NEMO Working Group
Internet-Draft
Expires : January 9, 2006

H. Morioka
ROOT Inc.
July 2005

Mobile Router Cooperation Protocol
draft-morioka-nemo-mrcoop-00.txt

Status of this Memo

Copyright Notice

Abstract

This protocol intended to provide cooperation between mobile routers in a mobile network. A mobile network is usually connected to the Internet through mobile routers with wireless interfaces. Link quality of the wireless interface changes frequently and rapidly. In case of several mobile routers in a mobile network, MNN should use the MR that has the best link quality. This protocol makes all MRs in a mobile network share link quality of MRs each other. Propagation of routing information in a mobile network is not out of sight of

this draft.

1. Introduction

This protocol intended to provide cooperation between mobile routers in a mobile network. A mobile network is usually connected to the Internet through mobile routers with wireless interfaces. Link quality of the wireless interface changes frequently and rapidly. In case of several mobile routers in a mobile network, MNN should use the MR that has the best link quality. This protocol makes all MRs in a mobile network share link quality of MRs each other. Propagation of routings in a mobile network is outside of scope of this draft.

MR sends a packet, which is called "Link Metric Message", periodically to all other MRs in the same mobile network. The packet consists of link metrics with the interface identifier, the timestamp, prefixes belonging to the MR and the hash value of the packet. The link metric is decided from the link quality and the pre-configured preference value. All MRs have a link metric table which maintains link metrics of all interfaces of all MRs in the same mobile network. When a MR receives a Link Metric Message, the MR updates the link metric table and compare link metrics of all interfaces. The MR selects a interface which has the largest metric. The MR that has this interface sends binding update to the home agent with all prefixes of the mobile network. And all routers should work as this MR is the gateway by some routing protocols.

2. Terminology

The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14, RFC 2119 [1].

Network Mobility - related terminology is defined in [2] and [3]. This document in addition defines the following terms.

Mobile Network Prefix

An IPv6 prefix delegated to a Mobile Router and advertised in the Mobile Network. More than one Mobile Network Prefix could

be advertised in a Mobile Network.

3. Overview of the protocol

The MR has a list of MRs which may be connected to the same mobile network. The MR sends the link metric message that includes the link quality of interfaces of the MR to other MRs periodically. All MRs in the mobile network share the link metrics by the link metric messages and maintain the link metric table by each MR. The MRs in the same mobile network selects the MR that has the largest link metric and make it as the gateway. Propagation of the routing in the mobile network is not considered in this draft. But the routing can change rapidly, so some routing protocols which work fast enough should be used.

The MRs also exchange the prefixes of the mobile networks. So the protocol supports connection and split of multiple mobile networks autonomously which will occur in reassemble of train, for example.

4. Transport protocol

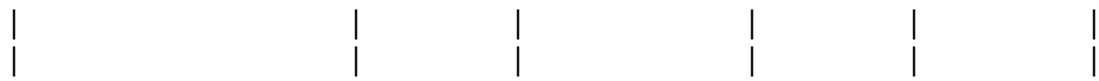
This protocol uses UDP.

5. Behavior of MR

5.1. Link Metric Table

Each MR maintains a link metric table. The link metric table contains the link metrics, the interface identifiers, the IP addresses of the ingress interface of MRs, the mobile network prefixes and the last updated time. Each item in the table expires in 300ms. For example, the link metric table will be as shown below.

IP address of MR	Prefix	Interface Identifier	Link Metric	Updated Time



5.2. Sending Link Metric Message

The Link Metric Message (LMM) is sent by the MR periodically. The interval of messages MUST NOT be greater than 300ms and SHOULD be less than 100ms unless receiving ICMP Destination Unreachable Message[4]. If the MR receives ICMP Destination Unreachable Message, the MR MAY increase the interval of the messages up to 1 second.

Each LMM includes link metrics with the interface identifier, a timestamp, prefixes belonging to the MR and the hash value of the packet.

LMM MUST include link metrics of all available egress interfaces of the MR. An available interface means that it can communicate with the point of attachment to the Internet with IP. Typically the interface link is up and at least one IP address are assigned. Link metrics of unavailable interfaces, which cannot communicate by IP, MAY NOT be included in the LMM. Detail of the link metric is described in later section.

