

Mipshop WG
Internet-Draft
Intended status: Standards Track
Expires: March 21, 2008

T. Melia, Ed.
NEC
G. Bajko
Nokia
S. Das
Telcordia
N. Golmie
NIST
S. Xia
Huawei
JC. Zuniga
InterDigital
September 18, 2007

Mobility Services Transport Protocol Design
draft-melia-mipshop-mstp-solution-00

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/ietf/lid-abstracts.txt>.

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

This Internet-Draft will expire on March 21, 2008.

Copyright Notice

Copyright (C) The IETF Trust (2007).

Abstract

This document describes a design solution for the IEEE 802.21 Media Independent Handover (MIH) protocol that addresses identified issues associated with the transport of MIH messages. The document describes mechanisms for mobility service (MoS) discovery and transport layer mechanisms for the reliable delivery of MIH messages.

Deleted: To be edited.

Requirements Language

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].

Table of Contents

- 1. Introduction 3
- 2. Terminology 3
- 3. Deployment Scenarios 4
- 4. Solution Overview 6
 - 4.1. Architecture 6
 - 4.2. MIHF Identifiers (FQDN, NAI) 7
- 5. MoS Discovery 7
 - 5.1. MoS Discovery in the home network while attached to the home link 8
 - 5.2. MoS Discovery in the local network and Services are local 9
 - 5.3. MOS Discovery in a roaming Network and Services are at Home 10
 - 5.4. MoS discovery in a remote network 11
- 6. MIH Transport 12
 - 6.1. MIH Message size 13
 - 6.2. MIH Message rate 13
 - 6.3. Retransmission 14
 - 6.4. NAT Traversal 14
 - 6.5. General guidelines 14
- 7. Operation Flows 14
- 8. Security Considerations 16
- 9. IANA Considerations 17
- 10. Acknowledgements 17
- 11. References 17
 - 11.1. Normative References 17
 - 11.2. Informative References 19
- Authors' Addresses 19
- Intellectual Property and Copyright Statements 21

1. Introduction

This document proposes a solution to the issues identified in the problem statement document [I-D.ietf-mipshop-mis-ps] for the transport of IEEE 802.21 MIH protocols.

The MIH Layer 3 transport problem is divided in two main parts: the discovery of mobility services (MoS) and the transport of the information between a mobile node (MN) and MoS. The discovery process is required for a MIH function (MIHF) located in the MN to discover the peer MIHF (e.g. the IP address) of the MoS in the network (e.g. the Point of Service, PoS) either during attachment or during handover. Upon successful discovery, the MIH peers can then exchange information in the form of MIH messages.

This document lists the major MoS deployment scenarios. It next describes the solution architecture, including the MSTP reference model and MIHF identifiers. A description follows of MoS discovery procedures when the MN is in a home or remote network. The remainder of the document describes the MIH transport architecture, example message flows for several signaling scenarios, and security issues.

Deleted: considers firstly standard track IETF-based solutions for the design and recommendations of the discovery and transport protocol components.

2. Terminology

The following terminology is being used in this document:

MIH Media Independent Handover

MIHF Media Independent Handover Function

MIHF USER MIH client initiating and terminating MIH signalling

MIHFID Media Independent Handover Function Identifier

MoS As defined in the problem statement document it includes IS, CS, ES services defined by the IEEE 802.21 standard.

MoSh Mobility Services assigned in the Home Network

MoSv Mobility Services assigned in the Visited Network

MoS3 Mobility Services assigned in a 3rd Party Network

MN Mobile Node

NN Network Node

MSTP Mobility Services Transport Protocol

Comment [DG1]: It might be useful to include one-sentence definitions for each of these. I can work on this if the DT thinks it is worth doing.

- IS Information Service
- ES Event Service
-
- CS Command Service
-
- FQDN
-
- NAI
-
- NAT Network Address Translator
-
- DHCP
-
- DNS
-
- MIH ACK MIH Acknowledgement Message

3. Deployment Scenarios

This section describes the various possible deployment scenarios for the MN and the MoS. The relative positioning of MN and MoS affects resource discovery as well as the performance of the MIH signaling service.

3.1 Scenario S1: Home Network MoS

in this scenario, the MN and the services are located in the home network. We refer to this set of services as MoSh as in Figure 1. The MoSh can be located at the access point the MN uses to connect to the home network, or it can be located elsewhere.

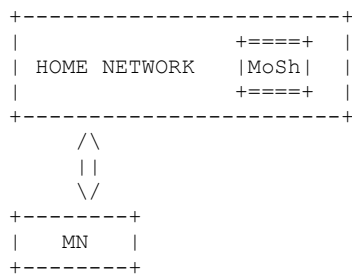


Figure 1: MoS in the Home network

3.2 Scenario S2: Visited Network MoS

In this scenario, the MN is in the visited network and mobility services are also provided by the visited network. We refer to this as MoSv as shown in Figure 2.

