Mobile IPv6 Extensions (mext)	C.P. Perkins
Internet-Draft	Tellabs
Intended status: Informational	Jul 11, 2011

SFF Extensions for Mobile IPv6
draft-perkins-mext-sffexts-01

Abstract

A mobile node with multiple radio interfaces running in single-radio mode will typically need IP address continuity as it migrates from one 4G wireless network to another; Mobile IPv6 is very well suited for that purpose. For such mobile nodes using Mobile IP, mobility management by the home agent can be extended to provide necessary information about the Signal Forwarding Functions (SFFs) that have been defined for WiMAX and for eHRPD/CDMA networks. In this document, we explain the operations required to support single-radio mobile nodes and specify new extensions to Mobile IPv6 Binding Update and Binding Acknowledgement for supporting ease of access between mobile nodes and SFFs.

Status of this Memo

Copyright Notice

Table of Contents

*1. Introduction

*2. Overview

*3. Co-locating SFF in the home network with the Home Agent

*4. Extension Formats

*4.1. SFF-REQ (SFF Parameters Request)

*4.2. SFF-REP (SFF Parameters Reply)

*5. Security Considerations

*6. IANA Considerations

*7. References

*7.1. Normative References

*7.2. Informative References

*Appendix A. Acknowledgements

*Author's Address

1. Introduction

There is growing interest to enable efficient handovers between heterogeneous radio access technologies (RATs) for networks owned by the same network operator, or network operators who have entered into roaming agreements. Since authentication is indispensible for enabling the attachment of a mobile node, a mutually accessible authentication authority is indispensible for enabling efficient handovers between such operator networks. Based on this authentication authority, we can develop trust relationships between agents in each network that are charged with responsibilities for aiding handovers.

Wireless devices that are designed to attach to networks using heterogeneous RATs must include radio interfaces enabling connectivity to each desired RAT. But each radio interface requires substantial power -- in fact, the radio interfaces for mobile wireless devices are quite often the biggest consumer of scarce battery power. For this reason, today, and into the foreseeable future, most mobile wireless devices that have multiple radio interfaces will nevertheless only keep one of them powered on at any particular time. Such devices are known as "single-radio" mobile nodes (MNs), notwithstanding the presence of multiple radio interfaces in each MN's hardware.

Single-radio nodes present design challenges, because if only a single radio interface is powered on at any particular time, it is not possible for the device to be simultaneously connected to two different networks. In such cases, handover protocols must try to compensate for the time during which the wireless device will be retuning its hardware to establish a link with the target network. This "break-before-make" mode of operation is susceptible to dropping packets during the time when the target radio access link is not yet established, but the link to the source network has already been released.

For smooth handovers, it is imperative to reduce the time between release of one radio link and establishment of the new radio link at the target network. Before the new link can be established in the target

network, some or all of the following procedures must typically be followed:

- Scheduling the radio link

- Authenticating the mobile node

- Creating proper context for the mobile node

- Allocating data paths for traffic to/from the mobile node

The specific details for each step vary quite a bit depending on the particular RAT used in the target network. But, regardless of the particular target RAT, completing the listed procedures is too time consuming to enable smooth handovers when faced with the "break-before-make" nature of a single-radio MN. For this reason, it is very important that the MN try to accomplish as many of the attachment procedures as possible before releasing its current radio link. So, for instance, while MN is still attached to network N1, it may try to transfer context to a target base station in a target network N2. In fact, almost all of the above procedures can be accomplished ahead of the actual radio link break, with operator agreement and mutual access to core network functions. For ease of discussion, in this document all such handover optimizations will collectively be termed as "pre-registration".
There has been considerable effort invested into protocol support for preregistration. To do the signaling from the current network into the target network, the mobile node needs the following information about the target network:

- Scheduling the radio link

- location of basestation or access point

- IP addresses of signaling endpoints for preregistration functional modules

- Security association parameters for those signaling endpoints

The latter requirement results from the possibility that preregistration signaling between the MN's current network and the target network may traverse the Internet, even though the networks are owned by the same operators or operators who have made roaming agreements. It may be impracticable for such information to be preconfigured into each of the millions of subscriber devices roaming around today's wireless networks, and the number of devices continues to increase rapidly from year to year. Given that, any preconfiguration strategy is likely to fail soon. Therefore, the MN must not only follow the require preregistration procedures for the target network, but it must also discover the necessary IP addresses for the target functional modules, and it must also establish a security relationship with each such target module. The discovery mechanisms for these handover agents typically involve DHCP or resolution of purpose-built DNS name. The former approach could be

integrated with other DHCP access procedures; using DNS affords a speed advantage to the latter approach. One can reasonably ask how the MN might get access to the proper DHCP server or DNS server, especially given the emphasis on private addressing in today's networks. Many restrictions and assumptions are required in order for the necessary information to be supplied to the MN.