An interface identifier is 16-bit unsigned integer. This is for identification of interfaces of the MR sending the LMM. Each interface in the MR MUST have a different interface identifier. The interface identifier SHOULD NOT be changed during operation.

A timestamp is adjusted to the clock of the MR that receives the LMM.

A LMM can include multiple prefixes which belongs to the MR.

A hash value is calculated from the LMM itself.

5.3. Receiving Link Metric Message

When the MR receives a LMM, the MR work as described in this section.

5.3.1. Checking Timestamp

At first, the MR compare the timestamp of the LMM and it in the link metric table. If the timestamp of the LMM is equal or smaller than the timestamp in the link metric table, the LMM is silently discarded.

If the difference between timestamp of the LMM and the clock of the MR is greater than 5 seconds, the MR sends the Time Adjusting Message described in later section to the sender of the LMM and discards the LMM.

5.3.2. Checking Hash Value

The MR compares the hash value according to the hash type. If the hash value does not match, the message is silently discarded.

5.3.3. Updating the Link Metric Table

When the MR receives a LMM, the MR MUST updates the link metric table

and selects the interface that has the largest metric, that is called primary interface, immediately. If multiple interfaces have the largest metric, the primary interface is selected as following. Upper condition has higher priority.

- The previous primary interface
- The interface belongs to a MR which has shorter mobile network prefix length
- The interface belongs to a MR which has larger IP address as 128-bit unsigned integer
- The interface which has smaller interface identifier

5.3.4. Changing Gateway

If the primary interface is changed from the previous primary interface, the MR MUST work as following.

The MR that has the primary interface MUST send the Binging Update to the home agent and announce to the mobile network by some routing protocols as the MR is the gateway. The Binding Update contains all

mobile network prefixes.

All other MRs also announce to the mobile network by some routing protocols as the MR that has the primary interface is the gateway.

The MR that has the previous primary interface MUST stop sending Binding Update.

5.4. Sending Time Adjusting Message

If the difference between timestamp of the received LMM and the clock of the MR is greater than 5 seconds, the MR MUST send the Time Adjusting Message to the sender of the LMM. The timestamp field of the Time Adjusting Message is set to the clock of the sender.

5.5. Receiving Time Adjusting Message

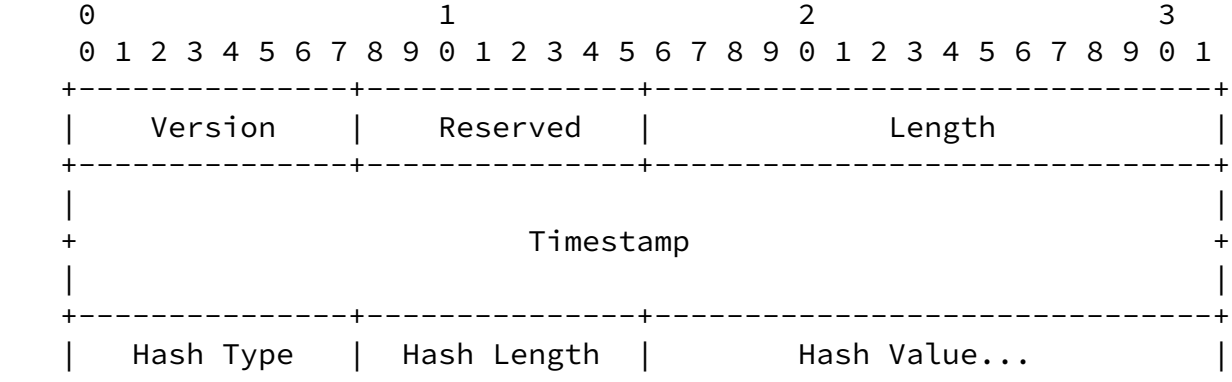
If the MR receives Time Adjusting Message (described below) from the correspondent MR, the MR SHOULD adjusts the timestamp after checking the hash value.

