Network Working Group
Internet Draft
Intended status: Informational
Expires: March 27, 2014

M. Liu
Y. Wang
ICT, CAS

September 27, 2013

Distributed Mobility Management: Service Flows Distribution and Handoff Technique based on MIPv6
draft-liu-dmm-flows-distribution-and-handoff-01

Abstract

This document has a normative description of the service flow management technology based on mobile IPv6 (MIPv6). It makes the upgrade of management model in MIPv6 from the entire node granularity to the single service flow granularity. It proposes a distributed mobility management solution, DMIPv6, which is compatible with MIPv6 and takes different mobility management strategies according to the Correspondent Node's position, network conditions and service requirements of different service flows so as to achieve the service flow handoff and transmission path control. The standard also provides route optimization mechanism between the Mobile Node and the ordinary Correspondent Node that doesn't support mobile IPv6.

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), 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/1id-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 27, 2014.

Table of Contents

1. Introduction

This standard proposes a distributed mobility management protocol, DMIPv6, which is compatible with the standard mobile IPv6 protocol. DMIPv6 introduces Distributed Home-Proxy (DHP) and Distributed Home

Address (DHoA) for a Mobile Node (MN) while there are Home Agent (HA) and Home-Of-Address (HoA) already. MN will use DMIPv6 proposed in this document if the DHP and DHoA are available, otherwise the standard mobile IPv6 is used. The deployment of the DMIPv6 could be implemented step by step, with the compatibility to the existing mobile IPv6.

What's more, compared to the standard mobile IPv6 in management model,DMIPv6 could select different DHP for a MN's different service flows.MN takes different management strategy for different service flows according to network conditions and the actual requirements during the move. The introduction of DHP not only reduces the home network congestion and HA load, but also greatly reduces the possible failures in home network and HA, and the bad impacts to the MN. Besides, the MN could achieve optimized transmission path and transmission delay even choosing bidirectional tunnel, because the DHP is located close to the Correspondent Node (CN). For CN that is a server, the introduction of DHP makes it possible for it to enhance its mobility support for its clients without any updates of itself.

2. Conventions and Terminology

2.1. Conventions Used in This Document

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. Terminology

All general mobility-related terms and their acronyms used in this document are to be interpreted as defined in the Mobility Support in IPv6 specification [RFC6275] and in the Proxy mobile IPv6 specification [RFC5213]. These terms include mobile node (MN), correspondent node (CN), home agent (HA), Care-of-Address (CoA), Home-of-Address (HoA), Binding Update (BU), and Binding

Acknowledgement (BA).

In addition, this document uses the following terms:

Distributed Home-Proxy (DHP) is a router near CN, with the function for an extension of the HA, which assigns distributed home address for the MN, receives and forwards the packet between the MN and CN. It plays a role in router optimization and handoff management on service flow granularity.

Distributed Mobile IPv6 (DMIPv6) is a distributed network layer mobility solution compatible with mobile IPv6, which would take different mobility management strategies according to the CN's position, network conditions and service requirements of different service flows so as to achieve the service flow handoff and transmission path control. And the standard will also provide route optimization mechanism between the MN and the ordinary CN that doesn't support mobile IPv6.

Distributed Home Address (DHoA) is a home address that MN gets from the corresponding DHP for establishing a connection with CN so as to achieve the service flow handoff and transmission path control.

3. Basic Framework

Distributed Mobile IPv6(DMIPv6), which is a distributed mobility management architecture compatible with Mobile IPv6, introduces Distributed Home-Proxy(DHP) to the existing Mobile IPv6 architecture. In DMIPv6, DHP can be deployed in subdomain of each network.

DHP is implemented based on HA, and multiple DHPs independent of each other can be deployed in the same domain. The DHP is deployed the same style as the HA and general router. Under such condition, MN can select one or more DHPs according to the state of DHP and service demand. In general, one DHP is enough, but multiple DHPs can be selected to backup or improve concurrent performance. Figure 1 shows the basic architecture of DMIPv6:

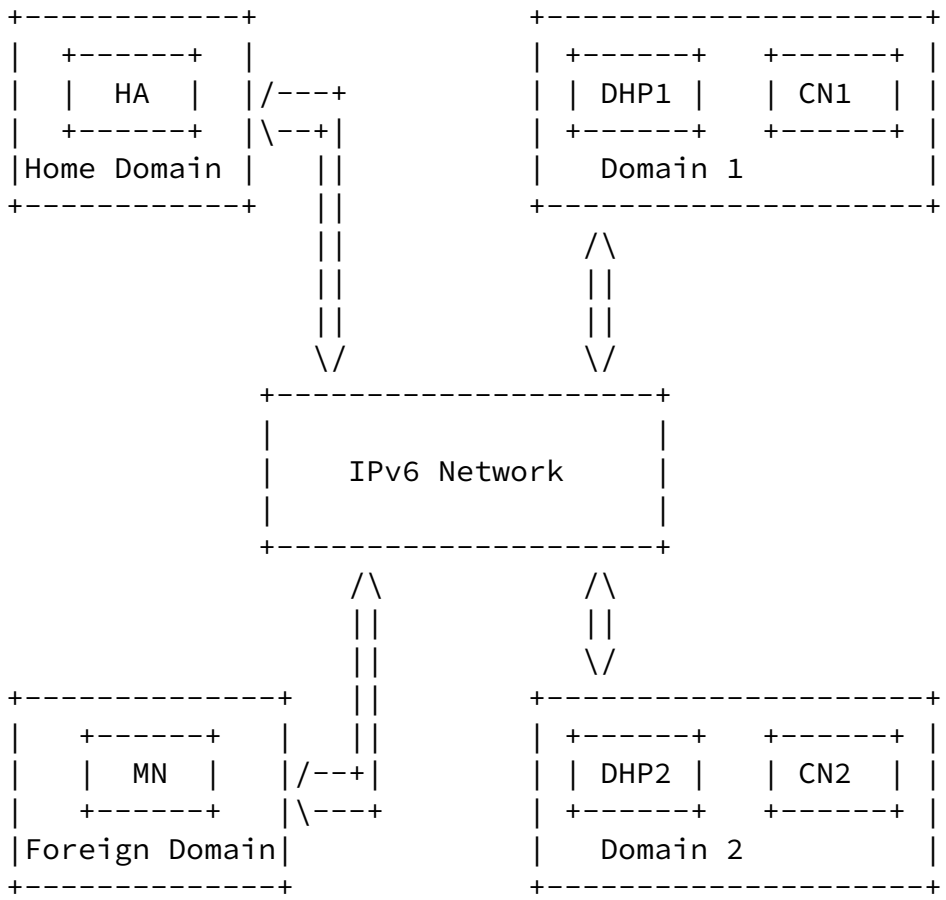


Figure 1 Architecture of Service Flow Distribution and Handoff Management

As Figure 1, there exists multiple independent DHPs in the CN

network, and MN can selecte one of them as the proxy server. The introduction of DHP greatly decreases the MN's dependence on HA, and can also optimize the transmission path and transmission delay.

When MN moves to a new link, the DHP can act as a proxy and forward the data for it. According to the deployment style and the available equipment's support to DMIPv6, MN will perform DMPv6 if the DHP and DHoA are available, otherwise the standard mobile IPv6 is used.

4. Message Types

In this standard, majority of equipments need to complete a series of interactions to transmit information. The following messages are extended from the standard ICMPv6 messages. All extension types of the extended ICMP messages are different from those of standards defined by international organizations like IETF. If collisions occur in the future, values of corresponding message types should be adjusted according to the actual situation.

4.1. Messages Between MN and HA

Messages between MN and HA include binding update message (BU) sent when MN moves and binding acknowledgment messages (BA). This standard is compatible with standard mobile IPv6 protocol. For detailed information about the above messages, refer to the IETF RFC 6275.

4.2. Messages Between MN and CN

Messages between MN and CN include binding update message (BU) sent when MN updates its CoA-address and binding acknowledgment messages (BA). This standard is compatible with standard mobile IPv6 protocol. For detailed information about the above messages, refer to the IETF RFC 6275.

4.3. DHP Query Message

DHP query message is used by MN to perform the DHP query and selection operations. This standard proposes 3 kinds of DHP query method. Corresponding query methods are depicted as follow:

4.3.1. Dynamic DHP Discovery Query/Acknowledgement Message

In this method, DHP query messages are sent to corresponding network

to request response directly. This procedure is similar to "dynamic home agent address discovery mechanism" in MIPv6. When adopt this method, all DHPs in a common CN domain should maintain the status information of other DHPs, i.e. every DHP maintains a list of information about all DHPs in current domain.

When comes to specific operation, MN query the DNS to get the DHP anycast address in the CN domain, and then send dynamic DHP discovery query message to that anycast address. According to the routing protocols, the topologically nearest DHP from the mobile node may receive the request message and then respond to it. Status information of all DHPs in the CN domain should be included in the reply message. MN can perform the HP selection based on this state information. This approach is the active query mode of MN.

4.3.1.1. DHP Query Message

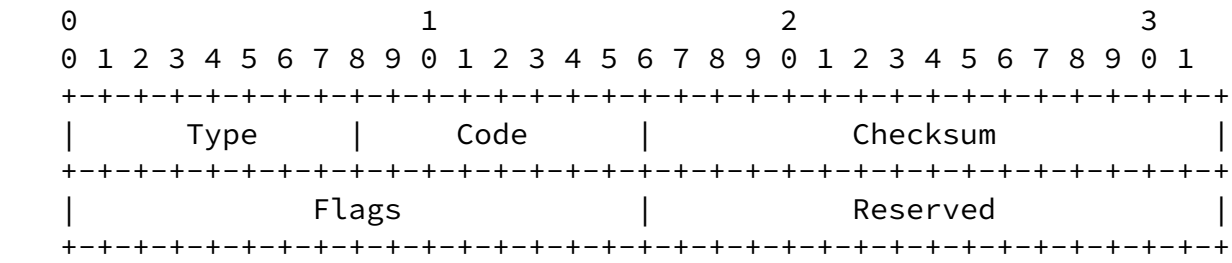


Figure 2 Dynamic DHP Discovery Query Message

o Source address: IPv6 address of the interface sending this message

o Destination address: anycast address of DHP in the CN domain

o Hop limit: 255

o Authentication Header: sender should contain this header field

when security association of IP authentication header present between sender and receiver.

o ICMP fields:

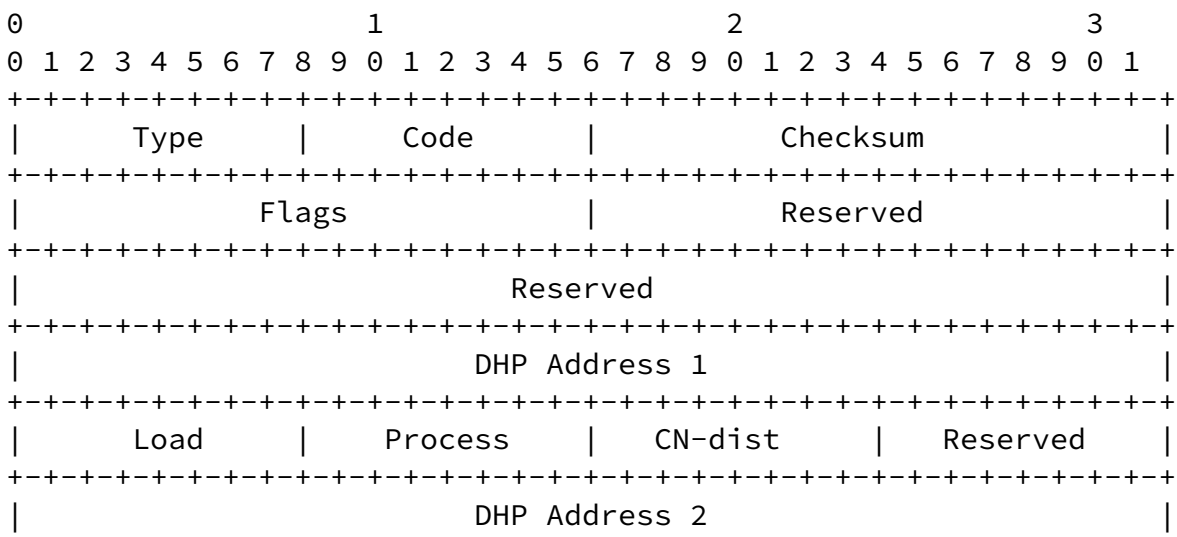
Type 160

Code 0

Checksum ICMP checksum

Reserved Reserved for future use. The value must be initialized to zero by the sender, and must be ignored by the receiver.

4.3.1.2. DHP Acknowledgement Message



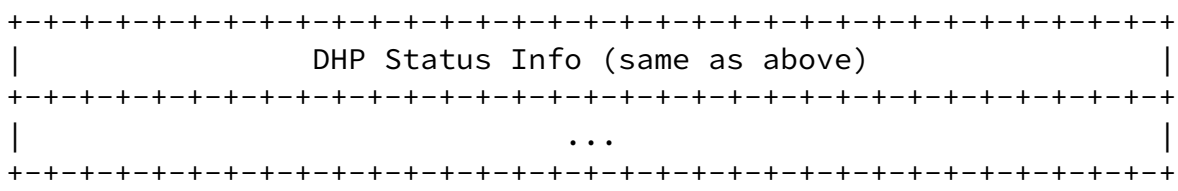


Figure 3 Dynamic DHP Discovery Acknowledgement Message

o Source address: IPv6 address of the interface sending this message

o Destination address: IPv6 address of MN

o Hop limit: 255

o Authentication Header: sender should contain this header field when security association of IP authentication header present between sender and receiver. Source address: IPv6 address of the interface sending this message

o ICMP fields:

Type 161

Code 0

Checksum ICMP checksum

Reserved Reserved for future use. The value must be initialized to zero by the sender, and must be ignored by the receiver.

o Options: Sender must contain following options in the request message:

DHP proxy server address: local IPv6 address of the sender. This address should be a DHP network interface address. If there exists more than one DHP in current network domain, information of all DHPs should be sequentially contained in the options part.

DHP status information: the current DHP state information should include load conditions, process capability, distance from CN and so on.

4.3.2. Multicast Request DHP Query/Acknowledgement Message

Through this method, IP address and status information of DHP in the CN domain can be obtained by sending multicast request message. This method requires all DHPs from one CN domain form a multicast group, then share a multicast address.

Firstly MN query the DNS to get the DHP multicast address in the CN domain, and then send query message to that multicast address. Since then, all DHPs in the multicast group will reply acknowledgement message to the MN which also contains DHP address and other status information. This also is a MN active query method.

4.3.2.1. DHP Query Message

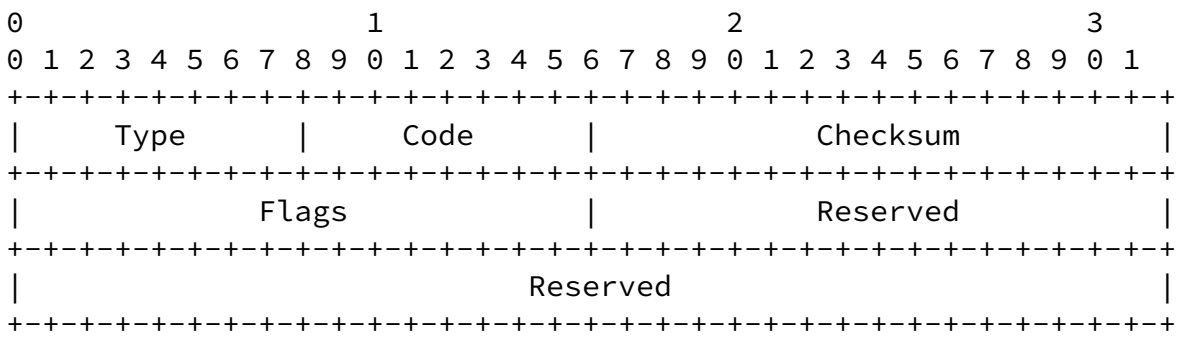


Figure 4 Multicast Request DHP Query Message

- Source address: IPv6 address of the interface sending this message
- Destination address: DHP multicast address in the CN domain
- Hop limit: 255

- Authentication Header: sender should contain this header field when security association of IP authentication header present between sender and receiver.
- ICMP fields:

Type 162

Code 0

Checksum ICMP checksum

Reserved Reserved for future use. The value must be initialized to zero by the sender, and must be ignored by the receiver.