These discovery and security procedures are to be undertaken after the MN determines that it would be beneficial to move to a new network. The benefit is typically for improved coverage, but in many cases also results from reduced cost or improved security or access to needed resources unavailable in the current network. For whatever reason, after the determination is made, the MN cannot yet start to carry out its preregistration tasks. The discovery and security tasks cannot be started until the target network can be identified, and the target network is closely associated with the current location of the MN.

In summary, once the MN starts to move to a new network, the following are required:

- Discovery of handover agent(s) in the target network

- Security establishment with target agents

- Pre-authentication using the security services trusted by the foreign network

- Possibly other pre-registration tasks.

Each of these procedures may require lengthy signaling transactions with the MN. It is the goal of this document to specify a way to reduce the time delay associated with the first two tasks. By doing so, it is expected that handover performance can be substantially improved. Moreover, given reasonable assumptions about operator roaming agreements, it is likely that this proposal will be simpler to deploy and simpler for ongoing network management.

The following abbreviations appear in this document:

HA: home agent

MN: mobile node

SFF: Signal Forwarding Function

OSFF: Signal Forwarding Function in the Originating Network

TSFF: Signal Forwarding Function in the Target Network

BU: Binding Update

BAck: Binding Acknowledgement

PoA: Point of Attachment

RAT: Radio Access Technology

2. Overview

Recent documents describing handovers between cooperating networks supporting different radio technologies have specified a new functional module called a Signal Forwarding Function (SFF). The SFF is the agent in the target network which assists the MN to carry out preregistration tasks while the MN still has radio access in its current network. The details of the signaling between the MN and the SFF fundamentally depend on the requirements of the target network; it is out of scope for this document to specify any preregistration protocol exchange that the SFF would handle in the target network on behalf of the MN. See Figure 1.

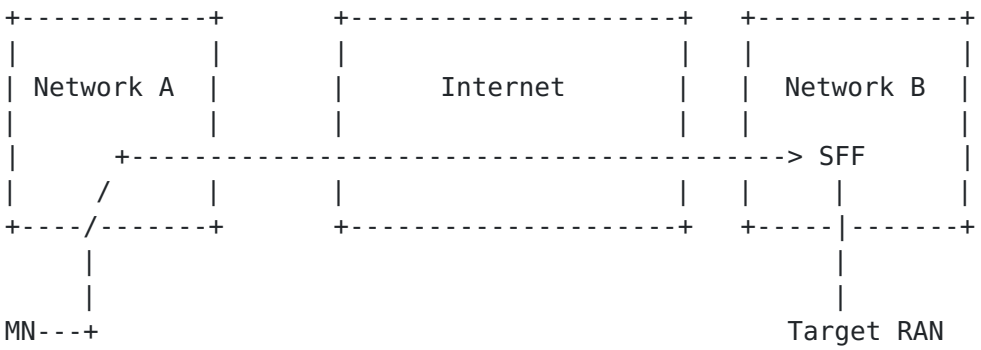


Figure 1: MN at current PoA signaling via SFF in target network

Here, Network A is the current point of attachment for the MN, and Network B is the target network. MN signals to SFF in Network B to prepare for the handover from Network A into Network B.

The SFF in the target network relays the MN signals to the network elements in the Radio Access Network (RAN) which will offer radio access to the MN.

SFF behavior has been specified in detail for eHRPD/CDMA networks as well as for WiMAX networks. For a variety of reasons, seemingly not all technical, 3GPP has chosen to recommend instead a more integrated approach for interworking between LTE networks and other target networks. Notably, LTE handovers are specified under the assumption that the MN's address belongs to the LTE operator. WiMAX and HRPD network technologies are more friendly to assisting MN's that are addressable from via domains supporting other RATs.

Signaling between single-radio MNs and the SFF in a target network may follow protocol under development in the 802.21(c) task group under the auspices of IEEE 802. This document can be viewed as a companion document to the SFF-based handover assistance being defined within 802.21(c).