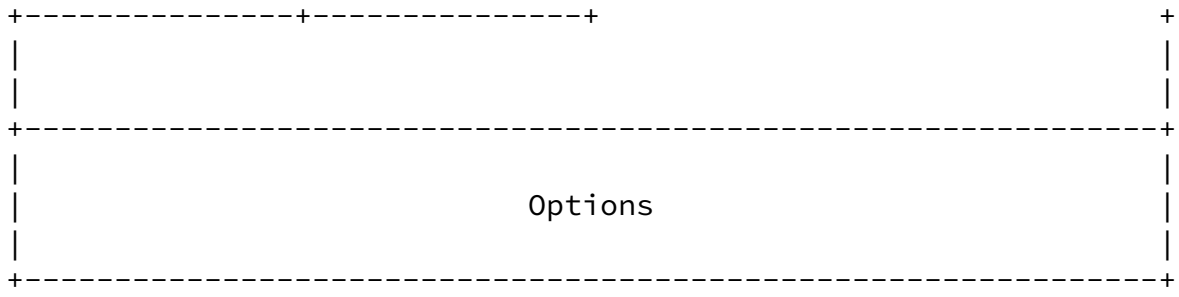
If the hash value does not match, the message is silently discarded.

6. Message Format

6.1. Link Metric Message

The format of Link Metric Message is described below.





Version
8-bit unsigned integer indicates the version of this protocol. Set to 1.

Reserved
This field is unused for now. The value MUST be initialized to 0 by the sender and MUST be ignored by the receiver.

Length
16-bit unsigned integer indicates the length in octets of the message, including the version, reserved and the length field.

Timestamp
64-bit unsigned integer indicates the time of generating the message. The MR MUST set this field to a 64-bit value specified by the Network Time Protocol[5]. This value MUST be greater than the timestamp value of any messages previously sent to the receiver.

Hash Type
8-bit unsigned integer indicates the type of hash algorism. The values shown below are decimal values.
1 keyed-MD5

keyed-MD5 MUST be supported by all MRs.

Hash Length
8-bit unsigned integer indicates the length of the hash value field in octets.

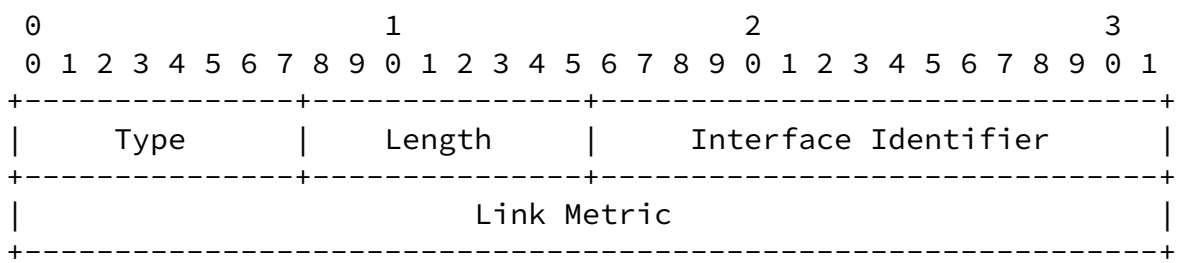
Hash Value
This field is hash value generated by the method indicated in

the hash type field and the length is indicated in the hash length field.

Options
The options field follows the hash value field.

6.1.1. Link Metric Option

The format of the link metric option is described below. Multiple link metric options can be included in a LMM.



Type
Set to 1.

Length
8-bit unsigned integer indicates the length in octets of this option, including the type and the length field. Set to 8.