Deleted: ¶
¶
¶

Comment [DG2]: The end of the section mentions the possibility that MoS can be spread among several locations. The lead paragraph could include a sentence stating that an actual deployment could consist of a linear superposition of a set of these scenarios. For example, if there are two MoSh (call them A and B) and one MoSv and the MN is not in the home network, then the service scenario could be written as (A+B)*S3 + S2. (I assume that any algorithm for choosing MoS from a set of available service locations is going to be left to the manufacturers.)

Note also that I messed around with the four figures to make them clearer. I was confused for a few seconds when I first saw these; it looked like the MoS was separate from its host network in some way.

Also: is it possible to have MoS located in a non-home network when the MN is home? Does an MN at home use only local MoS? What if there is no local MoS?

Deleted: The following scenarios have been identified:

Deleted: s

Deleted: 1 Home Network MoS,

Deleted: S2 Visited Network MoS

Comment [DG3]: Are there any restrictions on the MoSv? For example, must the MoSv be under the control of the same administrative authority as the home network?

Deleted: n

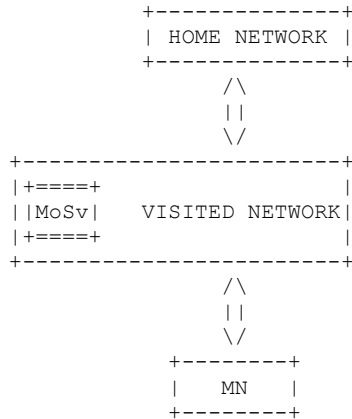


Figure 2: MoSV in the Visited Network

3.3 Scenario S3: Roaming MoS

In this scenario, the MN is located in the visited network and all MIH services are provided by the home network, as shown in Figure 3.

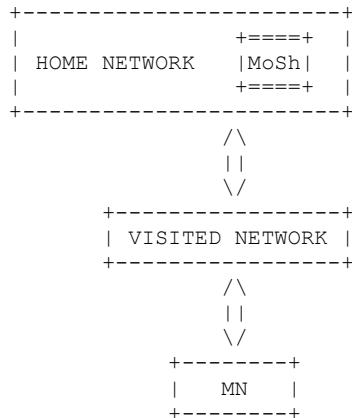


Figure 3: MoS provided by the home network while MN in visited network

3.4 Scenario S4: Third party MoS

In this scenario, the MN is in its home network or in a visited network and services are provided by a 3rd party network. We refer to this situation as MoS3 as shown in Figure 4.

Melia, et al.

Expires March 21, 2008

[Page 5]

Deleted: S3 Roaming MoS

Comment [DG4]: Are there any issues associated with running a MIH connection through a visiting network? For example, are there cases where MIH messages need to be encrypted or flagged so that they don't linger in router queues?

Deleted: ¶

Deleted:

Comment [DG5]: Since this is a roaming scenario, did you mean to call the MoS MoSr? Although MoSh certainly makes sense as well.

Deleted:

Deleted: S4 Third party MoS

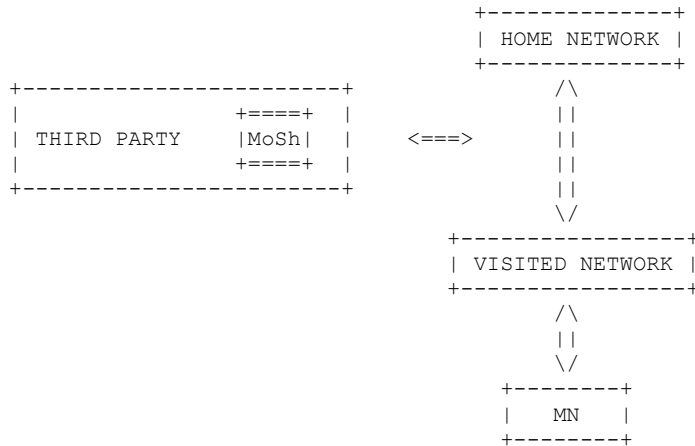


Figure 4: MoS from a third party network

Deleted: form

Different types of MoS can be provided independently of other types and there is no strict relationship between ES, CS and IS, nor is there a requirement that the entities that provide these types be co-located. However, while IS tends to involve large amounts of static information, ES and CS are dynamic services and some relationship between them can be expected, e.g. a handover command (CS) could be issued upon reception of a link event (ES). Hence, while in theory MoS can be implemented in different locations, it is expected that ES and CS will be co-located, whereas IS can be co-located with ES/CS or located elsewhere. Therefore, having the flexibility at the MSTP to discover different services in different locations is an important feature that can be used to optimize handover performance. Resource discovery is discussed in more detail in Section 5.

