HIP
Internet-Draft
Intended status: Standards Track
Expires: April 30, 2017

R. Moskowitz
X. Xu
B. Liu
Huawei

October 27, 2016

HIP Enabled ID/Loc separation for fast 5GPP IP mobility
draft-moskowitz-hip-based-5gpp-ip-mobility-01.txt

Abstract

HIP [RFC7401] stands alone in providing a secure Endpoint ID for decoupling the Internetworking and Transport protocol layers. The addition of a secure rendezvous service to facilitate mobility will form the cornerstones for this 5GPP mobility technology. This document will describe complete mobility environment and the additional components needed.

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, 2017.

Table of Contents

1. Introduction

IP mobility in the next generation cellular networks will demand shortest path routing, transportation of data secure from a laundry list of attacks, minimal cost infrastructure, and a viable business model for the providers of the 5GPP infrastructure.

Infrastructure costs for the 5GPP network come in many forms. Costs can arise from the cost to support network services, or costs to encapsulate data, or network over-provisioning costs to reduce network delays. At the heart of all the 3GPP mobility costs is the effort to reduce reconnection delays for IP packets so improve users experience. The preferred solution for the 5GPP infrastructure will offer the best possible user experience at the best delivery price point.

HIP, with some important infrastructure enhancements can deliver on these requirements. This document will detail the infrastructure environment needed along with how all the HIP pieces will fit together.

Further, HIP multihoming support can facilitate a "Make then Break" connectivity model that would add to the user experience and facilitate network providers offloading of traffic to more cost-effective connections.

Finally, HIP mobility is not an overlay solution to mobility. Infrastructure implications are principally requirements for RVS, HIP Proxies (for legacy host mobility access), and potentially HIP NAT traversal services.

2. Terms and Definitions

2.1. Requirements 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].

2.2. Definitions

X: X.

3. The components to a HIP-based Mobile world

Three fundamental components lay the foundation of a HIP-based mobile world. These need extreme scalability at numbers easily ranging from 10 billion to 1 trillion entries. Many portions can be fragmented. That is there is needed fore-knowledge to gain entry.

3.1. Service to HIT mapping by device/owner name

"I wish to make a video call to Alice" query to a video call service should return Alice's HIT. Alice could register her HIT with the video calling service mapping by proving ownership of the HIT (via a HIP registration exchange). Which is a separate exercise beyond the basic scope of this service.

3.2. HIT to IP mapping service

The HIT is then mapped to Alice's device's current IP address for setting up the HIP Security Association and the video stream connection between the IP addresses, mapped to the HITs rather than the location IP addresses.

Even at a later time, a cached HIT can be used to discover Alice's device's current IP address.

For a multihomed device, all addresses can be evaluated, perhaps by an analytics engine associated with the device's RVS for best route selection.

3.3. Shortest Path Routing support

Both Bob and Alice are very active people and their devices are constantly moving. However they wander after starting the session, their devices need to stay in contact with each other. This needs good performance for when the are in the same city or across the world.

For multihomed devices, all the addresses should be evaluated and the best route selected.

4. Providing services to meet mobility needs

4.1. Scaleable HITs

HITs as defined in RFC7401 [RFC7401] have a 96 bit flat address space. A 1 trillion deployment HITs would have a 0.0006% probability of a collision Appendix A. However, it is probably significantly worst than this due to historical problems with 'good' random number generators or asymmetric key pairs. Selecting a HIT that will not collide with a future communication peer is an effort in futility. Hierarchical HITs [I-D.moskowitz-hierarchical-hip] provides a manageable approach to HITs and supplies the basics for a viable business model for registering ownership of a HIT.

Alice selects a Hierarchical HIT Domain Authority (HDA) for her device A. This may be a different HDA than her device Q. She agrees to the policy of use by that HDA and follows their instructions to register the HHIT for the device. The HDA insures there is no authorized collision with her selected HHIT. She then publishes that HHIT for the services she wishes to be publicly known. Or she can just share her HHIT with friends and/or colleagues. At any time she may withdraw that HHIT. If she is found in violation of the HDA's policy, it can unregister her device.

4.2. Additional services associated with the HDA RVS

The RVS mechanism provides a rich environment to add additional services to enhance the overall performance of mobility.