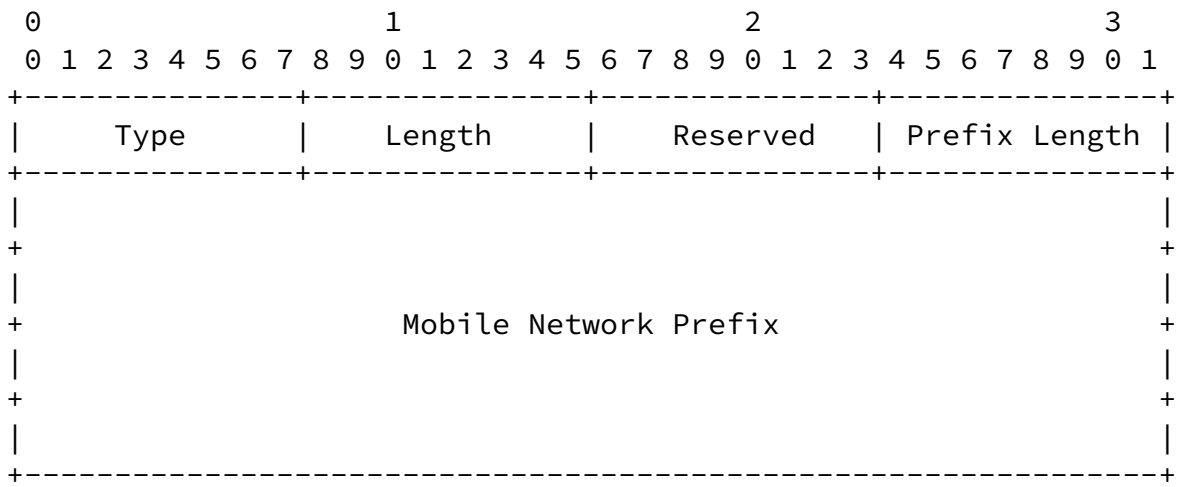
Interface Identifier
16-bit unsigned integer indicates the interface of the MR. This value is specified by the sender MR.

Link Metric
32-bit unsigned integer indicates the metric of interface. This value is generated by the method described in later section.

6.1.2. Prefix Option

The format of the prefix option is described below. Multiple prefix

options can be included in a LMM.



Type
Set to 6.

Length
8-bit unsigned integer indicates the length in octets of this option, including the type and the length field. Set to 20 in decimal.

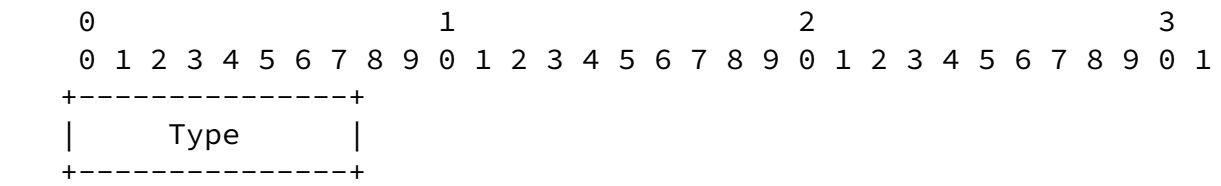
Reserved
This field is unused for now. The value MUST be initialized to 0 by the sender and MUST be ignored by the receiver.

Prefix Length
8-bit unsigned integer indicates the prefix length of the IPv6 prefix contained in the option.

Mobile Network Prefix
A 128-bit field containing the Mobile Network Prefix

6.1.3. Padding Option

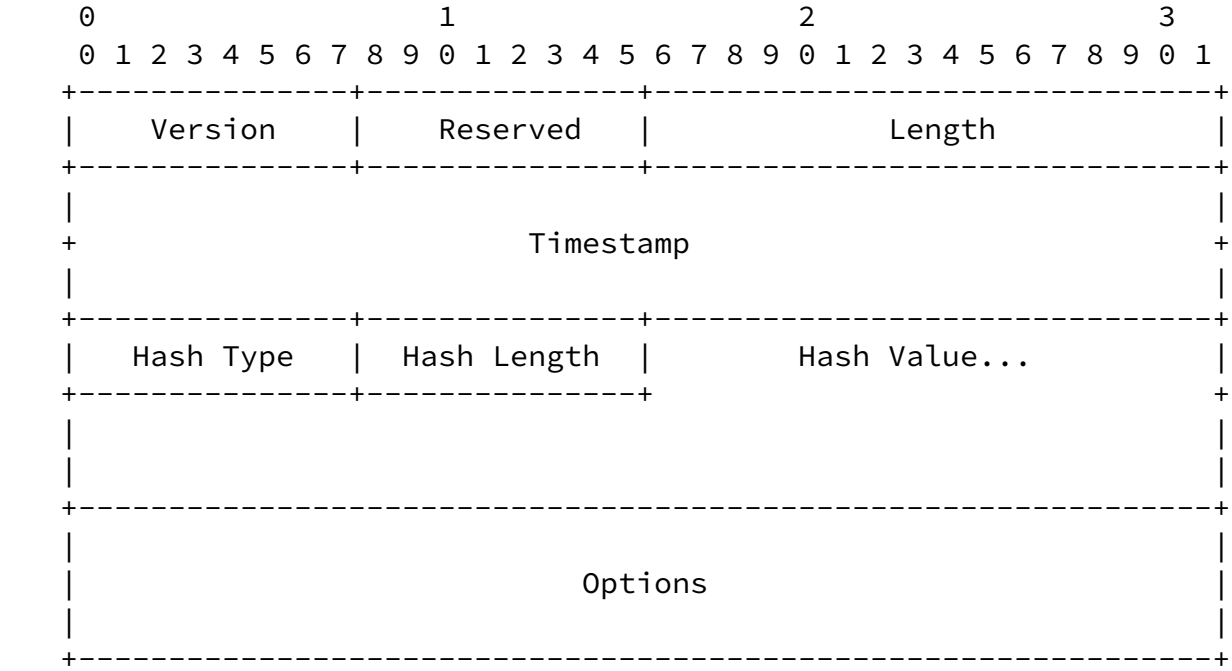
The format of the padding option is described below. Multiple padding options can be included in a LMM.



