Binding Update to any correspondent node that implements the extensions. Prior to the binding update, a return routability check through the home network is needed to create a binding management key (Kbm). This binding management key does not have persistence across mobile node readdressing.

An alternative may be to use the Diffie Hellman key exchange defined in the HIP base protocol to create keying material to authenticate binding updates, and to use the HIP mobility management technique (UPDATE/UPDATE ACK and address check) to authenticate via a keyed

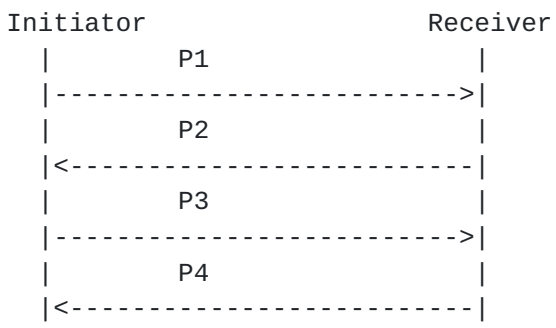
MAC. For example, the mobile node could initiate a "mobile IP-based" HIP exchange with the correspondent node using its home address as the source upper layer identifier, the correspondent node's IP address as the destination upper layer identifier, and some parameter or control bit to declare that the HIP I1 has "mobile IP" semantics. The client puzzle and nonce could be optionally included in the HIP R1, DIFFIE_HELLMAN would be mandatory, and signatures would be optional (variants could be defined that still used public keys for authentication if desired, and allowed their inclusion as additional HIP parameters).

One possible benefit of the above is that it more closely aligns with the presently defined mobile IPv6-- the handshake can be deferred (initiated, perhaps, only before a mobile node is ready to move), and there is no reliance on public key operations, although there is a path forward to add such if so desired. Use of a home agent becomes optional (via HIP rendezvous server). The overall approach provides a possible migration path from an enhanced mobile-IP-based solution (which does not require new name space management) to public-key based extensions that may (HIP backed up by PKI or certificates) or may not (opportunistic HIP, or Purpose-Built Keys) involve strong identity authentication.

### 4.2.2 Site multiHoming by IPv6 interMediation (shim6)

The shim6 WG is expected to be chartered to produce an IPv6 site multihoming solution based on a specific network layer shim architecture. The overall approach is discussed in a recent multi6 draft "Multihoming L3 Shim Approach" [13]. Some features of this solution have already been defined by the multi6 design team (e.g., hash-based addresses) [19], while other elements such as the context management protocol are still unspecified. Some goals stated in [13] are to use routable IP locators as the upper layer identifiers, and to permit context establishment to be deferred or to occur asynchronously with data packets.

The multi6 functional decomposition [10] describes a number of functions that could potentially be met by a generalized HIP protocol that used routable IP addresses (or even centrally-assigned unique local addresses [28]) as upper layer identifiers. Specifically, the identified M6 host-pair establishment exchange:




could be supported by a generalized HIP that allowed for non-HIT identifiers, and alternatives for shared secret generation (e.g., hash chains such as described in WIMP-F [27] could be defined for such a usage profile). Additionally, it seems that if locator set management techniques (Section 4 of [10]) are to be developed as part of the shim6 solution, such techniques should be reused and not reinvented by HIP.

## 5. Security Considerations

There are clearly security issues related to mixing and matching protocol elements, in terms of potentially weakening security properties of a given protocol such as HIP. However, we do not address the security properties of any particular usage profile supported by a more generalized protocol, but leave that instead for other drafts.

## 6. IANA Considerations

No specific proposals in this draft.

## 7. Acknowledgments

Jeff Ahrenholz, Pekka Nikander, and Jukka Ylitalo provided comments on an earlier version of this draft.

## 8 References

[1] Moskowitz, R., "Host Identity Protocol", draft-ietf-hip-base-01 (work in progress), October 2004.

[2] Johnson, D., Perkins, C. and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

[3] Castineyra, I., Chiappa, N. and M. Steenstrup, "The Nimrod Routing Architecture", RFC 1992, August 1996.

[4] Stoica, I., Adkins, D., Zhuang, S., Shenker, S. and S. Surana, "Internet Indirection Infrastructure (i3)", Proceedings of ACM SIGCOMM, August 2002.

[5] Francis, P. and R. Gummadi, "IPNL: A NAT-Extended Internet Architecture", Proceedings of ACM Sigcomm Conference, August 2001.