4.3.2.2. DHP Acknowledgement Message

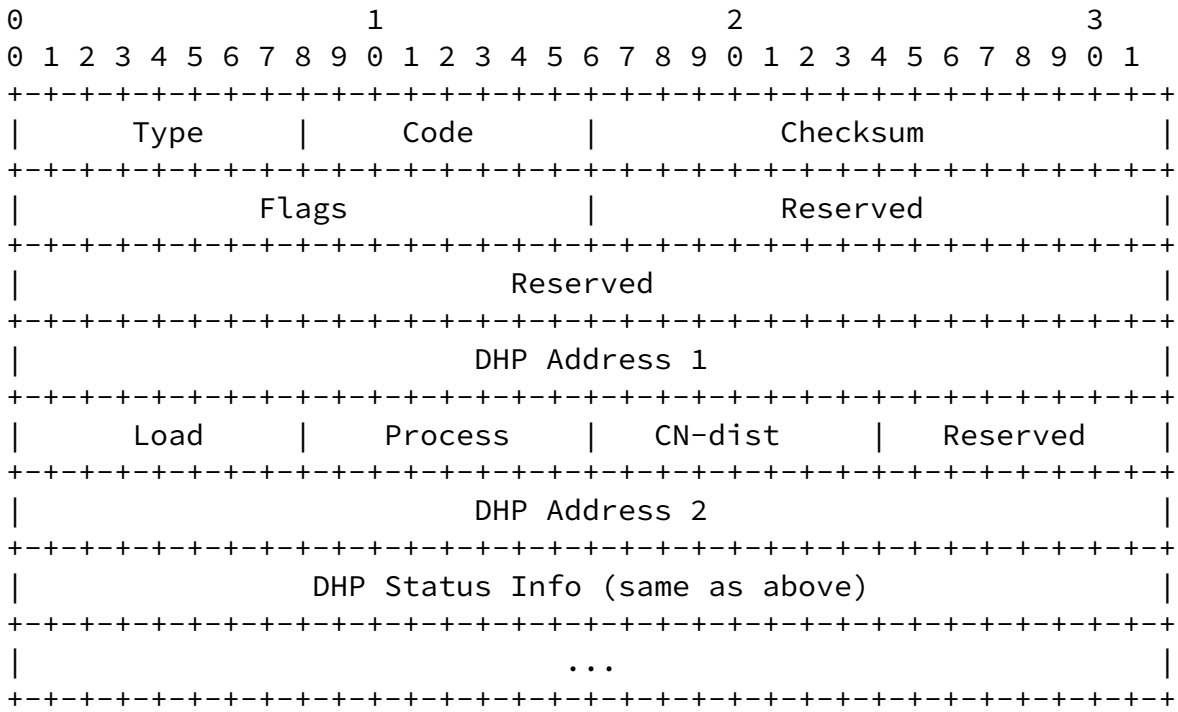


Figure 5 Multicast Request DHP Acknowledgement Message

o Source address: IPv6 address of the interface sending this message

o Destination address: IPv6 address of MN

o Hop limit: 255

o Authentication Header: sender should contain this header field

when security association of IP authentication header present between sender and receiver.

- o ICMP fields:

  Type 163

  Code 0

  Checksum ICMP checksum

  Reserved Reserved for future use. The value must be initialized to zero by the sender, and must be ignored by the receiver.

- o Options: Sender must contain following options in the request message:

  DHP proxy server address: local IPv6 address of the sender.

  DHP status information: state information of this machine, contains load conditions, process capability, distance from CN and so on.

  The distance here is as same as defined above. Depending on the routing protocols, it may be the number of hops or delay in the actual network topology.

4.3.3. Specific Server DHP Query/Response Message

The DHP selection can also use special DHP management server to complete. In actual circumstances, we can set global DHP management server to maintain all the DHP status information in the real-time network.

MN can use DNS to query the DHP management server's address, and then send the corresponding DHP query messages to the server, the server sends the request a timely response.

In accordance with different handling ways of MN, these methods can be divided into two categories: active and passive queries.

4.3.3.1. Active Query

In this way, the MN sends a request message to DHP management server, the server will send all of the information to the MN terminal, for MN itself to make a choice. It is called MN active query.

4.3.3.1.1. DHP query message

The DHP query message in this way is the same with the corresponding query message in 4.3.1, the difference is that the message type code is 164 and the destination address is DHP management server address.

4.3.3.1.2. DHP Query Response Message

DHP query response message in this way is the same with the corresponding query response message in 4.3.1, the difference is that the message type code is 165 and the destination address is DHP management server address.

4.3.3.2. Passive Query

Different from the above mentioned active query, in the passive way, the MN sends a request message to the DHP information management server, the request message further includes business type that MN initiate currently and other relevant requirements of DHP (including the ability to handle, the size of the load, the routing hops requests and so on. According to the requirements of MN, DHP information management server complete DHP preferred choice for MN in predetermined rules , then the selected DHP information response to MN. The Message format is as below:

4.3.3.2.1. DHP Query Message

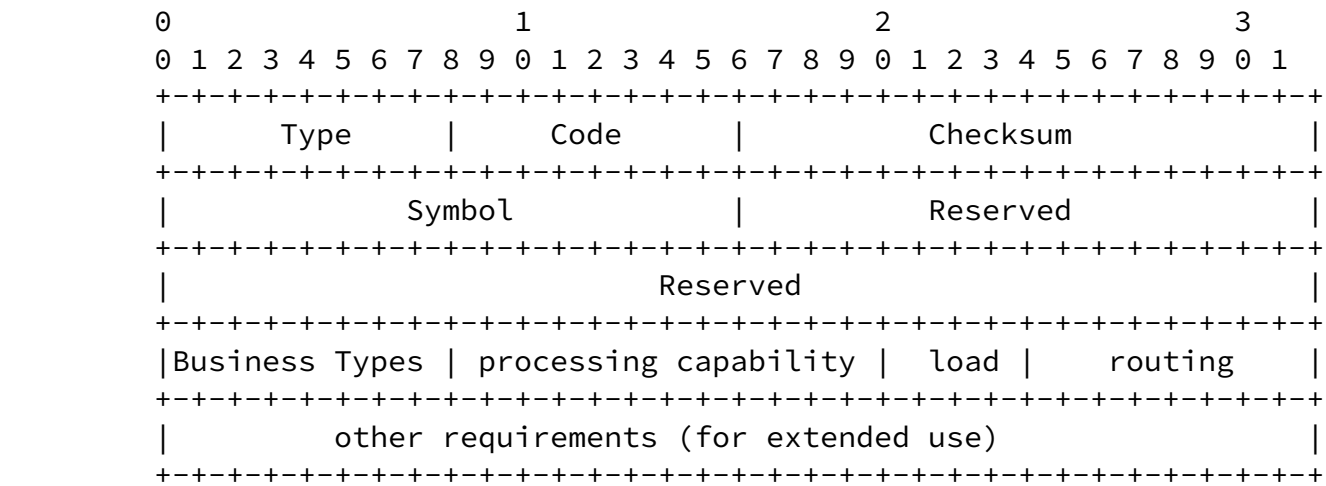


Figure 6 Specific Server DHP Query Message

o source address:IPv6 address of MN interface which send this message

- o destination address: DHP information management server address in CN domain
- o hop limit: 255
- o authentication header: if exists Security Association of IP authentication header between sending and receiving peer , the sending peer should include this header field
- o ICMP field:

  type 164

  code 0

  checksum ICMP checksum.

  retained this field is not used. The sender must initialize it to 0, the recipient must ignore it.

- o Options: the sending node must contain the following options in the request message sent:

  MN business requirement description: include business type to be initiated, processing capability, load requirements and the routing request and so on, users can also make further needs customization expansion according to the actual situation.

4.3.3.2.2. DHP Query Response Message

DHP query response message in this way is the same with the corresponding query response message in 4.3.2, the difference is that the message type code is 165 and the destination address is DHP management server address.

In particular, the CN can act as a DHP management server if it makes some upgrades and extensions. For example, the CN needs to be able to receive the DHP routing announcements of its domain and record the relevant information, while the normal CN doesn't have this feature.

4.4. DHoA Request/Response Message

After choosing DHP, MN needs to apply a specific DHoA from the selected DHP, which is completed by sending a message of DHoA application. Based on the domain prefix information and address generation algorithm, DHP generate the corresponding DHoA address,

and then back the address information to the MN, message format is shown in Figure 7 and figure 8.

4.4.1. DHoA Application Message

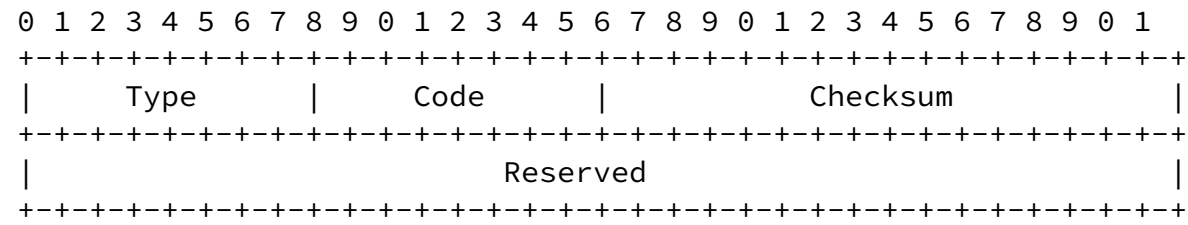


Figure 7 DHoA Request Message

- o source address:IPv6 address of MN interface which send this message
- o destination address: DHP information management server address in CN domain
- o hop limit: 255
- o authentication header: if exists Security Association of IP authentication header between sending and receiving peer , the sending peer should include this header field
- o ICMP field:

  type 166

  code 0

  checksum ICMP checksum.

  retained this field is not used. The sender must initialize it to 0, the recipient must ignore it

4.4.2. DHoA Request Response Message

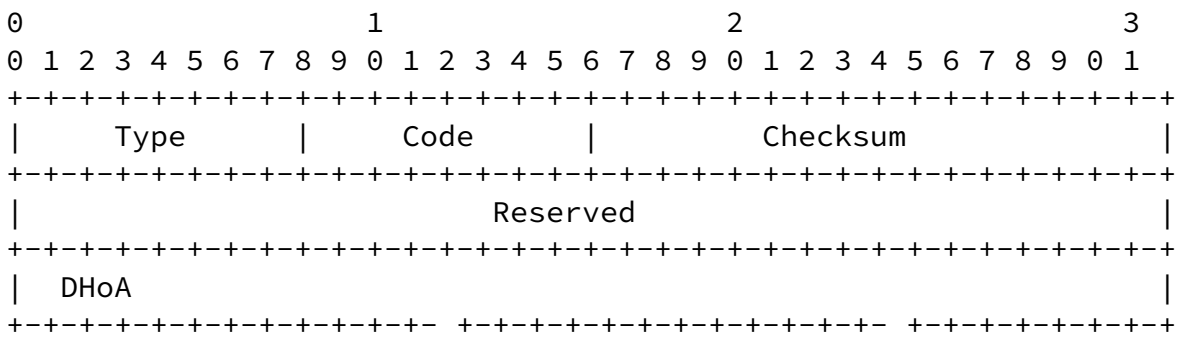


Figure 8 DHoA Request Response Message

o source address:IPv6 address of MN interface which send this message

o destination address: DHP information management server address in CN domain

o hop limit: 255

o authentication header: if exists Security Association of IP authentication header between sending and receiving peer , the sending peer should include this header field

o ICMP field:

type 167

code 0

checksum ICMP checksum.

retained this field is not used. The sender must initialize it to 0,the recipient must ignore it

The transmitting node must contain the following options in the request message

DHoA address: distributed by DHP for MN

4.5. DHP Binding Update/Confirmation Message

In this standard, if the DHP service is enabled, then when MN moves, we need to judge whether to continue the current business, then make a DHP binding update for current CoA address. This binding update

message format is similar with the binding update message of BU in MIPv6, but needs extend a byte to store the corresponding business flow port number in its message extension headerto distinguish different traffic flows. The message format is shown in Figure 9. Binding update confirm message between DHP and MN is the same with BA in MIPv6. The message format can be seen in IETF RFC6275.

