HIP Research Group
Internet-Draft
Intended status: Informational
Expires: September 7, 2011

Z. Cao
H. Deng
F. Cao
China Mobile
March 6, 2011

HIP Extension for Flow Mobility Management
draft-cao-hiprg-flow-mobility-00

Abstract

This document defines flow mobility extension to the Host Identity Protocol (HIP). A multi-homed HIP host makes the binding of a flow and one or more locators, through the new parameter "E-LOCATOR", which is the extension of "LOCATOR" defined in RFC5206, the host can acknowledgement his peers with addresses available that fit for some traffic flow. Peer hosts then selects the most appropriate address to transfer the traffic flow.

Table of Contents

1. Introduction

The Host Identity Protocol (HIP) [RFC4423] uses a new identity, named host identities, instead of IP addresses, as host identities. Packets between two HIP hosts are forwarded by IP addresses but identified by the host identities. Thereby when the IP address of a host is changed, the connections between the host and its peers can be sustained. [RFC5206] encompasses messaging and elements of procedure for basic network-level mobility and simple multihoming. A general "LOCATOR" parameter for HIP messages that allows for a HIP host to notify peers about alternate addresses at which it is reachable is defined. The LOCATORs may be merely IP addresses, or they may have additional multiplexing and demultiplexing context to aid the packet handling in the lower layers.

To enable the traffic control, HIP could be extended to support the flow mobility. This document extends LOCATOR to support end-to-end flow mobility of HIP. The extended LOCATOR, named as E-LOCATOR, includes locators defined in RFC5206 and a flow identifier mobility option, which defines the flow that is suitable transferred through the corresponding locator. The detail format of E-LOCATOR is described in Section 4.

The motivations to do HIP flow mobility include:

- Enable the flow mobility in HIP. That means flow can be transferred through the most appropriate interface or redirected to a better interface or address according to some factors, such as address enable situations, user preference and operator policy, etc.

- Enable the load sharing. The traffic to a certain interface of host can be distributed among different interfaces. When the resource of one connection is limited, other interfaces can be used to help deliver the data together.

A flow is defined as a set of IP packets matching a traffic selector. A traffic selector can identify the source and destination IP addresses, transport protocol number, the source and destination port numbers and other fields in IP and higher layer headers. For more flow information, please refer to [RFC6089].

2. Scenarios

End-to-end flow mobility is important to HIP multihoming. The traffic control, charging, QoS control and other operations can be operated based on flow.

A host that has one interface with multiple addresses, or a host that has multiple interfaces, each interface has a separate address are both multi-homed HIP hosts. It is envisioned that a multi-homed host can use several addresses simultaneously to transfer flows.

When different addresses are used simultaneously to transfer flows, first there must be policies in the multi-homed host about deciding a flow to be transferred through a certain address; we call this as flow binding. Then end-to-end address chosen and readdress are both necessary. Before a communication, the multi-homed host should be able to inform its peer about the reachable addresses, with the corresponding flow binding; peers should be able to choose the most suitable address for communication according to the flow going to be transferred; during the conversation, caused by IP address changing or in order to realize load balance, due to some mechanism, the multi-homed host may redirect some exiting flows with its peer from a previous interface or address to a new interface or address.

These situations are typical flow mobility scenarios. In these scenarios, there is a need for some helper functionality in the network, such as a HIP rendezvous server [RFC5204]. Such functionality is out of the scope of this document.

3. Protocol Operations

This protocol is based on "End-Host Mobility and Multihoming with the Host Identity Protocol" [RFC5206] .

This section introduces the solution of flow mobility. Using the parameters "E-LOCATOR" introduced in this specification, a multi-homed HIP host can notify peers about alternate addresses with corresponding flow mobility option; a flow can be identified by a FID in the mobility option. We can assume this as flow binding. Then the peers can select the most suitable address as the communication address. During the communication, when the using address is changed or in order to make load balance, the multi-homed host can redirect the existing flows to other addresses by using E-LOCATOR.

3.1. Flow binding

It is assumed that there should be some policies of flow binding. A flow binding in the multi-homed host is about a flow to be transferred through a certain address. In E-LOCATOR, a locator is followed by a "Flow Identification Mobility Option", which means flow with FID in the option is going to be transferred through the locator. The details of these policies are outside the scope of this document.

In this document, a host with HIP protocol that initializes a connection is Initiator; its peer host is Responder[RFC4423].