Deleted: contain more a

Deleted: sort

Deleted: of

Deleted: of a dynamic nature

Deleted: sometimes

Deleted: s

Deleted: could

Deleted: services

Deleted: l

Deleted: either

Deleted: l

Deleted: not

4. Solution Overview

As mentioned in Section 1 the solution space is being divided into two functional domains: discovery and transport. The following assumptions have been made:

- o The solution is aimed at supporting 802.21 MIH services, namely Information Services (IS), Event Services (ES), and Command Services (CS).
- o If the MIHFID is available, FQDN or NAI's realm is used for mobility service discovery. The recommendation to the IEEE 802.21 WG is to restrict discovery to only these two.
- o The solutions are chosen to cover all possible deployment scenarios as described in Section 3.

- o MIHF discovery can be performed during initial network attachment or thereafter.

Comment [DG6]: Is this MIHF or MoS?

For the discovering the location of an MoS, the MN could either be pre-configured with the address of the MoS, or this address could be dynamically assigned through DHCP or DNS by the network. The dynamic assignation methods are described in Section 5.

Comment [DG7]: I think that the word 'thereafter' is vague. If discovery doesn't happen during attachment, when does it take place?

The configuration of the MoS could be executed either upon network attachment or after successful IP configuration. The methodology to be used depends on the considered deployment scenario.

Once the MIHF peer has been discovered, MIH information can be exchanged between MIH peers over a transport layer protocol such as UDP (with MIH ACK for reliable delivery) or TCP. The usage of these protocols is described in Section 6.

Deleted: and

4.1. Architecture

Figure 5 depicts the MSTP reference model and its components within a node. The topmost layer is the MIHF user. This set of applications consists of one or more MIH clients that are responsible for such operations as maintaining MIH databases associated with the IS, processing Layer 2 triggers as part of the ES, and initiating and carrying out handover operations as part of the CS. Beneath the MIHF user set is the MIHF itself. This function is responsible for MoS discovery, as well as creating, maintaining, modifying, and destroying MIH signaling associations with other MIHFs located in MIH peer nodes. Below the MIHF are various transport layer protocols as well as address resolution functions.

Deleted: The following

Comment [DG8]: If I have missed anything important or misplaced the demarcations between the MIHF user and MIHF, please let me know.

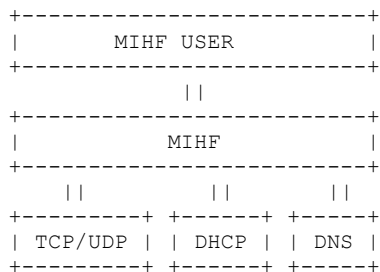


Figure 5: MN protocol stack

The MIHF relies on the services provided by TCP and UDP for transporting MIH messages, and relies on DHCP and DNS for peer discovery.

Deleted: As it can be seen, t

Deleted: as well

In cases where the peer MIHF IP address is not pre-configured, the source MIHF needs to discover it either via DHCP or DNS or a combination of both as described in Section 5. Once the peer MIHF is discovered, MIHF must exchange messages with its peer over either UDP or TCP. Specific recommendations regarding the choice of transport protocols are provided in Section 6.

Deleted: as

Deleted: using

Deleted: on

The above reference architecture does not include other services such as message fragmentation and security. Depending upon the MIH service type (e.g., ES, CS and IS), the message size can be very large. In cases where the underlying layers do not support fragmentation, this may be an issue. There are no security features currently defined as part of the MIH protocol level. However, security can

be

provided either at the transport or IP layer where it is necessary. Section 8 provides some guidelines and recommendations for security.

4.2. MIHF Identifiers (FQDN, NAI)

An MIHFID is an identifier required to uniquely identify the MIHF end points for delivering the mobility services (MoS). Thus an MIHF identifier needs to be unique within a domain where mobility services are provided and invariant to interface IP addresses. An MIHFID MUST be represented either in the form of an FQDN [RFC2181] or NAI [RFC2486]. An MIHFID can be pre-configured or discovered through the discovery methods described in Section 5.

5. MoS Discovery

The MoS discovery method depends on whether the MN attempts to discover an MoS in the local network, in the home network (if the MN is in a remote network), or in a 3rd party remote network that is neither the home network nor the visited network.

In case MoS is provided locally (scenarios S1 and S2), the techniques described in

[I-D.bajko-mos-dhcp-options] and [I-D.bajko-mos-dns-discovery] could be used to transfer MoS information from the network to the MN (via DHCP or DNS). In case MoS is provided in the home network while the MN is in the visited network (scenario S3), an interaction between the DHCP and AAA infrastructure is required similarly to what specified in [I-D.ietf-mip6-bootstrapping-integrated-dhc]. It is assumed therefore that MoS assignment is performed during access authentication and authorization. In case MoS is provided in a remote network other than visited or home networks (scenario S4), the MN uses

only DNS

based methods.