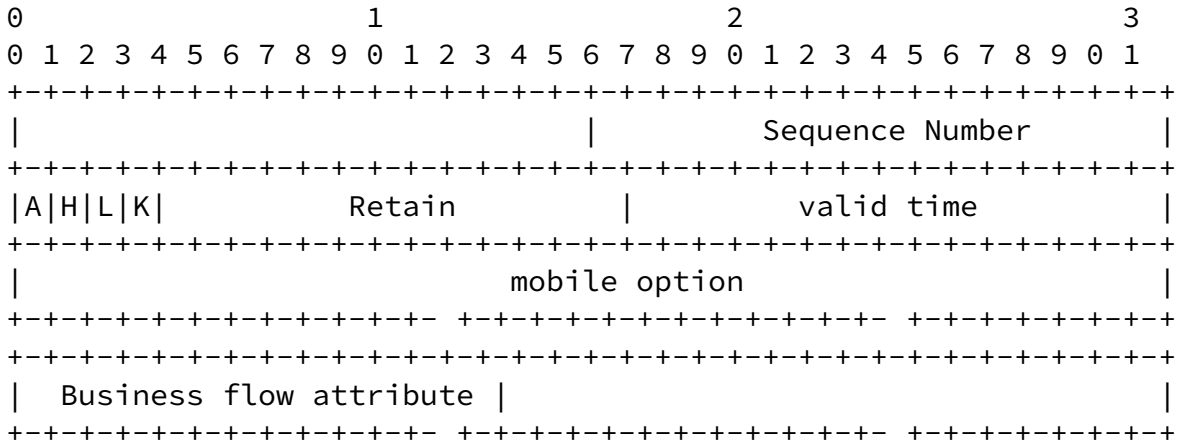


Figure 9 DHP Binding Update Message

o sequence number: same with the BU message regulations of standard MIPv6

o standard of related bits: same with the BU message regulations of standard MIPv6

- o valid time: same with the BU message regulations of standard MIPv6

- o retention

- o mobile options: same with the BU message regulations of standard MIPv6

- o extension field

- o The sending nodes contains the following options in the request message:

  Business flow attribute, business port number when initiating business locally, used to identify a service flow between the host and the corresponding DHP.

5. DMIPv6 Workflow

This standard provides a distributed MIPv6 compatible solution named DMIPv6 which enables service flow distribution and handoff management. We assume that MN has already moved to foreign network from home network here, thus MN should has DHoA address and CoA address, or HoA address and CoA address if the DMIPv6 is unavailable. We introduce the main processing workflow of the technical proposal in this standard, with 2 steps: the processing procedure of the new service flows and the MN handoffs, which corresponds to the service flow distribution and mobility handoff management.

5.1. The Processing Workflow of New Service Connection

It is the processing workflow in the DMIPv6 when there is a new service connection between MN and CN. The detailed procedure is introduced as follows, and the related message interaction diagram is introduced in Figure 10. The detailed message format is showed in Chapter 4.

5.1.1. The Decision of the Mobility Requirement of Service Flow

MN decides whether the service flow needs mobility support according

to the service type of the new connection request. The standard of this decision can refer to the requirement of the MN itself and set the decision rule in advance:

If MN decides that the service flow needs mobility support, then it goes to section 5.1.2; or MN will use the old CoA address to establish the connection with CN.

5.1.2. The Requirement Decision Started by the New Connection

Mobile nodes decides whether the new connection request is started by the local MN, if it is then MN goes to section 5.1.3; or MN uses HoA address to establish the connection with CN.

5.1.3. DHP Query

MN queries the DHP address and status of CN's network for its service flow, and there are 4 ways to realize the DHP query, which can be found in section 4.3. Figure 10 provides the message interaction diagram for different ways of query. Figure 10(a) is for the query of dynamic discovery and multicast request in section 4.3.1 and 4.3.2. Figure 10(b) is for the query which introduces DHP management server or uses CN in section 4.3.3 and 4.3.4.

5.1.4. DHP Selection

After the DHP query, MN needs to make the DHP selection. For the active query introduced in section 4.3, MN will decide which DHP serves itself according to different targets. The actual decision can be made in MN in advance, such as the distance to CN, processing ability, related workload information, etc. As for the passive query, MN can directly achieve the DHP address and the corresponding information.

Besides, during the process procedure of this standard, DHP always knows MN's location information and must ensure to avoid MN's information disclosure. As a result, the DHP selection introduces the selection of DHP's security mechanism. Each DHP will make its security warranty as one of the most important status information and can provide hierarchical classification on occasion. As for the active query in section 4.3, MN can decide to select which security level of DHP to serve it; as for the passive query, MN needs the

related management server to make selection policy and directly achieve the related information. It is preferred that these security requirements are considered as an integral part of the DMM design.

5.1.5. DHoA Address Application

MN will send the corresponding address application message to the DHP after deciding which DHP serves it. DHP can create the required DHoA message according to the address creation algorithm and local prefix information, and then inform the MN of this DHoA. At the same time, it will bind the allocated DHoA with MN's current address.