As the MN moves from one network to another, the SFF that was the target SFF becomes the SFF in the MN's current network. We observe that for operators offering SFF modules for handovers between heterogeneous network types, the SFF in the MN's current network (which can be called the "originating network") can manage security associations with SFFs in neighboring networks belonging to roaming partners. Such security associations facilitate a simplified approach for the necessary discovery and security establishment between a MN and a target SFF, as follows.

When the MN completes its handover to a target network, it will have a security association with the SFF in that target network. If the MN maintains this security association, then it can make use of the SFF in that network to assist in discovery and secure communication with a future SFF in a future target network. The abbreviation TSFF will be used for the target SFF, and the SFF in the MN's current network will be called the "Originating SFF", abbreviated OSFF. With that terminology, the handover between the originating network and the target network can be made faster using the services of the OSFF and the TSFF. See Figure 2.

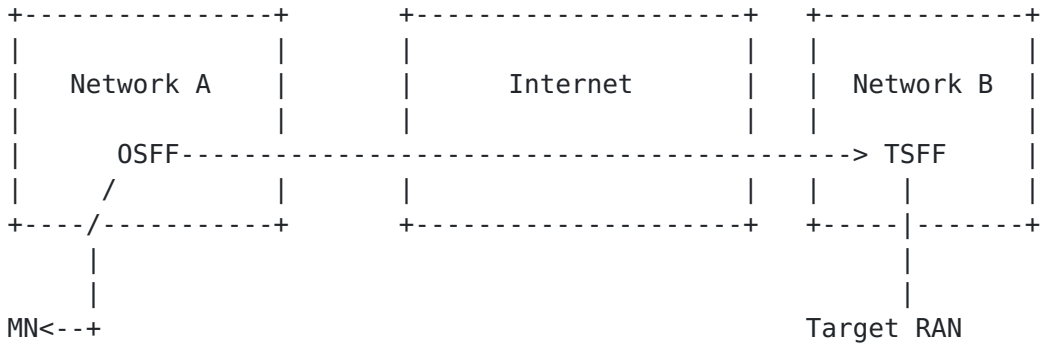


Figure 1: MN handover preparation via OSFF and TSFF

Again, Network A is the current point of attachment for the MN, and Network B is the target network. MN initially relays signals to TSFF (in Network B) by way of OSFF (in Network A) to prepare for the handover from Network A into Network B.

Specifically, when the MN has determined that a handover is beneficial, the following services should be offered by the OSFF:

- The OSFF should be able to identify the proper TSFF to help the MN with handover to the target network.

- The OSFF should be able to provide a shared key to establish a security association between the MN and the TSFF.

In other words, the OSFF enables optimized discovery and security establishment for the TSFF and thus substantially simplifies and shortens the handover preparation time needed by the MN. When the MN arrives at the target network, the TSFF becomes the OSFF and the MN has a security association with the OSFF useful for future handover services.

3. Co-locating SFF in the home network with the Home Agent

The foregoing overview does not explain how a MN might best get information about the SFF in the network providing the MN's initial point of attachment (PoA).
Up until this point in the current document, there has been no attention paid for the need of the MN to maintain IP address continuity as it moves from the originating network to a target network. For this purpose, the MN can use Mobile IPv6[RFC3775] (or Mobile IP for IPv4 devices[RFC3344]). The Binding Update (BU) from the MN is, more often than not, transmitted as soon as the MN has established a radio link at the target network; alternatively, the BU could be sent just as the radio link between the MN and the originating network were to be broken. This latter approach as the advantage of reducing the amount of time during which the home agent would be routing packets to the wrong network, but would not work as well if the target network required a long time to establish a new radio link.
When the mobile node (MN) is making its initial point of attachment, it does not yet need the services of any SFF. The MN could get the required address of the SFF and establish a security association at any time after its initial attachment procedures have completed. In this document, it is proposed that this information be delivered by the home agent as part of the Mobile IPv6 registration procedure. Furthermore, it is proposed that the SFF function in the home domain should be co-located with the home agent in that domain. Doing so has several advantages, as follows:

- The home agent is a natural repository for mobility management functions such as SFF. If the home agent is co-located with the SFF

in the MN's home domain, it can readily assist the MN with handovers from any visited network back to the home network. This is expected to be a very frequent case.

- The MN naturally already has a security association with the home agent. When the home agent is co-located with home SFF (i.e., HSFF), then the all of the necessary procedures for finding and securing communications with SFFs in all visited networks of roaming partners can be accomplished without any additional need for DHCP or IKEv2.