3.2. Base Exchange

Assuming that the Responder host has multiple addresses available at begin of the communication with its peer. When Initiator initializes the Base Exchange, a Responder host may include an E-LOCATOR parameter in the R1 packet that it sends to the Initiator. This parameter MUST be protected by the R1 signature.

The procedure of Base Exchange with RVS is followed:

1. First of all, Responder registers a RVS service with a RVS server; its current available IP addresses are maintained by the RVS.
2. An Initiator initializes the Base Exchange. First, it sends I1 packet with Initiator's and may be Responder's HIT, to the RVS, with which the Responder registers. The source IP address of I1 is Initiator's IP address. The destination IP address of I1 is RVS's IP address that can be got from a DNS server or other servers.
3. Then the RVS found that I1 is aimed to the Responder, so it updates the head of I1 packet and forwards it to the Responder. The source IP address of I1 is RVS's IP address. The destination address is currently available IP address of the Responder [RFC5204].
4. After authentication, the Responder sends R1 packet to the Initiator; an E-LOCATOR parameter is included in R1. This parameter is protected by the R1 signature. Currently available IP addresses of the Responder with corresponding flow are list in E-LOCATOR.
5. When the Initiator gets the R1 packet, according to the flow that to be transferred, it chooses the most suitable address among the entire addresses list in the E-LOCATOR, that is to say, choose the locator with the FID the same as the flow to be transferred. If there is only one locator in the parameter, then the Initiator chooses it as the communication address. If there is no locator with the corresponding flow, then the Initiator may choose the preferred locator to use. The Initiator should set the status as ACTIVE once an address has been determined and send the I2 packet to the new choose address. The I1 destination address and the new choose address may be identical. All new other locators must still undergo address verification once the Base Exchange completes [RFC5206].

During the Base Exchange, as the Initiator knows what kind of flow is to be transferred, it can make its most suitable address as the

source address. The Initiator may include one or more E-LOCATOR parameters in the I2 packet, independent of whether or not there was a E-LOCATOR parameter in the R1. These parameters must be protected by the I2 signature. Even if the I2 packet contains E-LOCATOR parameters, the Responder must still send the R2 packet to the source address of the I2. The new choosing address by the Responder should be identical to the I2 source address. If the I2 packet contains E-LOCATOR parameters, all new locators must undergo address verification as usual, and the ESP traffic that subsequently follows should use the addresses determined during the Base Exchange.

3.3. Flow Mobility

When a multi-homed host moves to a new place, the available address may be changed or there may be a new address available and the new address is more suitable for the existing flow, the multi-homed host can send UPDATE message to its peer to inform the new available or new more suitable address and then redirect the existing flow to the new address.

3.3.1. Readdress without Rekey

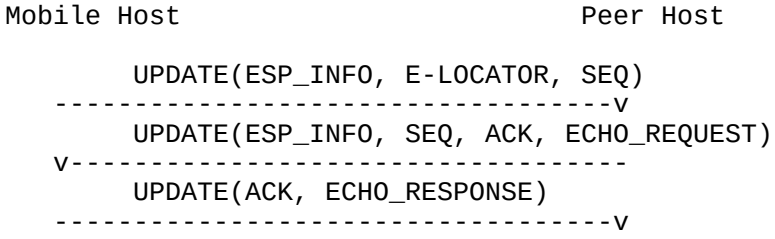

Figure 1: Readdress without Rekey

According to RFC5206, during the procedure of readdressing, hosts can use the old SAs or create new SAs. The first example considers the case in which no rekeying occurs on the SAs and the new IP address are within the same address family (Ipv4 or Ipv6) as the first address. The scenario is depicted in Figure 1.

1. The multi-homed host is disconnected from the peer host for a short period of time while it switches from one IP address to another. Upon obtaining a new IP address, the multi-homed host sends an E-LOCATOR parameter to the peer host in an UPDATE message. The same FID as existing flow must be included with the new locator. Set of ESP_INFO and SEQ parameters are the same as RFC5206 3.2.1 depicts.

2. When the peer host receives the UPDATE message, it performs as RFC5206 3.2.1 depicts.
3. The multi-homed host completes the readdress by processing the UPDATE ACK and echoing the nonce in an ECHO_RESPONSE. Once the peer host receives this ECHO_RESPONSE, it considers the new address to be verified and can put the address into full use.
4. The existing ESP traffic flow is transferred to the new address.