5.1.6. Establishing the Communication Connection

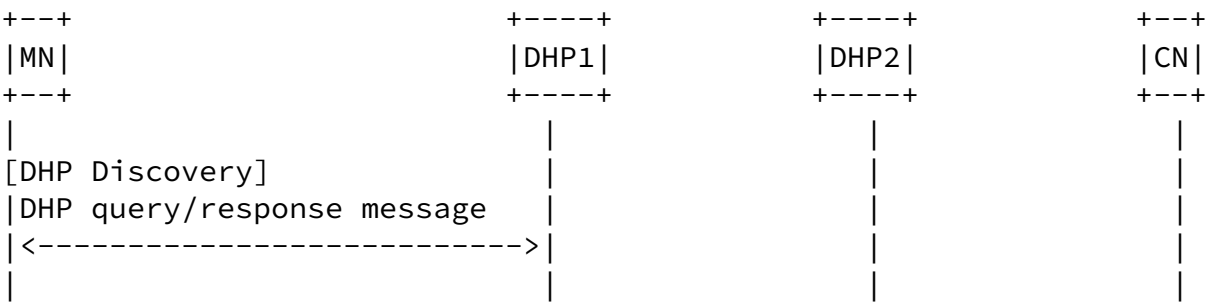
MN uses the queried DHoA to establish the connection with CN, and at the same time, DHP will save the information of DHoA and MN's address. It maintains a mapping table of the DHoA, MN and a service connection, and this mapping table is used for the management of mobility handoff.

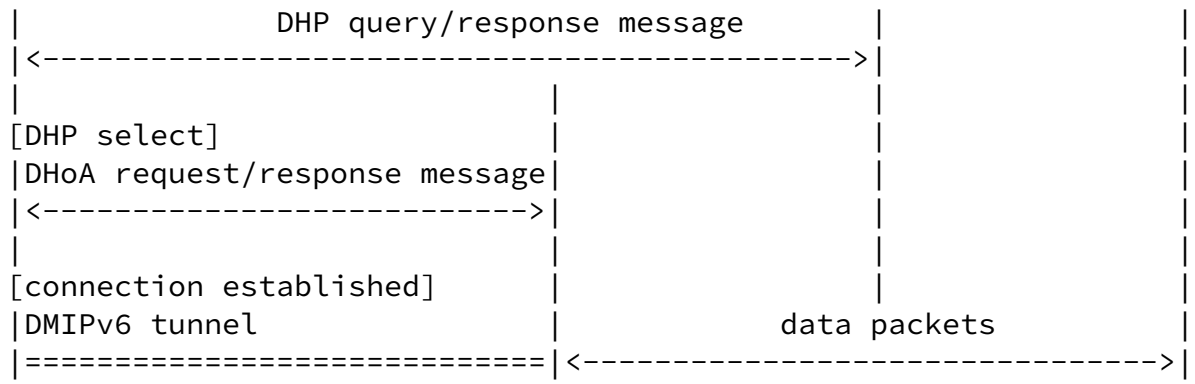
A notice is that, MN will use HoA to establish the connection with CN if the DHP query is failed in DHP, which means no DHP is found to serve the current MN. Later workflow is the same as that defined in MIPv6.

5.1.7. Confirming the Communication Mode

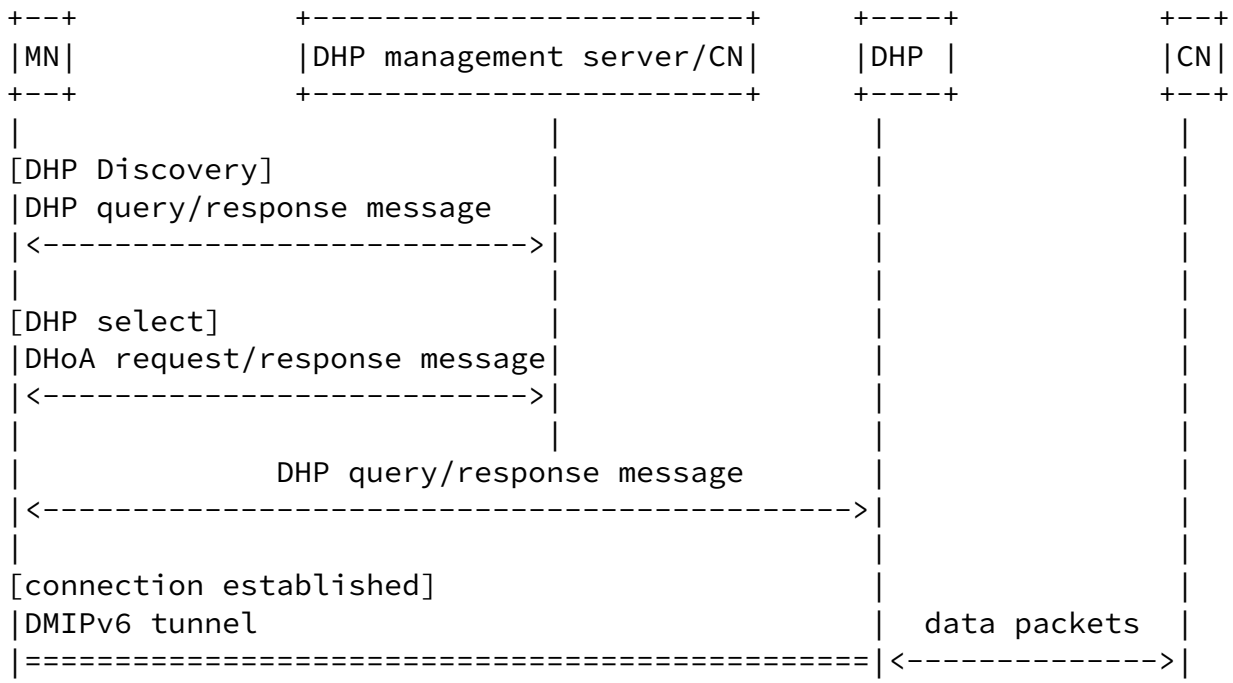
MN needs to decide whether to use routing optimization mode or bi-direction tunneling mode according to the situation how CN supports the routing optimization. MN will use routing optimization mode for

the CN which supports routing optimization; or it will use the bi-direction tunneling mode. After confirming the communication mode, MN will start data transmission with CN.