For example, where a device registers multiple locators on RVS registration, an analytics engine can assess connection costs for each HIP connection request (I1 or UPDATE) received.

4.3. Preparing to use an HHIT

HHIT strongly recommends using the HIP RVS. Even a truly stationary HIP-enabled server should use it and use the corresponding 'HIP fast Mobility' to stay connected with its mobile communication partners. An RVS could be used for active load balancing across servers with different HITs.

All devices mobile MUST maintain an active RVS connection. This is required even if device Q never publishes any services but always initiate the session. Q still needs RVS to support fast mobility. Without it the recovery from a double-jump would be left up to Q with no possible successful mobility update by its HIP peer until Q completes its mobility update.

4.4. Protecting privacy of an HHIT

An HDA may have a policy to only confirm the validity of a HHIT to HI mapping on receipt of an I2 or R2 packet from the recipient of that packet. This shows that the HIP device was actively connecting to the peer requesting validation and already has a HIT to HI pairing. This protects against robots and the like trolling for valid HHITs.

A device can have as many HHITs as it wishes, registering each with a different HDA, if desired. It can withdraw a HHIT and register a new one, provided the HDA permits this action. This is commonly done for identity privacy reasons. If Bob wants some medical advice, he can have his device register a new HHIT for this research then withdraw it when finished.

4.5. Contacting a device based on its HHIT

There can be a direct DNS mapping of the HDA within the HHIT to that HDA's RVS. This provides the access to the device where ever it may be.

4.6. Intra-HDA peering agreements

A HIP Client to RVS connection that spans the globe will work, as will the mobility updates. But this may not be the most efficient approach. An HDA may globally diversify its RVS and use DNS to direct the client to the 'nearest' RVS.

Alternatively, two HDAs could maintain a peering arrangement. The mechanism by which a client selects the 'best' HDA peer geographically and is contacted through that RVS rather than the HHIT native RVS is a future work item.

4.7. Maintaining the HIP session through all mobility events

With each peer in a HIP Security Association maintaining an active connection to their HHIT RVS, the HIP fast mobility mechanism ensures SA remapping to any location changes in a timely manner.

5. HIP proxies to Legacy (non-HIP) hosts

A HIP mobile host can use non-HIP connections to legacy, static servers. This approach would burden the communications with reconnects. 5GPP may well have a significantly higher occurrence of IP address changes than 4GPP. This would benefit from a HIP mobility enabled mechanism provided in HIP proxy solutions [I-D.irtf-hiprg-proxies].

6. IANA Considerations

There are no IANA considerations for this document.

7. Security Considerations

TBD

8. Acknowledgments

Sue Hares of Huawei contributed to the clarity in this document.

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

9.2. Informative References

[I-D.irtf-hiprg-proxies] Zhang, D., Xu, X., Yao, J., and Z. Cao, "Overview of HIP Proxy Scenarios and Solutions", draft-irtf-hiprg-proxies-05 (work in progress), March 2012.

[I-D.moskowitz-hierarchical-hip]
Moskowitz, R. and X. Xu, "Hierarchical HITs for HIPv2", draft-moskowitz-hierarchical-hip-01 (work in progress), September 2016.

[RFC7401] Moskowitz, R., Ed., Heer, T., Jokela, P., and T. Henderson, "Host Identity Protocol Version 2 (HIPv2)", RFC 7401, DOI 10.17487/RFC7401, April 2015, <http://www.rfc-editor.org/info/rfc7401>.

Appendix A. Calculating Collision Probabilities

The accepted formula for calculating the probability of a collision is:

$$p = 1 - e^{-k^2/(2n)}$$

P Collision Probability
n Total possible population
k Actual population

Authors' Addresses

Robert Moskowitz
Huawei
Oak Park, MI 48237
USA

Email: rgm@labs.htt-consult.com

Xiaohu Xu
Huawei
Huawei Bld, No.156 Beiqing Rd.
Beijing, Hai-Dian District 100095
China

Email: xuxiaohu@huawei.com

Bingyang Liu
Huawei
Huawei Bld, No.156 Beiqing Rd.
Beijing, Hai-Dian District 100095
China

Email: xuxiaohu@huawei.com