[6] Touch, J. and V. Pingali, "DataRouter: A Network-Layer Service for Application-Layer Forwarding", Proceedings of International Workshop on Active Networks (IWAN), December 2003.

[7] Tschudin, C. and R. Gold, "Network Pointers", ACM Computer Communications Review, January 2003.

[8] Clark, D., Braden, R., Falk, A. and V. Pingali, "FARA: Reorganizing the Addressing Architecture", Proceedings of ACM SIGCOMM FDNA Workshop, August 2003.

[9] Cheriton, D. and M. Gritter, "TRIAD: A New Next-Generation Internet Architecture", Unpublished, available at Citeseer, July 2000.

[10] Bagnulo, M. and J. Arkko, "Functional decomposition of the M6 protocol", draft-ietf-multi6-functional-dec-00 (work in progress), December 2004.

[11] Moskowitz, R., "Host Identity Protocol Architecture", draft-ietf-hip-arch-02 (work in progress), January 2005.

[12] Balakrishnan, H., Lakshminarayanan, K., Ratnasamy, S., Shenker,

S., Stoica, I. and M. Walfish, "A Layered Naming Architecture for the Internet", Proceedings of ACM SIGCOMM, August 2004.

[13] Nordmark, E. and M. Bagnulo, "Multihoming L3 Shim Approach", draft-ietf-multi6-l3shim-00 (work in progress), January 2005.

[14] Hinden, R. and B. Haberman, "Unique Local IPv6 Unicast Addresses", draft-ietf-ipv6-unique-local-addr-09 (work in progress), January 2005.

[15] Nordmark, E., "Strong Identity Multihoming using 128 bit Identifiers (SIM/CBID128)", draft-nordmark-multi6-sim-01 (work in progress), October 2003.

[16] Crocker, D., "MULTIPLE ADDRESS SERVICE FOR TRANSPORT (MAST):AN EXTENDED PROPOSAL", draft-crocker-mast-proposal-01 (work in progress), September 2003.

[17] Crocker, D., "Framework for Common Endpoint Locator Pools", draft-crocker-celp-00 (work in progress), February 2004.

[18] Arkko, J., "Failure Detection and Locator Selection in Multi6", draft-arkko-multi6dt-failure-detection-00 (work in progress), October 2004.

[19] Bagnulo, M., "Hash Based Addresses (HBA)", draft-ietf-multi6-hba-00 (work in progress), December 2004.

[20] Nikander, P., "End-Host Mobility and Multi-Homing with Host Identity Protocol", draft-ietf-hip-mm-00 (work in progress), October 2004.

[21] Nikander, P., "Host Identity Indirection Infrastructure (Hi3)", draft-nikander-hiprg-hi3-00 (work in progress), June 2004.

[22] Yan, R., "A proposal to replace HIP base exchange with IKE-H method", draft-yan-hip-ike-h-00 (work in progress), November 2004.

[23] Nikander, P., "Considerations on HIP based IPv6 multi-homing", draft-nikander-multi6-hip-01 (work in progress), July 2004.

[24] Kivinen, T. and H. Tschofenig, "Design of the MOBIKE protocol", draft-ietf-mobike-design-01 (work in progress), January 2005.

[25] Rosenberg, J., Weinberger, J., Huitema, C. and R. Mahy, "STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)", RFC 3489, March 2003.

[26] Krawczyk, H., "The IKE-SIGMA Protocol", draft-krawczyk-ipsec-ike-sigma-00 (work in progress), November 2001.

[27] Ylitalo, J., "Weak Identifier Multihoming Protocol (WIMP)", draft-ylitalo-multi6-wimp-01 (work in progress), July 2004.

[28] Hinden, R. and B. Haberman, "Unique Local IPv6 Unicast Addresses", draft-hinden-ipv6-global-local-addr-02 (work in progress), July 2003.

[29] Baugher, M., McGrew, D., Naslund, M., Carrara, E. and K. Norrman, "The Secure Real-time Transport Protocol (SRTP)", RFC 3711, March 2004.

## Author's Address

Tom Henderson
The Boeing Company
P.O. Box 3707
Seattle, WA
USA

EMail: thomas.r.henderson@boeing.com

## Intellectual Property Statement



## Disclaimer of Validity



## Copyright Statement



## Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.