3.3.2. Readdress with Multi-homed-Initiated Rekey

If the Multi-homed host decide to rekey the SAs at the same time that it notifies the peer of the new address. In this case, the above procedure described in Figure 2 is slightly modified. The UPDATE message sent from the Multi-homed host includes an ESP_INFO with the OLD SPI set to the previous SPI, the NEW SPI set to the desired new SPI value for the incoming SA, and the KEYMAT Index desired. Optionally, the host may include a DIFFIE_HELLMAN parameter for a new Diffie- Hellman key. The peer completes the request for a rekey as is normally done for HIP rekeying, except that the new address is kept as UNVERIFIED until the UPDATE nonce challenge is received as described above. Figure 2 illustrates this scenario.

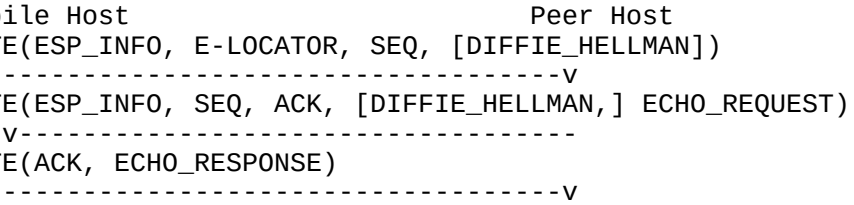

Figure 2: Readdress with Multi-homed-Initiated Rekey

3.3.3. Load balance

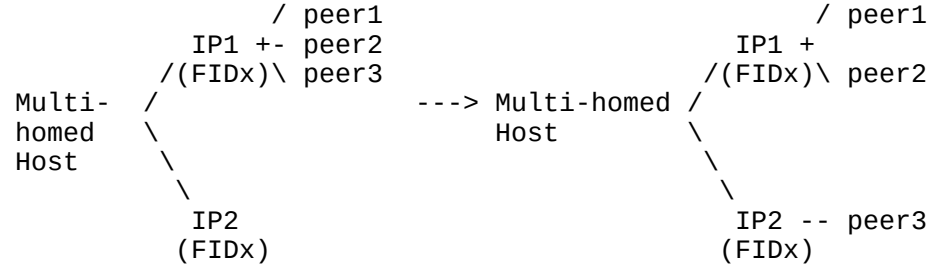

Figure 3: Load Balance

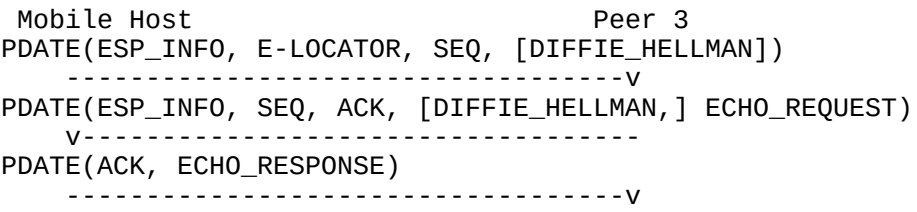

Figure 4: Flow Redirection

Considering the scenario that the multi-homed host has two address IP1, I23, which both are suitable for transferring flow X, identified by FIDx. Peer1 host and Peer2 both have flow X with multi-homed host through IP1. A new flow X is started between multi-homed host and Peer3, also using IP1. Then in order to make load balance, multi-homed host decides to redirect flow X with Peer3 to IP3. It then sends an UPDATE message to Peer 3. E-LOCAOR is included in the message, and there is only one locator, carries IP3 with FIDx option in the parameter. Once receiving the UPDATE message, since there is only one address available for FIDx, Peer3 redirects the flow X to IP3. The scenario is depicted as Figure 3. There must be policies for a multi-homed host to decide when to redirect the flow and which address is redirected to, the policies are out scope of this document.