- The MN is already required to securely transmit a BU to its home agent. Adding a new extension to the BU, requesting the IP address and shared key for the local SFF is economical and introduces fewer error conditions.

- In the typical case where the MN begins its initial network attachment in its home network, the MN can rely on its home agent as an OSFF for future handovers to target networks.

- For handovers from WiFi into any network of roaming partner, the MN can utilize its home agent/HSFF as an OSFF to establish preregistration signaling with any desired target network enabled for roaming.

Given the appropriate security model between roaming partners, co-locating the SFF function with the home agent in the home network enables also reduces the number of mobility agents requiring configuration and management.
In this document, only signaling elements for Mobile IPv6 (MIPv6) are specified. Similar extensions to Registration Request and Registration Reply for Mobile IPv4 can readily be specified.
The following extension to the Binding Update of MIPv6 is needed so that the MN can request information about the SFF in the network providing its care-of address

- SFF address Request (SFF-REQ)

The following extension to the Binding Acknowledgement is needed so that the HA can request information about the SFF to the requesting MN

- SFF address Reply (SFF-REP)

The SFF in the MN's current network (i.e., OSFF) will be tasked with enabling security associations between the MN and a future target SFF. Therefore the MN will require a security association with OSFF, and there does not appear to be a need for providing an "SFF address Request" extension that does not also imply a simulataneous request for key material to establish the security association with OSFF.
The Home Agent MAY supply an SFF-REP extension to the MN in its BAck even when the MN has not requested it, if the MN is known by preconfiguration or other means to support the ability to utilize OSFF for handover assistance.

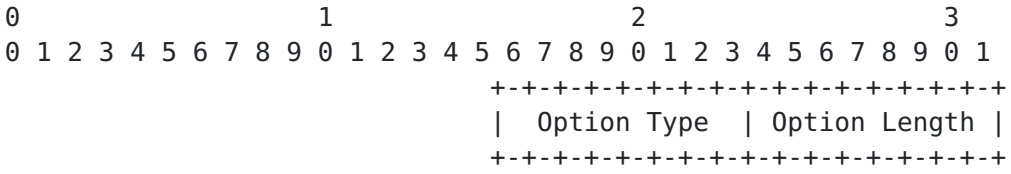
It is presumed in this initial version of the SFF-REQ and SFF-REP specification that the MN's care-of address is sufficient for the home agent to determine the proper and roaming network to which the OSFF belongs, and thus be able to determine the IP address for the OSFF. Future versions of this specification may specify additional location information to be included with the Binding Update.

4. Extension Formats

The SFF-REQ may only appear in a Binding Update IPv6 Mobility Header, and the SFF-REP may only appear in a Binding Acknowledgement IPv6 Mobility Header.

4.1. SFF-REQ (SFF Parameters Request)

A mobile node (MN) inserts the SFF-REQ extension appear in a Binding Update Header to request that the home agent supply information about the SFF in the network providing the Care-of Address to the MN.



Option Type

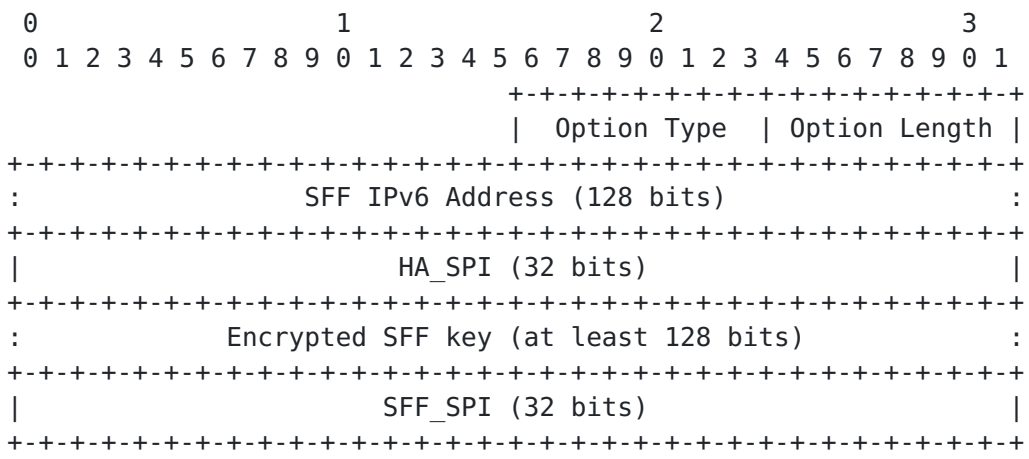
The Option Type will be allocated by IANA from the space of Mobility Option types.