(a)



(b)

Figure 10 New Service Connect Message interaction

5.2. The Processing Workflow when MN Moves

In the communication between MN and CN, when MN moves, first need to judge whether the DHP has been enabled. For the enabled DHP, to carry on the following steps, otherwise according to the standard MIPv6

protocol to execute.

5.2.1. The Qos Conditions Identification of A New Access Network

MN According to the Qos condition of a new access network, business priorities and the Qos requirement to judge whether the Qos requirement has been satisfied and whether the business should be continue. Specific we can achieve the condition of network interface, topology-aware, business flow parameter estimation of available bandwidth measurement, network packet loss rate and throughput to implement the requirement.

5.2.2. Handoff Management

For the service streams need to continue communication, will perform the following operations:

1. MN bind the CoA address and the port of the flow with the selected DHP.

2. DHP Replies binding update confirmation.

3. DHP performs proxy functions, intercepts the packets of CN sent to the MN existing home network, through the establishment of the tunnel DHP sent the packets to the new access network of MN.

4. For the CN of supporting the route optimization function, MN binds the new CoA address with CN, begin to communicate with CN until the CN's reply has been accepted. For the CN of not supporting the route optimization function, MN will carry on communication and transmission by bidirectional tunnel.

For the service streams that don't need to continue communication and Qos has no requirement. MN will stop the flow and will not bind the new CoA address with DHP.

For different businesses, MN can take different interrupt. Specifically, according to different transport layer protocols, and

its own characteristics MN will take different message exchange or notification.

6. Security Considerations

This standard is compatible with MIPv6, in the meantime, DHP equipments are added to it. Its basic procedures and messages exchanging schemes are similar to MIPv6, which lead to similar security issues like MIPv6's, including the security of dynamic DHP discovery, addresses binding and tunnels setting up between MN, HA, and CN. Detailed information in IETF RFC 6275.

This standard is compliant with standard MIPv6, which means MN still has HoA in home domain. When MN is initiating a new connection with DMIPv6, it will first apply for DHoA. According to MIPv6, MN's HoA is permanent during in its travelling, so CN always knows its HoA. So CN will see MN travel from home domain to network with same prefix like DHoA. In addition, DHP is commonly in CN's domain and is close to CN, so CN will identify that MN has already moved to place near itself. In the whole process, CoA is hidden from CN, which avoid some security risks to some extensions.

In the standard, DMIPv6 will be chosen when MN initates connection first. So, if there are random or periodic pseudo-connections, the process of DHP lookup and DHoA application will be triggered, which will impose heavy burden on MN and DHP. In fact, it's likely that from trojans and hackers' attacks. Under such circumstance, MN should use secured authentication to limit the number of pseudo-connections, and set bidirectional security mechanisms in DHP.

When DMIPv6 is turned on, DHP will always know MN's location, and can send the information to third parties, while those requests for location may be ill-intended. So, DHP needs to build enough security mechanisms to guard MN's information. Whether DHP has security mechanisms will be an important condition in MN's inqury to DHP. Detailed information see 5.1.4.

7. IANA Considerations

This document proposes 4 DHP query methods, and 8 message types totally for them:

- The Dynamic DHP Discovery Query Message, and the Dynamic DHP Discovery Acknowledgement Message, described in Section 4.3.1

- The Multicast Request DHP Query Message, and the Multicast Request DHP Acknowledgement Message, described in Section 4.3.2

- The Specific Server DHP Query Message, in Section 4.3.3.1.2
- The DHoA Request Message, in Section 4.4.1
- The DHoA Request Response Message, in Section 4.4.2
- The DHP Binding Update Message, in Section 4.5

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2460] Deering, S., "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, November 1997.

[RFC4862] Thomson, S., Narten, T. and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, September 2007.

[RFC5944] Perkins, Ed., C., "IP Mobility Support for IPv4, Revised", RFC 5944, November 2010.

[RFC6275] Perkins, Ed., C., Johnson, D., and J. Arkko, "Mobility Support in IPv6", RFC 6275, July 2011.

[RFC5380] Soliman, H., Castelluccia, C., ElMalki, K., and L. Bellier, "Hierarchical Mobile IPv6 (HMIPv6) Mobility Management", RFC 5380, October 2008.

8.2. Informative References

[RFC5213] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.

[RFC5026] Giaretta, G. Kempf, J. and V. Devarapalli, "Mobile IPv6 Bootstrapping in Split Scenario", RFC 5026, Oct 2007.

[NTMS2008]Bertin, P., "A Distributed Dynamic Mobility Management Scheme designed for Flat IP Architectures.", NTMS'2008, November 2008.

[I-D. yokota-dmm-scenario]

Yokota, H., Seite, P., Demaria, E., and Z. Cao, "Use case scenarios for Distributed Mobility Management", draft-yokota-dmm-scenario-00 (work in progress), October 2010.

Authors' Addresses

Min Liu
Institute of Computing Technology, Chinese Academy of Sciences,
No.6 Kexueyuan South Avenue, Zhongguancun, Beijing 100190, China
Email: liumin@ict.ac.cn

Yuwei Wang
Institute of Computing Technology, Chinese Academy of Sciences,
No.6 Kexueyuan South Avenue, Zhongguancun, Beijing 100190, China
Email: wangyuwei@ict.ac.cn