4. E-Locator Definition

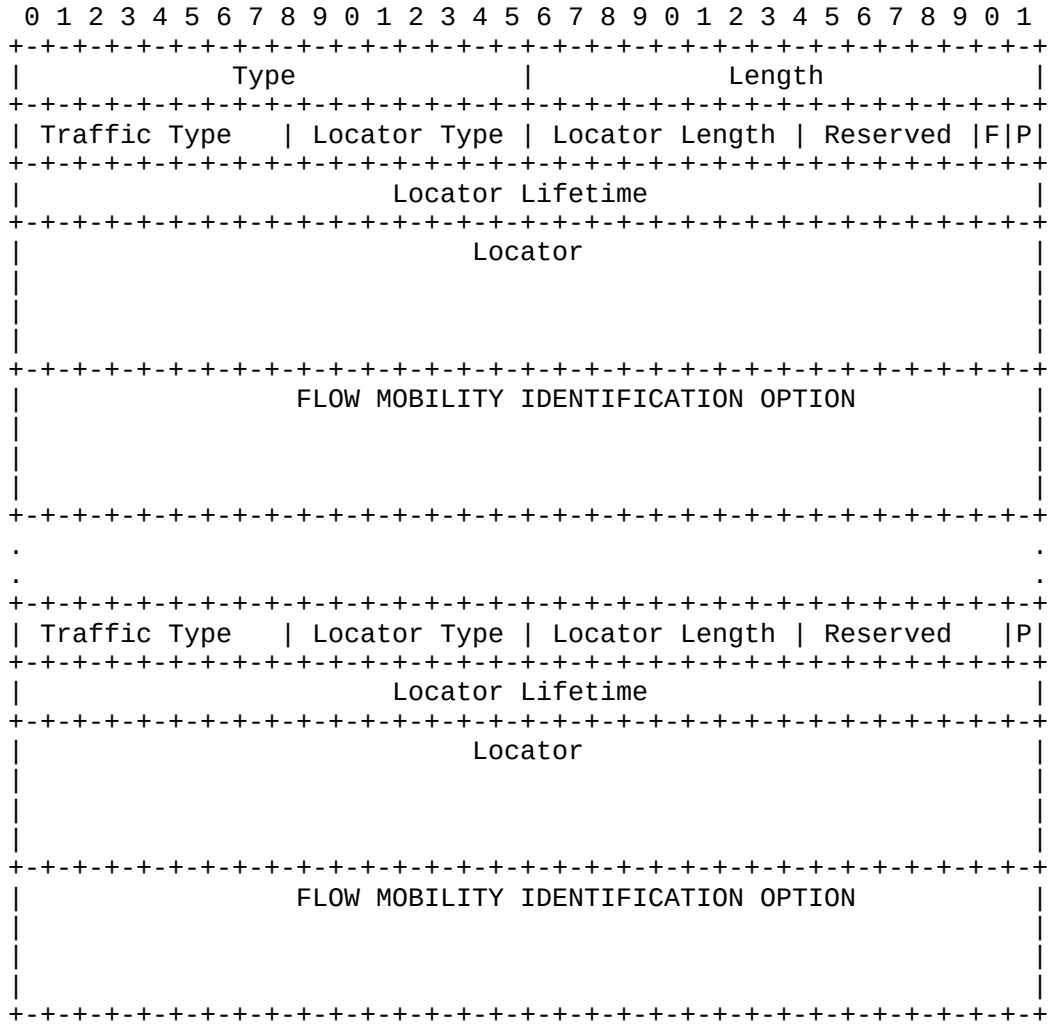

Figure 5: E-Locator

F Flag

A new flag, when the locator carries a corresponding flow identification mobility option, it is set to 1; otherwise it is set to 0, that means the locator is suitble for all flow;

Flow Identification Mobility Option: as defined in [RFC6089]

5. Security Considerations

TBD.

6. IANA Considerations

This document does not require any IANA actions.

7. Normative References

[RFC4423] Moskowitz, R. and P. Nikander, "Host Identity Protocol (HIP) Architecture", RFC 4423, May 2006.

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

[RFC5205] Nikander, P. and J. Laganier, "Host Identity Protocol (HIP) Domain Name System (DNS) Extensions", RFC 5205, April 2008.

[RFC5206] Nikander, P., Henderson, T., Vogt, C., and J. Arkko, "End-Host Mobility and Multihoming with the Host Identity Protocol", RFC 5206, April 2008.

[RFC6089] Tsirtsis, G., Soliman, H., Montavont, N., Giaretta, G., and K. Kuladinithi, "Flow Bindings in Mobile IPv6 and Network Mobility (NEMO) Basic Support", RFC 6089, January 2011.

Authors' Addresses

Zhen Cao
China Mobile
28 Xuanwumenxi Ave,Xuanwu District
Beijing 100053
China

Email: zehn.cao@gmail.com

Hui Deng
China Mobile
28 Xuanwumenxi Ave,Xuanwu District
Beijing 100053
China

Email: denghui@chinamobile.com

Feng Cao
China Mobile
28 Xuanwumenxi Ave,Xuanwu District
Beijing 100053
China

Email: fengcao@chinamobile.com