5.1. MoS Discovery when MN and MoSh are in the home network (Scenario S1)

To discover an MoS in the home network, the MN SHOULD use the DNS based MoS discovery method described in [I-D.bajko-mos-dns-discovery]. In order to use that mechanism, the MN MUST first find out the domain name of its home network. Home domains are usually pre-configured in the MNs, thus the MN can simply read its configuration data to find out the home domain name (scenario S1). The DNS query option is shown in Figure 6(a).

Alternatively, the MN MAY use the DHCP options for MoS discovery [I-D.bajko-mos-dhcp-options], as shown in Figure 6(b).

- Deleted: however
- Deleted: provide the model
- Deleted: for
- Deleted: ,
- Deleted: s
- Deleted: es
- Deleted: is
- Deleted: available
- Deleted: at

Deleted: by

Deleted: as

Deleted: The MoS discovery method depends on whether the MN wants to discover an MoS in the local network, home network or a remote network other than home network.

Formatted: Not Superscript/ Subscript

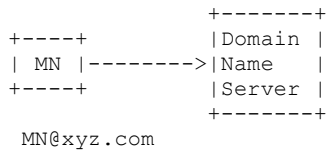
Comment [DG9]: Replace with SHOULD (based on contents of Section 5.1)?

Deleted: attached

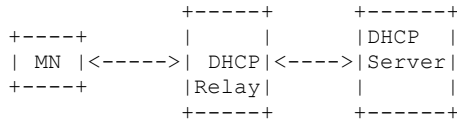
Deleted: apply

Deleted: while attached to the home link

Deleted: . Figure 6 provides such model



(a) using DNS Query



(b) Using DHCP Option

Figure 6: MoS Discovery (a) Using DNS query, (b) using DHCP option

5.2. MoS Discovery when MIN is in visited network and MoSv is also in visited network (Scenario S2)

To discover an MoS in the visited network, the MN SHOULD attempt to use the DHCP options for MoS discovery [I-D.bajko-mos-dhcp-options], as shown in Figure 7(a).

If the DHCP method fails, the MN SHOULD attempt to use the DNS based MoS discovery method described in [I-D.bajko-mos-dns-discovery], as shown in Figure 7(b). In

order to use that, the MN MUST first learn the domain name of the local network. There are a number of ways how the domain name of a network can be learned:

DHCP -- In order to find out the domain name of the local network, the MN SHOULD use the dhcpv4 option 15 for learning the domain name [RFC1533]. A similar solution is available for dhcpv6 [I-D.ietf-dhc-dhcpv6-opt-dnsdomain] .

Reverse dns query -- When DHCP does not provide the required domain name, the MN MAY use reverse DNS (DNS PTR record) [RFC X] to find the domain name associated with the IP address it is using in the visited network. Note, that when a NAT device exists between the MN and the visited network, the MN will first need to find out the external IP address of the NAT device. Some possible methods for determining the NAT's external IP address are STUN [RFC3849] or UPnP [UPnP_IDG_DCP]. Once the MN has determined the external IP address of the NAT device, it MUST use that address in the reverse DNS query.

Comment [DG10]: In this figure and in Figure 7, do we need to include more detail, such as the position of the DNS or DHCP servers to the home or visited network?

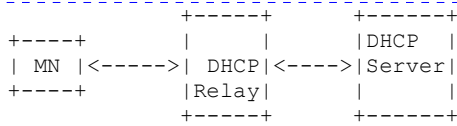
Deleted: the local

Deleted: Services are local

Deleted: s

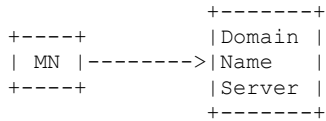
Deleted: local

Deleted: local



Deleted: Figure 7 provides such model.

(a) MOS Discovery using DHCP options



(b) Reverse DNS Query (starting from the IP address)

Figure 7: Discovery (a) using DHCP option, (b) Using DNS

5.3. MOS Discovery when the MN is in a visited Network and Services are at the Home network (Scenario S3)

Deleted: roaming

To discover an MoS in the visited network when MIH services are provided by the home network, the MN SHOULD use the DHCP option along with network access authentication. This procedure is shown in Figure 8. Upon network access authentication and

Deleted: roaming

interaction with the NAS, the home AAA (AAAh) verifies in the AAA profile that the MN is allowed to use the MoS in the home network. The AAAh assigns the

Comment [DG11]: This is the NAS in the visited network, right? The language could be read as referring to a NAS in the home network.

MoS in the home network and sends back the information to the NAS. The MN sends a

DHCP information request as per [RFC3315] containing Home Network Identifier Option indicating the need to allocate the MoS in the home network. The relay agent in the visited network intercepts the information request from the MN

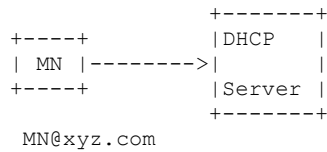
and it forwards to the DHCP server inserting the MIH Relay Agent Option containing the info received by the AAAh. The DHCP server can then reply to the MN by sending the Home Network Information Option. The MN receives the MoSh address.