Option Length

The Option Length is 0.

4.2. SFF-REP (SFF Parameters Reply)

A home agent (HA) inserts the SFF Parameter Reply (SFF-REP) in a Binding Acknowledgement. The SFF-REP contains the IP address of the SFF (i.e., OSFF) in the MN's current network, as well as an encrypted key to enable secure communication between the MN and OSFF.



Option Type

The Option Type will be allocated by IANA from the space of Mobility Option types.

Option Length

The Option Length is 24 + [# of bytes for Encrypted SFF key].

SFF IPv6 Address

The SFF IPv6 Address (128 bits)

HA_SPI

HA_SPI (32 bits) is used by the MN to select the proper Mobility Security Association with its home agent so that it can use the correct security parameters in its computation to recover the SFF key.

Encrypted SFF key

Encrypted SFF key (at least 128 bits)

SFF SPI

The SFF SPI (32 bits) is used by the MN as needed for any future secure communications with the SFF in the network supporting its current Care-of Address. This same SPI will be also be used by the SFF for its secure communications with the MN.

The home agent first picks a random number to be used for K_sff, the desired shared key between MN and SFF. Then, the home agent computes the Encrypted Key as follows, using the parameters it supplies in the SFF-REP:

Encrypted SFF key = [K_sff (+) HMAC_SHA1 (SFFaddr, SFF_SPI)]

where:

K_sff is the desired shared key between MN and SFF

Encrypted SFF key hides K_sff for transmission to the MN

(+) is XOR

HMAC_SHA1[RFC2401] is the algorithm to be used by the Home Agent to encrypt the K_sff for delivery in encrypted form to the mobile node. HMAC_SHA1 uses the key forming the basis of the mobility security association (indexed by HA_SPI) between the MN and the HA

SFFaddr is the IPv6 address of the SFF

SFF_SPI is the SPI of the security association between the MN and SFF, used here simply as a random number.

The mobile node computes the following value from the parameters in the SFF-REP:

K_sff = [Encrypted SFF key (+) HMAC_SHA1 (SFFaddr, SFF_SPI)]

where:

K_sff is the desired shared key between MN and SFF

(+) is XOR

HMAC_SHA1[RFC2401] is the algorithm to be used by the MN to recover the K_sff delivered in encrypted form by the home agent. HMAC_SHA1 uses the key forming the basis of the mobility security association (indexed by HA_SPI) between the MN and the HA

SFFaddr is the IPv6 address of the SFF

SFF_SPI is the SPI of the security association between the MN and SFF, used here simply as a random number.

5. Security Considerations

This document uses techniques from RFC 2104 (and RFC 3957) for key distribution. Up until now, no security weaknesses have been reported for those techniques, as long as the basic encryption algorithms are themselves secure. HMAC_SHA1 is recommended for encryption.
In future revisions of this specification, SHA-256 or AES may be instead specified, since SHA-1 has been shown to have some potential vulnerabilities. However, for low volume (comtrol plane) signaling, such vulnerabilities are unlikely to have any significant effect.
This specification should be considered as an initial draft. The exact nature of the algorithm used to compute the Encrypted Key field of the SFF-REP is subject to discussion and changes are likely.

The home SFF (HSFF) colocated with home agent is also charged with the responsibility for supplying K_sff to the SFF in the network supporting the mobile node's Care-of Address (i.e., OSFF). Messages currently undergoing specification within IEEE 802.21(c) and 802.21(a) are likely to be used between HSFF and OSFF. The nature of the algorithm used to provide confidentiality for the IEEE 802.21(c) messages between HSFF and OSFF may well be different than the algorithm used for SFF-REP computation.

6. IANA Considerations

This document requires allocation of two new extensions to Mobile IPv6 Binding Update and Binding Acknowledgement.

7. References

7.1. Normative References

[RFC2401]	Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.
[RFC3344]	Perkins, C., "IP Mobility Support for IPv4", RFC 3344, August 2002.
[RFC3775]	Johnson, D., Perkins, C. and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

7.2. Informative References

[cool_draft]	Doe, J. and J. Doe, "A cool draft. ", Internet-Draft draft-does-cia-rules.txt, 2010.

Appendix A. Acknowledgements

This document has benefitted from discussions with the following people, in no particular order: Anthony Chan, Subir Varma

Author's Address

Charles E. Perkins Perkins Tellabs Phone: +1-408-421-1172 EMail: charliep@computer.org