Type
Set to 0.

6.2. Time Adjusting Message

The format of Time Adjusting Message is described below.



Version
8-bit unsigned integer indicates the version of this protocol.
Set to 1.

Reserved
This field is unused for now. The value MUST be initialized to 0 by the sender and MUST be ignored by the receiver.

Length
16-bit unsigned integer indicates the length in octets of the

message, including the version, reserved and the length field.

Timestamp
64-bit unsigned integer indicates the time of generating the message. The MR MUST set this field to a 64-bit value specified by the Network Time Protocol.

Hash Type
8-bit unsigned integer indicates the type of hash algorism. The values shown below are decimal values.
1 keyed-MD5
keyed-MD5 MUST be supported by all MRs.

Hash Length
8-bit unsigned integer indicates the length of the hash value field in octets.

Hash Value
This field is hash value generated by the method indicated in the hash type field and the length is indicated in the hash length field.

Options
The options field follows the hash value field. No options are defined for now.

6.3. Hash Value

The hash value is used for authentication of the message. This protocol supports the following hash types.

6.3.1. keyed-MD5

In case of using keyed-MD5[6] for authentication, the hash value is generated from the following byte stream with "prefix+suffix" mode.

- the shared secret defined between the MRs and by hash type, followed by
- the message with hash value field filled by 0 excluding UDP and IP headers, followed by
- the shared secret again

Then the hash value field is filled with the computed value.

7. Link Metric

The link metric is the sum of the link quality value of the interface and the pre-configured preference value, with a exception. The exception is the case the link quality value is 0. In this case the link metric MUST set to 0.

The link metric is 32-bit unsigned integer and the larger interface metric means the interface has higher priority. If a metric is 0, it means the interface is unavailable or will be going to be unavailable, for example, the interface of multi-channel media will start channel scan.

The link quality value is 16-bit unsigned integer. This value changes dynamically according to the quality of the link. The MR MUST set it to the value by the profile defined for the media by other document.

The preference value is 32-bit unsigned integer and MUST NOT be greater than 0xffff0000.

8. Security Consideration

The MR MUST filter the received messages by their source IP address and the hash value for avoiding the attack of fake messages. Replay attack is avoidable by using the timestamp.

9. References

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

[2] Manner, J. and M. Kojo, Eds., "Mobility Related Terminology", RFC 3753, June 2004.

[3] Ernst, T., and H.-Y. Lach, "Network Mobility Support

Terminology", Work in Progress, October 2004.

[4] Conta, A., "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", RFC 2463, December 1998.

[5] Mills, D., "Network Time Protocol (Version 3): Specification, Implementation and Analysis", RFC 1305, March 1992.

[6] Rivest, R., "The MD5 Message-Digest Algorithm", RFC 1321, April 1992.

Authors' Addresses

Hitoshi Morioka
ROOT INC.
2-1-22-307 Momochihama,
Sawara-ku, Fukuoka
814-0001
Japan

EMail: hmorioka@root-hq.com

Intellectual Property Statement

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.

Disclaimer of Validity

Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.