It should be noted that the AAAh does not know the preferences of the MN, i.e. whether the MoS should be allocated in the home or in visited. The MoS info is stored at the relay agent and forwarded to the MN according to the flags in the Home Network Identifier Option.

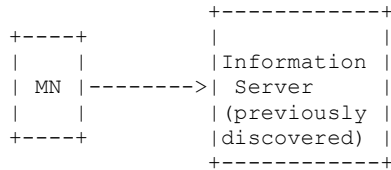
Deleted: what are

Deleted: Figure 8 describes such a model.

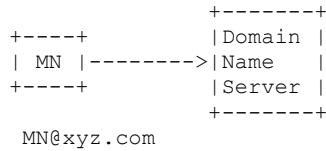
be noted that step c can only be performed upon obtaining the domain name of the remote network.



(a) Discover MoS in local network with DHCP



(b) Using IS query to find the FQDN on the remote network



(c) using DNS Query in the remote network

Figure 9: MOS Discovery using (a) [DHCP Options](#), (b) [IS Query to a known Server](#), (c) [DNS Query](#)

Deleted: DNS Query,

6. MIH Transport [Options](#)

Once the Mobility Services have been discovered, MIH peers MUST exchange information over either TCP or UDP, [as described in \[I-D.draft-rahman-mipshop-mih-transport\]](#). While either protocol can provide the basic transport functionality required, there are performance trade-offs and unique characteristics [associated](#) with each that need

to be considered in the context of the MIH services for different network loss and congestion conditions. [The objectives of this section](#) are to discuss these trade-offs for different MIH settings such as the MIH message size and rate, and the retransmission parameters. In addition, factors such as NAT traversal are also discussed. Given the reliability requirements for the MIH transport, it is assumed in this discussion that the MIH ACK mechanism is to be used in conjunction with UDP, while it is preferred to avoid using [MIH ACKs](#)

Deleted: Thus, the

with TCP since TCP includes acknowledgement and retransmission functionality.

Deleted: a similar

6.1. MIH Message size

Although the MIH message size varies widely from about 30 bytes (for a broadcast capability discovery request) to around 65000 bytes (for an IS MIH_Get_Information response primitive), a typical MIH message size for the ES/CS service ranges between 50 to 100 bytes [IEEE-802.21].

Thus,

considering the effects of the MIH message size on the performance of the transport protocol brings us to discussing two main issues, related to fragmentation of long messages in the context of UDP and the concatenation of short messages in the context of TCP. Since transporting long MIH messages may require fragmentation that is not available in UDP, if MIH is using UDP a limit MUST be set on the size of the MIH message, unless fragmentation functionality is added to the MIH layer or IP layer fragmentation is used instead. In this latter case, the loss of an IP fragment leads to the retransmission of an entire MIH message, which in turn leads to poor end-to-end delay performance in addition to wasted bandwidth utilization. Additional recommendations in [I-D.ietf-tsvwg-udp-guidelines] apply for limiting the size of the MIH message when using UDP and assuming IP layer fragmentation. In terms of dealing with short messages, TCP has the capability to concatenate very short messages in order to reduce the overall bandwidth overhead. However, this reduced overhead comes at the cost of additional delay to complete an MIH transaction, which may not be acceptable for CS and ES services. Note also that TCP is a stream

oriented protocol and measures data flow in terms of bytes, not messages. Thus it is possible to split messages across multiple TCP segments if they are long enough. Even short messages can be split across two segments. This can also cause unacceptable delays, especially if the link quality is severely degraded as is likely to happen when the MN is exiting a wireless access coverage area.

6.2. MIH Message rate

The frequency of MIH messages varies according to the MIH service type. It is expected that CS/ES message arrive at a rate of one in hundreds of milliseconds in order to capture quick changes in the environment and/ or process handover commands. On the other hand, IS messages are exchanged mainly every time a new network is visited which may be in order of hours or days. Therefore a burst of either short CS/ES messages or long IS message exchanges (in the case of multiple MIH nodes requesting information) may lead to network congestion. While the built-in rate-limiting controls available in TCP may be well suited for dealing with these congestion conditions, this may result in large transmission delays that may be unacceptable for the timely delivery of ES/CS messages. On the other hand, if UDP is used, a rate-limiting effect similar to the one obtained with TCP may be obtained by adequately adjusting the parameters of a token bucket

regulator as defined in the MIH specifications [IEEE-802.21]. Recommendations for token bucket parameter settings are specific to the scenario considered.

Deleted: token bucket

6.3. Retransmission

For TCP, the retransmission timeout is adjusted according to the measured RTT. However due to the exponential backoff mechanism, the delay associated with retransmission timeouts may increase significantly with increased packet loss.

Deleted:

If UDP is being used to carry MIH messages, MIH MUST use MIH ACKs. An MIH message is retransmitted if its corresponding MIH ACK is not received by the generating node within a timeout interval set by the MIHF. This approach does not include an exponential backoff and therefore tends to degrade more gracefully than TCP when the packet loss rate becomes large, in the sense that the expected delay does not increase exponentially. The number of retransmissions is limited, which reduces head-of-line blocking of other MIH messages, but this can cause important ES/CS messages to be lost.

6.4. NAT Traversal

There are no known issues for NAT traversal when using TCP. The default connection timeout of 24 hours is considered adequate for MIH transport purposes. However, issues with NAT traversal using UDP are documented in [I-D.ietf-tsvwg-udp-guidelines]. Communication failures are experienced when middleboxes destroy the per-flow state associated with an application session during periods when the application does not exchange any UDP traffic. Hence, communication between the MN and the MoS SHOULD be able to gracefully handle such failures and implement mechanisms to re-establish their UDP sessions. In addition and in order to avoid such failures, MIH messages MAY be sent periodically, similarly to keep-alive messages, to attempt to refresh middlebox state (e.g. ES reports could be used for this purpose). As [RFC4787] requires a minimum state timeout of two minutes or more, MIH messages using UDP as transport SHOULD be sent once every two minutes.

6.5. General guidelines

Since ES and CS messages are small in nature and have tight latency requirements, UDP in combination with MIH acknowledgement SHOULD be used for transporting ES and CS messages. On the other hand, IS messages are more resilient in terms of latency constraints and some long IS messages could exceed the MTU of the path to the destination. Therefore, TCP SHOULD be used for transporting IS messages. For both UDP and TCP cases, if a port number is not explicitly assigned (e.g. by the DNS SRV), MIH messages sent over UDP or TCP MUST use the default port number.

7. Operation Flows

Figure 10 gives an example operation flow between MIHF peers when an MIH user requests an IS service. Scenario 1 is in effect, i.e. the MoS and the MN are both in the MN's home network. Thus DHCP is used for MoS discovery and TCP is used for establishing a transport connection to carry the IS messages. When MoS is not pre-configured, the MIH user needs to discover the IP address of MoS to communicate with the remote MIHF. Therefore the MIH user sends a discovery request message to the local MIHF as defined in [IEEE-802.21].

In this example, we assume that MoS discovery is performed before a transport connection is established with the remote MIHF, and the DHCP client process is invoked via some internal APIs. DHCP Client sends DHCP INFORM message according to standard DHCP and with the MoS option as defined in [I-D.bajko-mos-dhcp-options]. The DHCP server replies via a DHCP ACK message with the IP address of the MoS. The MoS address is then passed to the MIHF locally via some internal APIs. MIHF generates the discovery response message and passes it on to the corresponding MIH user. The MIH user generates an IS query addressed to the remote MoS. MIHF invokes the underlying TCP client which establishes a transport connection with the remote peer. Once the transport connection is established, MIHF sends the IS query in a MIH protocol REQUEST message. The message and query arrive at the destination MIHF and MIH user respectively. The MoS MIH user responds to the corresponding IS query and the MoS MIHF sends the IS response via a MIH protocol RESPONSE message. The message arrives to the source MIHF which passes the IS response on to the corresponding MIH user.

Comment [dwg12]: I like the example here, but I think it would help the reader's understanding if we make this example Section 7.1, and then create a Section 7.2 to include a CS/ES example as well, in which UDP is used for transport and another MoS location scenario is in effect.

- Deleted: Following
- Deleted: for
- Deleted: chosen
- Deleted: whereby
- Deleted: requests
- Deleted: via a discovery message
- Deleted: s
- Deleted: then
- Deleted: then
- Deleted: available
- Deleted: via
- Deleted: s
- Deleted: to
- Deleted: remote
- Deleted: us
- Deleted: it
- Deleted: it

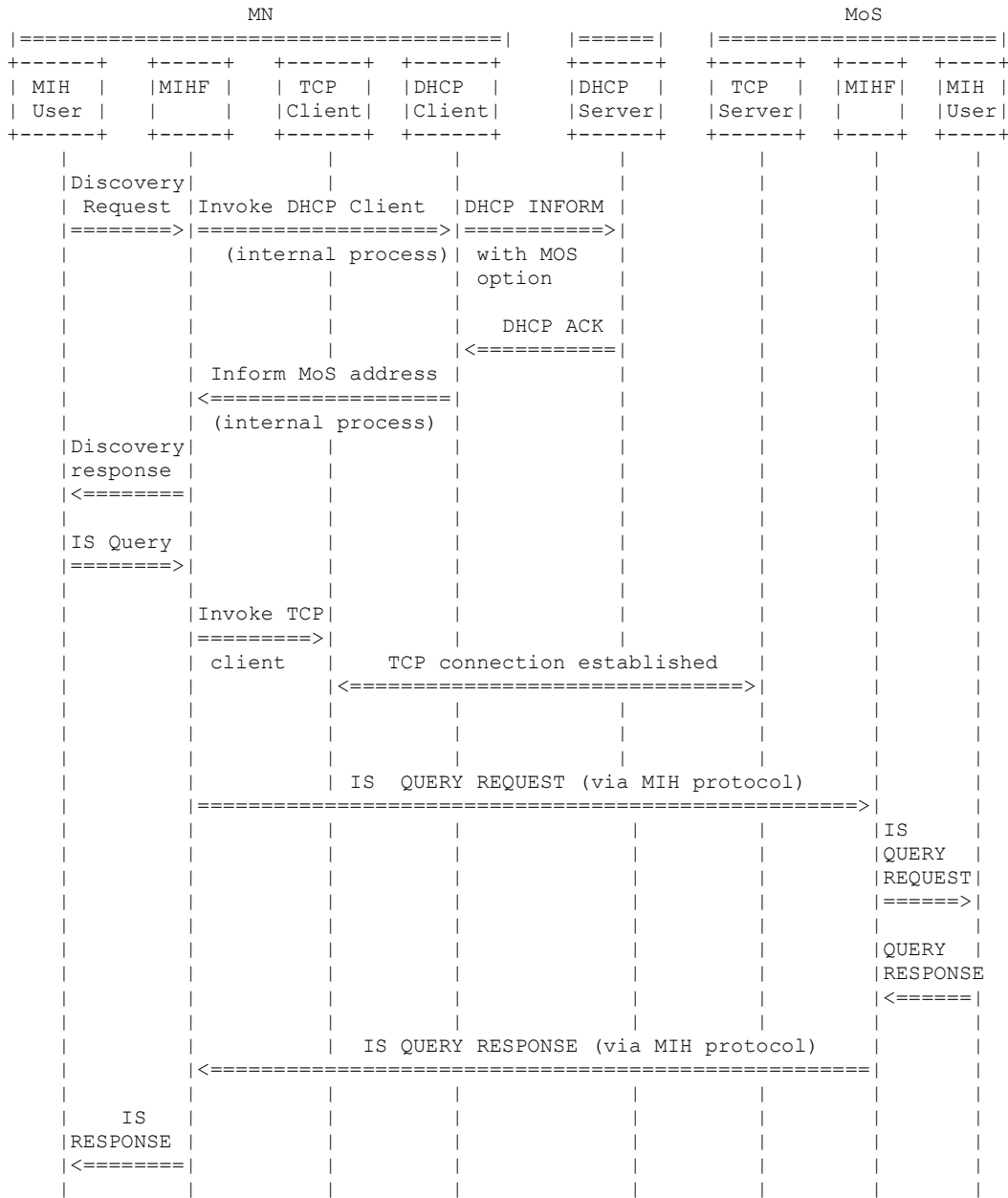


Figure 10: Example Flow of Operation Involving MIH User

8. Security Considerations

There are a number of security issues that need to be taken into account during node discovery and information exchange via a transport connection [I-D.ietf-mipshop-mis-ps]

In case where DHCP is used for node discovery and authentication of the source and content of DHCP messages are required, it is recommended that network administrators should use DHCP authentication option described in [RFC3118]. This will also protect the denial of service attacks to DHCP server. [RFC3118] provides mechanisms for both entity authentication and message authentication.

In case where DNS is used for discovering MoS, fake DNS requests and responses may cause DoS and the inability of the MN to perform a proper handover, respectively. Where networks are exposed to such DoS, it is recommended that DNS service providers use the Domain Name System Security Extensions (DNSSEC) as described in [RFC4033]. Readers may also refer to [I-D.ietf-dnsop-dnssec-operational-practices] to consider the aspects of DNSSEC Operational Practices.

In case where reliable transport protocol such as TCP is used for transport connection between two MIHF peers, TLS [RFC4346] should be used for message confidentiality and data integrity. In particular, TLS is designed for client/server applications and to prevent eavesdropping, tampering, or message forgery. Readers should also follow the recommendations in [RFC4366] that provides generic extension mechanisms for the TLS protocol suitable for wireless environments.

In case where unreliable transport protocol such as UDP is used for transport connection between two MIHF peers, DTLS [RFC4347] should be used for message confidentiality and data integrity. The DTLS protocol is based on the Transport Layer Security (TLS) protocol and provides equivalent security guarantees.

Alternatively, generic IP layer security, such as IPSec [RFC2401] may be used instead of a specific transport layer security for a specific transport.

9. IANA Considerations

This document registers the following TCP and UDP port(s) with IANA:

Keyword	Decimal	Description
-----	-----	-----
ieee-mih-IS	XXX/tcp	Media Independent Handover Information Services
ieee-mih-IS	XXX/udp	Media Independent Handover Information Services
ieee-mih-ES	XXX/tcp	Media Independent Handover Event Services
ieee-mih-ES	XXX/udp	Media Independent Handover Event Services
ieee-mih-CS	XXX/tcp	Media Independent Handover Command Services
ieee-mih-CS	XXX/udp	Media Independent Handover Command Services
Melia, et al.		Expires March 21, 2008

10. Acknowledgements

The authors would like to thank Patrick Stupar for his valuable comments and fruitful discussions.

11. References

11.1. Normative References

[I-D.bajko-mos-dhcp-options]

Bajko, G., "Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Options for Mobility Servers (MoS)", draft-bajko-mos-dhcp-options-00 (work in progress), August 2007.

[I-D.bajko-mos-dns-discovery]

Bajko, G., "Locating Mobility Servers", draft-bajko-mos-dns-discovery-00 (work in progress), August 2007.

[I-D.ietf-dhc-dhcpv6-opt-dnsdomain]

Yan, R., "Domain Suffix Option for DHCPv6", draft-ietf-dhc-dhcpv6-opt-dnsdomain-04 (work in progress), June 2007.

[I-D.ietf-dnsop-dnssec-operational-practices]

Gieben, R. and O. Kolkman, "DNSSEC Operational Practices", draft-ietf-dnsop-dnssec-operational-practices-08 (work in progress), March 2006.

[I-D.ietf-mip6-bootstrapping-integrated-dhc]

Chowdhury, K. and A. Yegin, "MIP6-bootstrapping for the Integrated Scenario", draft-ietf-mip6-bootstrapping-integrated-dhc-05 (work in progress), July 2007.

[I-D.ietf-mipshop-mis-ps]

Melia, T., "Mobility Services Transport: Problem Statement", draft-ietf-mipshop-mis-ps-03 (work in progress), August 2007.

[I-D.ietf-tsvwg-udp-guidelines]

Eggert, L. and G. Fairhurst, "UDP Usage Guidelines for Application Designers", draft-ietf-tsvwg-udp-guidelines-03 (work in progress), September 2007.

[I-D.draft-rahman-mipshop-mih-transport]

Raman, A., Olvera-Hernandez, U., Zuniga, JC., Wafta, M., and Kim, H.W., "Transport of Media Independent Handover Messages Over IP," draft-rahman-mipshop-mih-transport-03 (work in progress), July 2007.

- [RFC1533] Alexander, S. and R. Droms, "DHCP Options and BOOTP Vendor Extensions", RFC 1533, October 1993.
- [RFC1536] Kumar, A., Postel, J., Neuman, C., Danzig, P., and S. Miller, "Common DNS Implementation Errors and Suggested Fixes", RFC 1536, October 1993.

[\[IEEE-802.21\] "Draft IEEE Standard for Local and Metropolitan Area Networks: Media Independent Handover Services," IEEE LAN/MAN Draft IEEE P802.21/D06.00, June 2007.](#)

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
- [RFC2132] Alexander, S. and R. Droms, "DHCP Options and BOOTP Vendor Extensions", RFC 2132, March 1997.
- [RFC2181] Elz, R. and R. Bush, "Clarifications to the DNS Specification", RFC 2181, July 1997.
- [RFC2401] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.
- [RFC2486] Aboba, B. and M. Beadles, "The Network Access Identifier", RFC 2486, January 1999.
- [RFC2988] Paxson, V. and M. Allman, "Computing TCP's Retransmission Timer", RFC 2988, November 2000.
- [RFC3118] Droms, R. and W. Arbaugh, "Authentication for DHCP Messages", RFC 3118, June 2001.
- [RFC3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.
- [RFC3849] Huston, G., Lord, A., and P. Smith, "IPv6 Address Prefix Reserved for Documentation", RFC 3849, July 2004.
- [RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, March 2005.
- [RFC4346] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.1", RFC 4346, April 2006.
- [RFC4347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security", RFC 4347, April 2006.

[RFC4366] Blake-Wilson, S., Nystrom, M., Hopwood, D., Mikkelsen, J., and T. Wright, "Transport Layer Security (TLS) Extensions", RFC 4366, April 2006.

[RFC4787] Audet, F. and C. Jennings, "Network Address Translation (NAT) Behavioral Requirements for Unicast UDP", BCP 127, RFC 4787, January 2007.

11.2. Informative References

Comment [dwg13]: We can add the MIH Transport paper that has been submitted to the Springer journal, if the DT feels that it is appropriate.

Authors' Addresses

Telemaco Melia (editor)
NEC
Email: telemaco.melia@nw.neclab.eu

Gabor Bajko
Nokia

Email: Gabor.Bajko@nokia.com

Subir Das
Telcordia

Email: subir@research.telcordia.com

Nada Golmie
NIST

Email: nada.golmie@nist.gov

Sam Xia
Huawei

Email: xiazhongqi@huawei.com

Juan Carlos Zuniga
InterDigital

Email: j.c.zuniga@ieee.org

Full Copyright Statement

Copyright (C) The IETF Trust (2007).

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, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR 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.

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).